



DETECÇÃO E PREVENÇÃO DE AMEAÇAS CIBERNÉTICAS



Co-funded by the
Erasmus+ Programme
of the European Union



Financiado pela União Europeia. Os pontos de vista e as opiniões expressas são as do(s) autor(es) e não refletem necessariamente a posição da União Europeia ou da Agência de Execução Europeia da Educação e da Cultura (EACEA). Nem a União Europeia nem a EACEA podem ser tidos como responsáveis por essas opiniões.



Índice

1. Introdução

2. O conceito de cibercriminalidade e conceitos relacionados

- 2.1. Cibercriminalidade
- 2.2. Classificação das formas de cibercriminalidade
- 2.3. Cyberattack
- 2.4. RESUMO / PRINCIPAIS RESULTADOS DO CAPÍTULO

3. Protecção penal contra a cibercriminalidade

- 3.1. Cibercrime em documentos internacionais e da CE/UE
- 3.2. Aspectos substantivos da cibercriminalidade na Polónia
- 3.3. Aspectos substantivos da cibercriminalidade em Portugal

4. Manifestações de cibercriminalidade

- 4.1. Engenharia Social
- 4.2. Botnet
- 4.3. Malware
- 4.4. Ransomware
- 4.5. Spam
- 4.6. Phishing, Pharming, Spear Phishing, Vishing, Smishing
- 4.7. Compromisso de e-mail comercial (BEC)
- 4.8. Sítios Web fraudulentos (empresas)
- 4.9. Hacking
- 4.10. Cracking
- 4.11. Pirataria na Internet (informática)
- 4.12. Sniffing
- 4.13. Ataques DoS, DDoS, DRDoS
- 4.14. Divulgação de conteúdos defeituosos
- 4.15. Ataques cibernéticos em redes sociais
- 4.16. Roubo de identidade
- 4.17. APT (Ameaça Persistente Avançada)
- 4.18. Ciberterrorismo
- 4.19. RESUMO / PRINCIPAIS RESULTADOS DO CAPÍTULO

5. Conclusão

6. Lista de referência

1. Introdução

Actualmente, as tecnologias de informação e comunicação são indispensáveis. A sua contribuição para a sociedade em todas as áreas da actividade humana (por exemplo, ciência médica, investigação, segurança, transportes, etc.) é indiscutível. O campo das tecnologias da informação e da comunicação é o ramo mais rápido e mais proliferante da actividade humana.

O que precisa de ser realizado é o facto de que a informação ou dados e a sua utilização envolvem um potencial económico e político considerável. A informação, como dados em bruto e fluxo de dados, pode determinar não só a existência ou não existência de um indivíduo ou empresa, mas também, pela sua natureza, influenciar o desenvolvimento global.

No entanto, a utilização das tecnologias de informação e comunicação tem também os seus inconvenientes. Um deles, sem dúvida, é o aumento gigantesco e dinâmico do "novo tipo" de crime, que deve ser tratado de forma a não pôr em perigo e violar os interesses da sociedade. Este crime pode ser colectivamente designado por cibercriminalidade.[1]

É de notar que, a uma escala global, podem ser observados esforços consideráveis, tanto a nível jurídico como de segurança, para tomar medidas adequadas para responder a este novo e dinâmico fenómeno de hoje.[2]

Três factos tornaram-se **pontos-chave para o desenvolvimento da cibercriminalidade**. [3] O primeiro é a ligação de quatro computadores universitários e a criação de uma rede informática para a partilha de dados. [4] O segundo é a criação do primeiro Computador Pessoal da IBM no final dos anos 80. O terceiro e, na minha opinião, o marco mais importante é tornar a Internet acessível ao público em geral, incluindo a modificação de aplicações individuais para uma forma mais fácil de utilizar.

O desenvolvimento da sociedade digital de hoje não se baseia directamente no desenvolvimento económico associado aos recursos materiais, mas no desenvolvimento das TI, na ligação de cada vez mais utilizadores à Internet, mas especialmente nas aplicações como tal e, por último mas não menos importante, na obtenção de informações e dados dos próprios utilizadores. Estas mudanças estão ligadas ao desenvolvimento das TI, tanto social como economicamente, e são uma das causas da cibercriminalidade.

O ciberespaço é actualmente a arma mais eficaz e perigosa nas mãos dos cibercriminosos. Não é que o ciberespaço ou a própria Internet sejam perigosos ou desprovidos de segurança. A questão é que um sistema é sempre tão forte como o seu elo mais fraco. Neste caso, o elemento mais fraco é, mais do que nunca, um utilizador. De facto, um utilizador é a maior "ameaça" para si próprio e para o seu meio envolvente, porque apesar de ter personalidade jurídica [5], muitas vezes tem apenas um conhecimento mínimo dos seus direitos e obrigações.

A Internet tornou-se uma parte da nossa vida quotidiana e especialmente o seu aspecto multimédia está a desenvolver-se muito rapidamente. A Internet, quer queiramos quer não, é um meio mais poderoso e predatório do que a televisão ou qualquer outro meio de comunicação de massas. Hoje em dia, mesmo um simples utilizador pode transmitir ou forçar os seus pensamentos ou opiniões a toda a população global através de uma interface simples. E não importa se os pensamentos são banais ou perversos de alguma forma.

Por um lado, a Internet oferece possibilidades praticamente ilimitadas para quase todos na obtenção e processamento de informação sobre quase tudo, sem necessidade de passar tempo em bibliotecas ou centros de informação fora de casa (a obtenção da informação em questão é uma questão de poucos segundos).

O Google e a Wikipédia tornaram-se relevantes e muitas vezes as únicas fontes de informação para as nossas decisões. A Internet permite a comunicação entre pessoas, facilita uma série de actividades graças à possibilidade de encontrar uma solução ou instruções, oferece uma série de canais de informação diferentes, etc. Ao mesmo tempo, permite-lhe fazer tudo isto a partir da sua casa e com um sentimento de anonimato quase absoluto.

Por outro lado, trabalhar neste ambiente virtual pode resultar em graves perdas financeiras, medo de intrusões na sua privacidade por parte de estranhos, perda de dados pessoais valiosos, comunicação online de pessoas mentalmente perturbadas (pedófilos, toxicódependentes, filosoficamente à deriva, etc.), comunicação destas pessoas com os nossos próprios filhos nas nossas costas, organização de grupos criminosos para actividades ilegais sem possibilidade de escuta por terceiros, fraude, intrusões não autorizadas em esferas privadas de empresas, redireccionamento de encomendas comerciais, roubo de contas de outras pessoas, destruição de dados e bases de dados, violação de direitos de autor, etc.

Não se pode permitir que o ciberespaço se torne um ambiente onde os perpetradores possam cometer qualquer crime praticamente sem punição. Mas há apenas um ponto de partida para combater o crime no ciberespaço, e que é o próprio ciberespaço. É necessário compreender o que o ciberespaço realmente representa, em que princípios funciona, que tipos de crime podem ocorrer neste mundo virtual, e o que todas as agências de aplicação da lei, mas especialmente o próprio utilizador, podem fazer contra esta actividade ilegal.

Como já foi mencionado, a cibercriminalidade tem vindo a ganhar ímpeto nos últimos tempos. Devido à sua natureza variada, uma vasta gama de cada um dos nossos direitos humanos fundamentais é violada, e as tecnologias de informação e comunicação tornam-se assim os meios pelos quais o crime é cometido ou são eles próprios o alvo desta actividade.

Uma diferença significativa entre o cibercrime e outros tipos de crime é a sua considerável latência, frequentemente um elevado nível de tolerância por parte da sociedade (incluindo a indiferença do utilizador a potenciais ameaças), o anonimato real ou percebido do perpetrador e a sua difícil identificação, bem como todo o processo de prova. Por conseguinte, é necessário não só abordar a questão da acção repressiva contra os infractores mas também a questão da prevenção do crime nesta área, bem como a questão da possível protecção da sociedade contra este crime.

A prevenção efectiva destes fenómenos negativos deve necessariamente começar pelos utilizadores finais, porque no ciberespaço são eles que são a típica primeira vítima de um agressor. Com base na minha experiência, estou convencido de que a educação e formação dos utilizadores deve ser uma parte essencial da penetração das tecnologias de informação e comunicação nas nossas vidas. Acredito que a construção da literacia da informação deve estar inextricavelmente ligada à criação, distribuição e promoção de produtos ou serviços associados às tecnologias da informação e da comunicação. A verdadeira educação nesta área, ou melhor, a aprendizagem sobre possíveis ameaças, riscos e inconvenientes colocados pelas TI, deveria fazer parte do ensino de todas as formas de estudo em todos os níveis de ensino.

No que diz respeito às pessoas que lidam com esta questão a nível profissional, são colocadas exigências ainda maiores a estes especialistas, uma vez que devem aprender e treinar constantemente para serem capazes de enfrentar ataques sempre novos e dinamicamente crescentes por meios TIC e no ambiente das TIC.

[1] A **cibercriminalidade** é frequentemente referida por vários nomes. Creio que o cibercrime é o termo mais apropriado para esta infracção. Nesta monografia, os termos **cibercrime**, **cibercriminalidade** ou **actividade criminosa cibernética** serão também utilizados para se referir a este fenómeno.

Na próxima parte desta publicação será incluída uma definição das diferenças entre crime e actividade criminosa nesta área, bem como uma definição dos pontos de vista de vários autores sobre o rótulo exacto para esta actividade criminosa. O termo cibercriminalidade será utilizado na sua maioria nesta publicação.

[2] Por exemplo: *Luta contra o cibercrime: patrulhas cibernéticas e equipas de investigação na Internet para reforçar a estratégia da UE*. [em linha]. [cit.10.7.2016]. Disponível a partir de: <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827>

[3] Estes factos foram então apoiados por uma série de outras circunstâncias (por exemplo, falta de legislação em relação à Internet, incapacidade de aplicar a lei, o sentimento de anonimato entre os utilizadores, etc.).

[4] Para mais detalhes ver ARPANET ou NSFNET. Estamos no final da década de 1960.

Cf. *Mapas Históricos de Redes de Computadores*. [em linha]. [cit.10.7.2016]. Disponível a partir de:

<https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html>

[5] Eles têm direitos e obrigações. Os utilizadores estabelecem, alteram e possivelmente terminam relações jurídicas.

2. O conceito de cibercriminalidade e conceitos relacionados



2.1. Cibercriminalidade

A utilização de tecnologia informática, sistemas e tecnologias de informação e a sua integração em quase todos os ramos da actividade humana é um fenómeno característico da actualidade. Pode-se afirmar que, **em princípio, não é possível encontrar tal área de actividade humana, onde a tecnologia informática, ou sistema de informação ou tecnologia de informação ou comunicação, não seria utilizada directa ou indirectamente.**

Infelizmente, à medida que as possibilidades de utilização destas conveniências modernas e o progresso científico e técnico aumentam, aumentam também as possibilidades e ao mesmo tempo a frequência da sua má utilização para cometer crimes.

Nos anos 90, o termo "**crime informático**" (počítačová kriminalita, *Computer kriminalität*) foi estabelecido para o crime informático. Na sua publicação, Smejkal define, em meados dos anos 90, o *crime informático* como uma mistura diversificada de crimes cujo factor comum é o computador, o programa e os dados. O termo crime informático "... deve ser entendido como cometer um crime em que o computador como um agregado de hardware e software, incluindo dados, ou um grande número de computadores separados ou ligados a uma rede informática é central para ser o sujeito de tal crime, embora com **excepção de um crime em que o referido dispositivo é o sujeito do crime como simples propriedade, ou como instrumentos do crime**".^[1] Da definição acima referida resulta claro que o crime informático se relacionava apenas com sistemas informáticos como alvos de ataque.

O termo "crime informático" evoca a ideia de que um crime deve ser cometido num computador ou através de um computador, na maioria das vezes um computador pessoal (PC). Tal entendimento é agora simplista e, ao mesmo tempo, reduz um pouco, em termos quantitativos, o número de fenómenos que podem ser incluídos no conceito de crime cometido através das tecnologias da informação e da comunicação. Muitos dispositivos técnicos de hoje, graças à implementação de microprocessadores juntamente com a sua miniaturização, assumiram o papel de computadores pessoais (PCs) há muito tempo atrás, sem serem chamados computadores pessoais. Estes são híbridos que desempenham várias funções, que anteriormente eram desempenhadas por dispositivos especiais. Os dispositivos técnicos modernos que permitem a comunicação entre eles e os seus utilizadores e cuja concepção é orientada pelo princípio de *ALL-IN-ONE* são capazes de um poder de computação muito mais elevado do que as unidades de computação mais modernas da primeira metade dos anos 90. E mesmo estes dispositivos^[2], embora não sejam chamados computadores, podem ser o alvo do crime ou um meio de o cometer. Por estas razões, os termos "crime informático" ou "delito informático" são agora quase inexistentes na literatura científica. Em vez do termo "computador", são utilizados os termos "tecnologia de informação e comunicação" (ICT) e "crimes ICT".

Em 2000, o Conselho da Europa emitiu uma definição de criminalidade informática ao abrigo do Estatuto da Comissão de Peritos em Cibercriminalidade: "*Uma infracção contra a integridade, disponibilidade ou segredo dos sistemas informáticos ou uma infracção no sentido tradicional que utiliza as modernas tecnologias da informação e da comunicação*".^[3]

A Decisão-Quadro 2002/584/JAI do Conselho da UE sobre o mandado de detenção europeu refere-se à "**criminalidade informática**" como conduta dirigida contra um computador ou conduta em que o computador é um meio de cometer um crime. A definição de cibercrime baseia-se também na redacção do Mandado de Detenção Europeu.

Nas convenções internacionais, o termo "**cibercrime**" é mais frequentemente utilizado para o crime cometido através das tecnologias da informação, e a utilização deste termo foi também transferida da área normativa para o vocabulário do público profissional. O conceito de cibercriminalidade tem um carácter semelhante aos conceitos de "*crime violento*", "*delinquência juvenil*", "*crime económico*", etc. *Tais termos referem-se a grupos de infracções que têm um certo factor comum, como a forma de execução, a pessoa do perpetrador (pelo menos genericamente), etc. na sua essência, pode ser uma mistura muito diversa de infracções, ligadas por um factor comum (computador, programa, dados)*.^[4]

Ao definir o conteúdo do conceito de **cibercrime**, é necessário perceber que, juntamente com o crescimento das possibilidades de utilização de dispositivos de informação e comunicação, a possibilidade da sua utilização (abuso) para cometer crimes está também a crescer. Por conseguinte, na sua essência, não existe uma definição universal, geralmente aceite, que afecte plenamente o âmbito e a profundidade deste conceito.

Uma das definições possíveis de crime informático ou cibercrime também pode ser encontrada no Cybersecurity Glossary^[5]:

Cibercriminalidade

"Actividade criminosa em que um computador aparece de alguma forma como um agregado de hardware e software (incluindo dados), ou apenas alguns dos seus componentes podem aparecer, ou por vezes aparece um número maior de computadores quer isolados quer interligados numa rede informática, e isto quer como o objecto de interesse desta actividade criminosa (com excepção de tal actividade criminosa cujos objectos são os dispositivos descritos como bens imóveis) ou como o ambiente (objecto) ou como o instrumento da actividade criminosa (Ver Criminalidade informática)".

Crime informático / Cibercrime

"Crime cometido utilizando um sistema de processamento de dados ou rede informática ou directamente relacionado com os mesmos".

Estas duas definições mostram um esforço para definir todos os aspectos do cibercrime, mas os autores têm sido culpados de algumas imprecisões. Primeiro, utilizam ambos os termos sinonimamente, mas na definição de cibercrime, ignoram os factores de que o computador é simultaneamente um alvo e um meio de ataque. Problemas semelhantes associados a esta definição real de cibercriminalidade podem ser encontrados também noutros locais.

Num esforço para definir o cibercrime, é apropriado fazer uso da Convenção do Conselho da Europa nº 185 sobre o Cibercrime, de 23 de Novembro de 2001.^[6] Contudo, esta convenção não define o conceito de cibercriminalidade. Apenas define as medidas que devem ser adoptadas por uma parte ratificante a nível nacional. Estas medidas de direito penal substantivo definem então um quadro aproximado de crimes que são considerados cibercrimes. Este quadro (juntamente com outros crimes contidos no Protocolo Adicional n.º 189 do Conselho da Europa à Convenção sobre Cibercriminalidade^[7]) fornece um âmbito básico para uma unificação jurídica uniforme dos delitos penais que podem ser considerados cibernéticos, em todos os países. A definição efectiva, frequentemente muito rigorosa, de determinados crimes é bastante benéfica, uma vez que não limita a implementação nacional (mais detalhada ou elaborada) destes crimes mas, ao mesmo tempo, garante o cumprimento de requisitos mínimos (normas) por todas as partes ratificantes.

Também devido ao considerável desacordo sobre o que é e o que não é cibercrime, na parte seguinte deste capítulo iremos definir este conceito, tanto em termos de positivo como de negativo.

Nos termos mais gerais, o cibercrime pode ser definido como uma **conduta dirigida contra um computador, ou rede informática, ou como uma conduta em que um computador é utilizado como um instrumento para cometer um crime**. Um critério indispensável para a aplicação da definição de cibercrime é o facto de a rede informática, ou ciberespaço, ser então o ambiente em que esta actividade tem lugar.

Ao definir o conceito de cibercrime, é primeiro necessário **definir o conceito de crime em geral**. Relativamente à utilização de sistemas de informação, tecnologia informática ou dispositivos de comunicação, há uma série de acções que são certamente indesejáveis, mas que não são puníveis ao abrigo do direito penal, embora possam ser muito perigosas (prejudiciais) para a sociedade. Tais acções *a priori* não podem ser qualificadas como crime informático, informativo ou qualquer outro - não são de todo crimes. Ao definir o termo de criminalidade (e esta definição pode ser dada de vários pontos de vista - sociologicamente, criminalmente, etc.), confiamos na definição de criminalidade como um **resumo de todas as acções que podem ser classificadas sob um elemento objectivo, regulado pelo direito penal. Portanto, com base nesta definição, a criminalidade não envolve tais actos que não satisfaçam qualquer elemento objectivo de uma infracção penal, ou seja, nem sequer um delito ou outra infracção administrativa**. Tal definição do termo criminalidade é relativamente precisa e pode ser utilizada no domínio das tecnologias da informação e da comunicação.

Contudo, é uma característica da prática de crimes no domínio das TIC que tais práticas ou meios sejam utilizados para os cometer, cuja utilização não cumpre qualquer elemento objectivo de um crime, mas é parte integrante ou pré-requisito para o envolvimento em comportamentos criminosos.^[8] Além disso, estas práticas ou meios não criminosos são componentes importantes no processo de descoberta e esclarecimento do crime, cuja identificação e compreensão desempenha um papel importante na detecção de perpetradores deste tipo de crime.^[9]

O cibercrime representa o conjunto mais amplo para todos os crimes que ocorrem no ambiente das tecnologias de informação e comunicação. As infracções cometidas dentro deste conjunto podem ser ainda classificadas e etiquetadas com termos diferentes, de acordo com vários aspectos. "Crime na Internet", "e-crime", "ciberterrorismo" ou, por exemplo, "pirataria" podem então formar subconjuntos de crimes cibernéticos, embora esta lista não esgote os possíveis subconjuntos de acções que podem ser classificadas como crimes cibernéticos.

O cibercrime é mais frequentemente utilizado em publicações profissionais para descrever tais **actos** criminosos **em que os meios das tecnologias da informação e da comunicação são:**

- a) **utilizado como instrumento para cometer um crime,**
- b) **o alvo do ataque do infractor,** o que constitui um delito.

Contudo, tal definição de cibercrime já não é válida hoje em dia. Isto incluiria crimes que envolvem a utilização de tecnologias de informação mas não no contexto da sua utilização ou intenção normal (por exemplo, casos em que um infractor feriu uma pessoa ao bater com um monitor ou outra parte do computador na cabeça da parte lesada com a intenção de causar danos pessoais; ou no caso de roubo de um camião com componentes informáticos, etc.). Estes são crimes em que as TIC são utilizadas para além da sua finalidade - por exemplo, como uma arma, como uma coisa que tem um certo valor monetário, independentemente da finalidade a que se destinam ou deveriam destinar-se. Ao descobrir e esclarecer estes actos, serão utilizadas outras metodologias de investigação (tais como a metodologia de investigação de roubo, etc.), e não métodos de investigação de crimes informáticos.

Para falar de crimes informáticos, as tecnologias de informação e comunicação que tenham sido utilizadas para cometer um crime ou que tenham sido alvo de um tal crime devem ser contextualizadas. Neste espírito, é portanto necessário atribuir um outro ponto que contenha esta condição aos dois pontos acima referidos. O cibercrime, portanto, é um crime em que os meios das tecnologias da informação e da comunicação são:

- a) **utilizado como instrumento para cometer um crime,**
- b) **são o alvo do ataque do perpetrador, e esse ataque é uma ofensa,**

desde que estes dispositivos sejam utilizados ou mal utilizados num ambiente de informação, sistema, programa ou comunicação (isto é, no ciberespaço).

No entanto, tal definição de cibercrime continua a ser inadequada. Utilizando os critérios estabelecidos desta forma para determinar se uma conduta específica pode ou não ser considerada crime informático, concluímos que, por exemplo, aspectos da definição de participação (organização, orientação e assistência) no sentido da Secção 24 da Lei n.º 40/2009 Sb., Código Penal, tal como emendada,^[10] é possível cometer qualquer crime intencional através de meios de informação (por exemplo, uma pessoa faz com que outra pessoa cometa um crime de homicídio intencional por correio electrónico). Será semelhante para outras formas de cooperação criminal (por exemplo, incitação, endosso de um crime). Estas também podem ser cometidas utilizando tecnologias de informação. **Contudo, tais acções não podem ser descritas como crimes cibernéticos. Como resultado, aceitar o ponto de vista oposto levaria à única conclusão possível - qualquer crime em que um criminoso utilizasse de qualquer forma as tecnologias da informação e da comunicação é um crime cibercriminoso.** Deste ponto de vista, seria difícil encontrar crimes que não possam ser considerados como crimes cibernéticos.

Do acima exposto resulta que não basta definir o cibercrime apenas positivamente, mas também é necessário defini-lo através de uma lista de acções que, em princípio, não podem ser consideradas cibercriminalidade.

Neste espírito, será possível incluir crimes de três categorias diferentes sob o termo cibercrime:

- 1) crimes em que o objecto individual que caracteriza o elemento objectivo é directamente a protecção do sistema informático, do seu equipamento e componentes contra tipos específicos de ataques ou os legítimos interesses das pessoas na utilização ininterrupta destes dispositivos técnicos,
- 2) crimes que são cometidos através das tecnologias de informação e comunicação é uma das características do elemento objectivo,

3) outros crimes elegíveis que não se enquadram nem na primeira nem na segunda categoria, mas que também podem ser cometidos no caso específico através das tecnologias de informação e que satisfazem a definição acima referida, porque podem ser utilizados procedimentos de detecção semelhantes aos da investigação de crimes da primeira e segunda categorias (por exemplo, pareceres de peritos com objectivos semelhantes) para os descobrir e esclarecer.

[1] SMEJKAL, Vladimír, Tomáš SOKOL e Martin VLČEK. *Počítačové právo*. Praga: C. H. Beck, 1995, p. 99

[2] Actualmente, existem vários dispositivos, que são referidos como um sistema informático.

[3] MATĚJKA, Michal. *Počítačová kriminalita*. Praga: Computer Press, 2002, p. 5

[4] Smejkal, Vladimír. *Kybernetická kriminalita*. Plzeň: Aleš Čeněk, 2015, p. 19

[5] JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Výkladový slovník kybernetické bezpečnosti*. [online]. 2ª edição actualizada. Praga: AFCEA, 2015, p. 57 e 73. [online]. [cit.10.7.2016]. Disponível em: <https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovník-kyberneticke-bezpecnosti--druhe-vydani/>

[6] A seguir referida como a **Convenção sobre Cibercriminalidade**. Para mais pormenores, ver <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>

[7] A seguir referido como o **Protocolo Adicional**. ETS No. 189 Protocolo Adicional à Convenção sobre Cibercriminalidade, relativo à criminalização de actos de natureza racista e xenófoba cometidos através de sistemas informáticos

Para mais detalhes, ver <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189>

[8] Por exemplo, o envio de spam. Por vezes, o spam só pode ser uma mensagem publicitária (comercial). Tal conduta não é punível ao abrigo do direito penal. Pode-se imaginar, por exemplo, o envio de SPAM por razões políticas, religiosas ou outras. Outras vezes, o SPAM pode conter malware que lhe permite obter um nome de utilizador e senha para a conta bancária do cliente (que em determinadas circunstâncias pode ser qualificado, por exemplo, como preparação para um crime).

[9] Por exemplo, quando o perpetrador comunica com o seu ambiente, é possível localizar o endereço IP do seu PC e depois localizar a localização da ligação do perpetrador à Internet.

[10] A seguir referido como **Código Penal** ou **CC**.

2.2. Classificação das formas de cibercriminalidade

Creio que se quisermos abordar a questão do crime cibernético, seria apropriado pelo menos definir os parâmetros que delimitam este crime. No final deste subcapítulo, quero apresentar ao leitor algumas classificações de crimes cibernéticos (ou informáticos) tal como são percebidos pelas diferentes regras processuais e por vários autores ou organizações que estão envolvidos na luta contra o crime cibernético. Quero também demonstrar nestas categorias a génese da visão da questão do cibercrime.

1. Classificação de acordo com a Convenção sobre Cibercriminalidade e de acordo com o Protocolo Adicional.

A Convenção sobre o Cibercrime divide o cibercrime em quatro categorias:

1. **Ofensas contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos,**
2. **Infracções relacionadas com a informática,**
3. **Infracções relacionadas com o conteúdo,**
4. **Infracções relacionadas com a violação dos direitos de autor e direitos conexos.**

O Protocolo Adicional define então outros cibercrimes:

1. **Divulgação de material racista e xenófobo através de sistemas informáticos,**
2. **Ameaça de motivação racista e xenófoba,**
3. **Insulto de motivação racista e xenófoba,**
4. **Negação, minimização grosseira, aprovação ou justificação de genocídio ou crimes contra a humanidade.**

2. Classificação do Comité de Peritos sobre o Crime no Ciberespaço

De acordo com o Estatuto do Comité de Peritos sobre o Crime no Ciberespaço do Conselho da Europa de 2000, o crime cibernético pode ser dividido em:

1. **De acordo com a posição do computador ao cometer um crime:**

- *alvo do ataque;*
- *meios (ferramenta) do ataque.*

2. **De acordo com o tipo de acto:**

- *infracções tradicionais* (tais como contrafacção, etc.)
- *novas infracções* (tais como phishing, DDoS, etc.)

3. Classificação de acordo com a eEurope+

Este documento dividiu os crimes informáticos em:

1. **Crimes que violam a privacidade**

- Recolha, armazenamento, modificação, divulgação e divulgação ilegais de dados pessoais.

2. **Crimes relacionados com conteúdo informático**

- Pornografia infantil, racismo, incitamento à violência, etc.

3. **Económico**

- Acesso não autorizado, sabotagem, hacking, transmissão de vírus, espionagem informática, falsificação informática e fraude.

4. **Crimes relacionados com a propriedade intelectual^[1]**

4. classificação da criminalidade informática de acordo com a criminologia

Porada e Konrád^[2] divide o cibercrime em cinco grupos básicos.

1. **Alteração não autorizada de dados introduzidos**

- alteração do documento de entrada para processamento informático,
- criação de um documento contendo dados falsos para posterior tratamento de dados por computador,

2. **Alterações não autorizadas aos dados armazenados**

- manipulação de dados, adulteração não autorizada dos mesmos e posterior regresso ao normal,

3. Instruções não autorizadas para operações informáticas

- instrução directa para executar a operação ou para instalar o software que executa as operações automaticamente,

4. Intrusão não autorizada em computadores, sistema informático e respectivas bases de dados

- acesso informativo à base de dados, sem a utilização de informação,
- utilização não autorizada de informações para uso pessoal,
- alterações, destruição ou substituição de informação por outros,
- interceptação "ilegal" e registo do tráfego de comunicações electrónicas,

5. Ataque do computador, software e ficheiros e dados de outrem em bases de dados

- criação de programas de ataque,
- introdução de um vírus no software informático,
- infecção por vírus ou outros programas.

5.O foco da Europol em certos tipos de cibercrime por gravidade

A Europol respeita a Convenção sobre a Criminalidade Cibernética e cumpre a repartição das infracções nela contidas. O Centro Europeu do Cibercrime (EC3)[3] foi criado no seio da Europol para apoiar a luta contra a cibercriminalidade e assistir os Estados-Membros. Esta equipa declarou claramente o seu âmbito de actividade na luta contra a cibercriminalidade e identificou as três áreas seguintes (pontos focais - PF) de que trata:

1. **FP TERMINAL - Fraude de pagamento.** Um grupo dedicado à prestação de apoio em matéria de fraude em linha.
2. **FP Cyborg - Crimes de alta tecnologia.** Um grupo dedicado e que presta apoio a vários ciberataques que afectam infra-estruturas críticas[4] e sistemas de informação. Em particular, estes são ataques tais como: malware, resgates, hacking, phishing, roubo de identidade, etc.
3. **Gêmeos FP - Exploração Sexual Infantil.** Um grupo dedicado e que presta apoio na investigação do abuso sexual de crianças.

6. Classificação do cibercrime de acordo com a sua "relação" com o ambiente digital

Com o desenvolvimento da cibercriminalidade como tal, nos últimos anos, surgiu uma opinião que propõe a possibilidade de ver a cibercriminalidade como um acto que poderia ser descrito como cibercrime "puro" ou "genuíno". Apenas os ciberataques que tiveram lugar no ciberespaço e cujo objectivo e ferramenta era um sistema informático ou dados poderiam ser subsumidos sob tal conduta. Tipicamente, estes são ataques identificados como hacking, DoS, ataques DDoS, ataques a infra-estruturas críticas, etc.

Outros crimes cometidos no ambiente do ciberespaço só são considerados como a transferência de conduta criminosa "antiga" ou "ordinária" para o novo ambiente digital.

De acordo com a divisão acima referida, seria então possível compreender a cibercriminalidade numa

- Conceito estreito ("puro" cibercrime);
- Conceito amplo (conduta criminosa "ordinária" num novo ambiente).

Outras classificações possíveis de cibercriminalidade

Existem muitos outros métodos de classificação, para ilustrar outra possível divisão da cibercriminalidade.[5]

Neste ponto, gostaria de mencionar a minha classificação baseada nas minhas próprias descobertas obtidas especialmente na interpretação da cibercriminalidade em vários seminários ou conferências.

De uma forma simplificada, pode afirmar-se que o cibercrime pode ser visto de três perspectivas:

1. De acordo com a frequência (natureza) dos ataques:

- a) **violação de direitos de autor** (ver pirataria na Internet (informática). No ciberespaço, prevalece este acto que envolve a violação da propriedade intelectual. Os esforços para combater este fenómeno são particularmente evidentes por parte das organizações privadas de direitos de autor.);
- b) **outros ciberataques** (ver manifestações de cibercriminalidade. Excepto a pirataria na Internet (informática)).

2. De acordo com a punibilidade pelo direito penal:

- a) **conduta resolvida pelo direito penal** - alguns dos actos mencionados são subsuficientes sob o elemento objectivo do crime;
- b) **conduta não abordada (impune) pelo direito penal** - alguns dos actos mencionados não podem ser incluídos nos elementos objectivos legais da infracção penal, mesmo utilizando uma analogia admissível[6]).

3. De acordo com o grau de tolerância da sociedade maioritária:

- a) **conduta tolerada pela sociedade** (a conduta de violação dos direitos de autor é mais tolerada);
- b) **conduta não aceite pela sociedade** (por exemplo, pornografia infantil, etc.).

[1] Para mais detalhes: JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praga: Grada, 2007, p. 92

[2] Para mais detalhes: STRAUS, Jiří et al. *Kriminalistická metodika*. Plzeň: Aleš Čeněk, 2006, pp. 272-274

[3] *Combate ao Cybercrime na Era Digital*. [online]. [cit.7.5.2018]. Disponível a partir de: <https://www.europol.europa.eu/ec3>

[4] Relativamente à definição do termo infra-estrutura crítica, na República Checa (no caso do ciberespaço) é necessário proceder a partir da Lei sobre Cibersegurança e sobre a alteração de actos relacionados (Lei sobre Cibersegurança). A seguir referida como a Lei de **Segurança Cibernética**, ou **AoCS**. Na Secção 2 (b), esta lei define o termo de infra-estrutura de informação crítica e o elemento ou sistema de infra-estrutura crítica.

A definição do termo "infra-estrutura de informação crítica" baseia-se na legislação que rege a área da gestão de crises. A infra-estrutura de informação crítica é uma parte da infra-estrutura crítica, que é definida pela Lei n.º 240/2000 Sb., sobre gestão de crises e sobre alterações a certas leis (Lei de Crise), tal como alterada (doravante referida como a "Lei de Gestão de Crises"). Para ser incluído na infra-estrutura de informação crítica, um determinado sistema ou serviço de informação e rede de comunicações electrónicas deve satisfazer os critérios de definição da infra-estrutura crítica, bem como o elemento de infra-estrutura crítica definido pela Lei de Gestão de Crises e os critérios transversais e específicos de cada ramo estabelecidos pelo Decreto Governamental n.º 432/2010 Sb., sobre os Critérios para a Determinação do Elemento de Infra-estrutura Crítica.

O ponto VI foi inserido nos critérios específicos do ramo para determinar o elemento crítico da infra-estrutura desde a eficácia do acto e da cibersegurança. "*Sistemas de comunicação e informação*"; *G: ciber-segurança*. Os critérios específicos do ramo para a identificação de um dado sistema de informação, serviço ou rede de comunicações electrónicas por uma infra-estrutura de informação crítica são aqui estabelecidos.

No entanto, esta definição aplica-se apenas à área da ciber-segurança. Em geral, **é possível definir infra-estruturas críticas da seguinte forma:**

1. Infra-estrutura crítica significa um elemento de infra-estrutura crítica ou um sistema de elementos de ruptura de infra-estrutura crítica, cuja função teria um impacto significativo na segurança do Estado, na satisfação das necessidades básicas de vida da população, na saúde humana ou na economia do Estado.

2. Elemento de infra-estrutura crítica significa um edifício, instalação, ferramenta ou infra-estrutura pública determinada de acordo com critérios transversais e sectoriais, que são estabelecidos pelo Decreto Governamental n.º 432/2010 Sb., sobre os Critérios de Determinação do Elemento de Infra-estrutura Crítica.

3. O critério transversal para determinar o elemento crítico da infra-estrutura é o aspecto de

a) vítimas com um limiar de mais de 250 mortes ou mais de 2.500 pessoas com hospitalização subsequente por mais de 24 horas,

(b) um impacto económico com um limiar de perda económica do Estado superior a 0,5% do produto interno bruto, ou

(c) Um impacto no público com um limiar de restrição em grande escala na prestação de serviços essenciais ou outras interferências graves na vida quotidiana de mais de 125.000 pessoas.

[5] Cf. PROSISE, Chris e Kevin MANDIVA. *Incident Response & Computer Forensic, segunda edição*. Emeryville: McGraw-Hill, 2003, p. 22 e seguintes.

Depois, por exemplo, o *Crime Cibernético*. [online]. [cit.1.2.2015]. Disponível em:

<http://www.britannica.com/EBchecked/topic/130595/cybercrime/235699/Types-of-cybercrime>; etc.

[6] **Analogia significa a inclusão de um caso não explicitamente declarado no direito penal ao abrigo de uma disposição estatutária semelhante, especificada na lei.** Em contraste com a interpretação mais ampla, uma disposição é utilizada por analogia que, segundo o seu significado, não se aplica ao caso subsumido. Uma interpretação mais ampla é feita de acordo com a finalidade da lei penal e dentro dos seus limites, enquanto que a analogia ultrapassa estes limites imaginários. Utilizando uma analogia, **são preenchidas lacunas nas leis**. Trata de casos que um legislador não regulamentou através de uma norma legal. No contexto checo e português, **não podem ser utilizadas em detrimento de um infractor** (*in malam partem*).

2.3. Cyberattack

Prosise e Mandiva caracterizam um "**evento de segurança informática**" (que pode ser entendido como um ataque informático ou crime informático), como uma acção ilegal, não autorizada e inaceitável que envolve um sistema informático ou uma rede informática. Tal acção pode centrar-se, por exemplo, no roubo de dados pessoais, spam ou outro tipo de assédio, desvio de fundos, divulgação ou posse de pornografia infantil, etc.^[1]

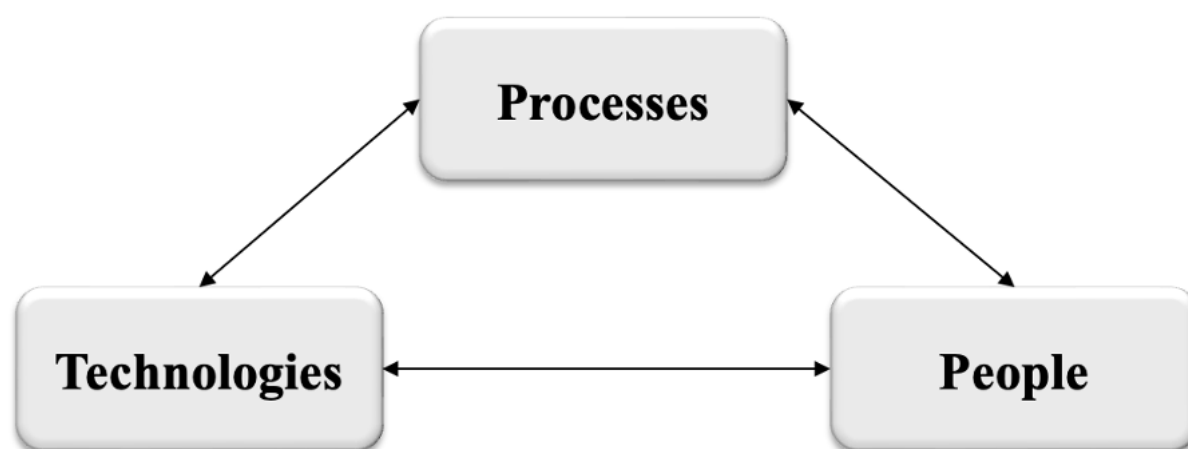
Jirásek et al. definem um ciberataque como: "*Um ataque a uma infra-estrutura informática para causar danos e obter informações sensíveis ou estrategicamente importantes*". É mais frequentemente utilizado no contexto de ataques de motivação política ou militar".^[2]

Uma tal definição de ataque cibernético reduziria significativamente e não afectaria todas as actividades negativas dos utilizadores do ciberespaço^[3], especialmente porque combina cumulativamente as condições de danos informáticos e de recuperação de informação. Um ciberataque pode também incluir acções sob a forma de engenharia social, em que o único objectivo é obter informação, ou, inversamente, um ataque DoS ou DDoS, em que o único objectivo pode ser suprimir (ou seja, não danificar) a funcionalidade de um ou mais sistemas ou serviços informáticos.

Com base no acima exposto, um **ataque cibernético**^[4] pode, portanto, ser definido como **qualquer conduta ilegal de um agressor no ciberespaço que seja dirigida contra os interesses de outra pessoa**. Estes actos nem sempre assumem a forma de um crime. A sua característica essencial é que perturbam o modo de vida normal da parte lesada. Um ataque cibernético conta, quer esteja concluído, em preparação ou numa fase de julgamento.^[5]

Um cibercrime também deve ser um ciberataque, mas nem todos os ciberataques devem ser um crime. Muitos ciberataques, mesmo devido à ausência de uma norma de direito penal, podem ser subsumidos a uma conduta que será, pela sua natureza, um delito administrativo ou civil, ou não pode ser uma conduta que seja punível por qualquer norma legal. (Pode ser, por exemplo, apenas uma conduta imoral ou indesejada).

O sucesso de um ciberataque reside tipicamente na violação de um dos elementos que compõem a ciber-segurança (**pessoas, processos e tecnologias**). **Estes elementos têm de ser aplicados ou modificados ao longo de todo o seu ciclo de vida. Em particular, eles dizem respeito à prevenção, detecção e resposta a ataques**. A segurança das TI, da informação e dos dados depende também directamente do respeito pelos princípios de "C", "I" e "A".



Elementos de ciber-segurança: Processos - Tecnologias - Pessoas

Se quisermos definir o termo ciberataque, é apropriado utilizar as definições que resultam da Lei n.º 181/2014 Sb., sobre Ciber-segurança e sobre a Alteração de Leis Relacionadas (Lei sobre Ciber-segurança).^[6] Esta Lei define na Secção 7 os termos de evento de cibersegurança e incidente de cibersegurança. O **evento de ciber-segurança** é "*um evento que pode causar uma quebra na segurança da informação nos sistemas de informação ou uma quebra na segurança dos serviços ou na segurança e integridade das redes de comunicações electrónicas*". Na realidade, é um evento sem uma consequência negativa real para um determinado sistema de comunicação ou de informação. No fundo, é apenas uma ameaça, mas deve ser real.

Um **incidente de ciber-segurança** é "*uma violação da segurança da informação nos sistemas de informação ou uma violação da segurança da prestação de serviços ou uma violação da segurança e integridade das redes de comunicações electrónicas devido a um evento de ciber-segurança*". Um incidente de ciber-segurança representa assim uma verdadeira violação da segurança da informação nos sistemas de informação ou uma violação da segurança dos serviços ou da segurança e integridade das redes de comunicações electrónicas, ou seja, uma violação de um sistema de informação ou de comunicação com um impacto negativo.

[1] PROSISE, Chris e Kevin MANDIVA. *Resposta a Incidentes & Forense Informática, segunda edição*. Emeryville: McGraw-Hill, 2003, p. 13

Ver também: CASEY, Eoghan. *Evidência Digital e Crime Informático: Forensic Science, Computers, and the Internet, Segunda Edição*. Londres: Academic Press, 2004, p. 9 e seguintes.

[2] JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Výkladový slovník kybernetické bezpečnosti*. [online]. 2ª edição actualizada. Praga: AFCEA, 2015, p. 59. Disponível a partir de: <http://afcea.cz/cesky-slovník-pojmu-kybernetické-bezpečnosti/>.

[3] A definição acima carece especialmente de uma definição de qualquer motivação do atacante que não seja a de... *causar danos ou ganhar informações estrategicamente importantes*. Um exemplo não abrangido por esta definição pode ser os ataques com motivações económicas, que estão a crescer dramaticamente no presente.

[4] É necessário distinguir o conceito de ciberataque do conceito de **incidente de segurança**, que representa uma violação da segurança SI/TI e das regras definidas para a sua protecção (política de segurança).

[5] Por exemplo, o ataque do vírus Conficker criado por Botnet. Isto completou o ataque. No entanto, permanece a questão de saber para que fins esta rede pode ser utilizada. (Pode estar em preparação para um ciberataque muito mais grave).

[6] A seguir referida como a **Lei sobre Ciber-segurança**, ou **AoCS**.

2.4. RESUMO / PRINCIPAIS RESULTADOS DO CAPÍTULO



RESUMO

- Para compreender a questão dos ciberataques e cibercriminalidade, é necessário conhecer a terminologia básica que está directamente relacionada com a área seleccionada. Este capítulo apresenta termos técnicos bem como jurídicos seleccionados.
- Não é possível encontrar uma área de actividade humana, onde a tecnologia informática, ou melhor, o sistema de informação, a tecnologia da informação ou da comunicação não seria utilizada directa ou indirectamente.
- O conceito de cibercrime tem um carácter semelhante aos conceitos de "crime violento", "delinquência juvenil", "crime económico", etc. Tais termos referem-se a grupos de infracções que têm um certo factor comum, como a forma de execução, a pessoa do perpetrador (pelo menos genericamente), etc. No fundo, pode ser uma mistura muito diversificada de infracções, ligadas por um factor comum (computador, programa, dados).
- O cibercrime pode ser definido como uma conduta dirigida contra um computador ou, em alguns casos, contra uma rede informática, ou como uma conduta em que um computador é utilizado como um instrumento para cometer um crime. Um critério indispensável para a aplicação da definição de cibercriminalidade é o facto de a rede informática, ou ciberespaço, ser então o ambiente em que esta actividade tem lugar.
- O cibercrime representa os actos criminosos em que se encontram os meios de informação e as tecnologias da comunicação:
 - o utilizado como instrumento para cometer um crime,
 - o o alvo de um ataque de um infractor, o que constitui uma ofensa.
 - o desde que estes dispositivos sejam utilizados ou mal utilizados num ambiente de informação, sistema, programa ou comunicação (isto é, no ciberespaço).
- Não basta definir o cibercrime apenas positivamente, mas também é necessário defini-lo através de uma lista de acções que, em princípio, não podem ser consideradas cibercriminalidade.
- Um ciberataque pode ser definido como qualquer conduta ilegal de um agressor no ciberespaço que seja dirigida contra os interesses de outra pessoa.
- O evento de cibersegurança é *"um evento que pode causar uma quebra na segurança da informação nos sistemas de informação ou uma quebra na segurança dos serviços ou na segurança e integridade das redes de comunicações electrónicas"*.
- Dados informáticos significa *"qualquer expressão de factos, informações ou conceitos de uma forma adequada ao processamento num sistema informático, incluindo um programa capaz de levar um sistema informático a executar uma função"*.
- A informação *"são dados que foram processados numa forma útil para um destinatário. Assim, cada informação é um dado, mas qualquer dado armazenado não se torna necessariamente informação"*.



PALAVRAS-CHAVE A LEMBRAR

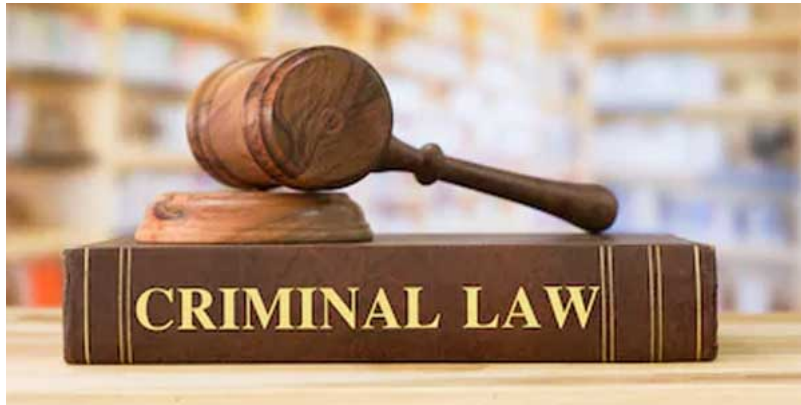
- cibercriminalidade
- ciberataque
- evento de ciber-segurança
- crime
- ciberespaço



PERGUNTAS DE VERIFICAÇÃO DE CONHECIMENTOS

- que é a cibercriminalidade?
- que não é a cibercriminalidade?
- que é um ciberataque?
- Qual é a diferença entre a cibercriminalidade e o ciberataque?
- Qual é a diferença entre dados e informação?
- que é a tríade da CIA?

3. Protecção penal contra a cibercriminalidade



Os esforços para regulamentar a lei e punir as actividades criminosas cometidas através das tecnologias da informação e da comunicação podem ser virtualmente observados desde o início destas actividades negativas. O cibercrime é muito diferente de outros tipos de crime, e esta diferença reside principalmente na possibilidade do seu desenvolvimento dinâmico e mudança imediata (de acordo com o sucesso ou fracasso de qualquer tipo de ataque), o que pode trazer certos problemas em relação à legislação.

No direito penal substantivo, aplica-se o princípio de que não é possível utilizar a analogia em detrimento de um infractor (*in malam partem*). No entanto, os ciberataques podem muitas vezes ser subsumidos a uma disposição legal de um elemento objectivo específico, embora esta natureza factual visasse originalmente "formas mais tradicionais" de cometer um crime (tipicamente ataques como violação dos direitos de autor, abuso de crianças para pornografia, etc.). No entanto, há uma série de novos ataques para os quais esta possibilidade está fora de questão. Nestes casos, os legisladores nacionais têm procurado, até à data, responder numa base *ad hoc* a estes novos tipos de crime, preenchendo assim as lacunas da legislação nacional.

Antes da análise real da actual legislação válida e eficaz no domínio da cibercriminalidade, deve notar-se que existe um esforço claro para implementar instrumentos jurídicos mais eficazes, e não apenas no seio da União Europeia, que seriam capazes de responder de forma atempada e adequada à cibercriminalidade. Isto elimina gradualmente inconsistências e deficiências nas normas jurídicas dos Estados-Membros da UE e de outros Estados que decidiram envolver-se activamente na luta contra a cibercriminalidade.

Um dos primeiros documentos sobre cibercrime adoptados a nível internacional é o **Manual das Nações Unidas sobre a prevenção e controlo da criminalidade informática** (Havana, 1990).^[1]

"Os métodos de protecção de dados e sistemas de informação são hoje objecto de muitos estudos científicos. No entanto, sem uma base jurídica, a protecção técnica destes sistemas e dados pode ser ineficaz devido à definição pouco clara de até onde é possível ir com tal protecção. Neste contexto, a inconsistência dos regulamentos legais de cada Estado com os regulamentos legais de outros Estados manifesta-se plenamente. Graças ao desenvolvimento das tecnologias informáticas e de informação, que indicam o carácter internacional do cibercrime, a protecção eficaz dos sistemas informáticos e dos dados é impensável sem a existência de um quadro jurídico internacional ou transnacional, não só entre os Estados-Membros da UE, mas também a nível mundial".

^[1]Manual das Nações Unidas sobre a prevenção e controlo da criminalidade informática. [em linha]. [cit.20.8.2016]. Disponível em: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf

3.1. Cibercrime em documentos internacionais e da CE/UE

A Convenção sobre o Cibercrime e o seu Protocolo Adicional associado devem ser mencionados em primeiro lugar, uma vez que estes são os dois documentos legais mais importantes que contribuem para a protecção da sociedade contra o cibercrime, estabelecendo um quadro básico para o cibercrime e fornecendo ao mesmo tempo os meios para o detectar e investigar. Serão igualmente apresentados documentos jurídicos da UE e da CE relacionados com a cibercriminalidade.

3.1.1 Convenção nº 185 do Conselho da Europa sobre Cibercriminalidade

A Convenção sobre o Cibercrime é o documento jurídico mais importante sobre o crime cibernético. O seu principal objectivo é unificar a legislação nacional no domínio da cibercriminalidade. O acima exposto é implementado pelo facto de a Convenção sobre o Cibercrime obrigar as partes contratantes a implementar nos sistemas jurídicos nacionais tais instrumentos que permitirão a punição de crimes cibernéticos definidos. É a definição completa do elemento objectivo do crime que constitui uma condição para a utilização das regras do direito penal no ciberespaço. Além disso, a Convenção sobre o Cibercrime cria um quadro jurídico para uma acção uniforme e conjunta contra os autores destes crimes, independentemente do local onde o crime foi cometido.

A Convenção sobre o Cibercrime foi aprovada pelo Comité de Ministros do Conselho da Europa na sua 109ª reunião de 8th de Novembro de 2001. A Convenção sobre o Cibercrime foi aberta à assinatura a 23rd de Novembro de 2001 em Budapeste.[\[1\]](#) Esta convenção entrou em vigor a 1st de Julho de 2004.

A República Checa assinou a Convenção sobre o Cibercrime a 9th de Fevereiro de 2005 e ratificou-a a 22nd de Agosto de 2013, entrando em vigor a 1st de Dezembro de 2013, enquanto Portugal a assinou no primeiro dia, mas só a ratificou a 24th de Março de 2010, entrando em vigor a 1st de Julho seguinte. Os Estados-Membros da UE comprometeram-se a ratificar a Convenção sobre o Cibercrime e a incorporar tais disposições nos seus sistemas jurídicos, o que tornaria possível esclarecer e investigar a referida actividade criminosa.[\[2\]](#) A Convenção sobre o Cibercrime também foi assinada e ratificada, por exemplo, pelos Estados Unidos, Japão e outros.

A Convenção sobre o Cibercrime[\[3\]](#) é constituída por um **preâmbulo** e **48 artigos**, que se dividem em 4 capítulos:

1. Utilização de termos

2. Medidas a tomar a nível nacional

Parte 1 - Direito penal substantivo (Artigos 2-13)

Parte 2 - Direito processual (Artigos 14-21)

Parte 3 - Jurisdição (Artigo 22)

3. Cooperação internacional

Parte 1 - Princípios gerais (artigos 23-28)

Parte 2 - Disposições específicas (artigos 29º-35º)

4. Disposições finais

Um passo importante para a unificação do direito é a definição de quatro grupos básicos de infracções penais (ver Capítulo II; Artigos 2-13) e a ancoragem de outros institutos gerais de direito penal substantivo. É a definição uniforme (denominação) dos ciberataques que permitirá a sua repressão mais eficaz nos países que ratificaram a Convenção sobre a Criminalidade Cibernética. Em particular:

1) **Ofensas contra a confidencialidade, integridade e disponibilidade de dados e sistemas informáticos.** (Artigos 2-6),

2) **Infracções relacionadas com a informática.** (Artigos 7-8),

3) **Infracções relacionadas com o conteúdo.** (Artigo 9º),

4) **Infracções relacionadas com a violação dos direitos de autor e direitos conexos.** (Artigo 10º).

Em termos de princípios gerais substantivos, *Tentativa e auxílio ou cumplicidade*. (Artigo 11º) e a *responsabilidade das empresas* por uma infracção penal ao abrigo da Convenção sobre a Cibercriminalidade são definidos com mais pormenor.

3.1.2 Protocolo Adicional nº 189 do Conselho da Europa à Convenção sobre a Cibercriminalidade

O Protocolo Adicional nº 189 do Conselho da Europa sobre a Convenção sobre a Cibercriminalidade[\[4\]](#), adoptado em 28th Janeiro 2003[\[5\]](#), define o leque de infracções que não são abrangidas pela Convenção sobre a Cibercriminalidade. A Convenção sobre a Criminalidade Cibernética não abrange as infracções relacionadas com a divulgação de determinado "*material nocivo*".[\[6\]](#) O Protocolo Adicional define as infracções penais que consistem principalmente na divulgação de material que contém material racista, xenófobo ou que de outra forma manifesta intolerância racial. A razão para não incluir os crimes em questão na Convenção sobre Cibercriminalidade foi, em particular, a assinatura e subsequente aceitação da Convenção sobre Cibercriminalidade pelos EUA.[\[7\]](#)

O Protocolo Adicional é constituído por um **preâmbulo** e **16 artigos**, que estão divididos em 4 capítulos:

1. Disposições comuns

2. Medidas a tomar a nível nacional

- Artigo 3 - Divulgação de material racista e xenófobo através de sistemas informáticos
- Artigo 4 - Ameaça de motivação racista e xenófoba
- Artigo 5 - Insulto de motivação racista e xenófoba
- Artigo 6 - Negação, minimização grosseira, aprovação ou justificação de genocídio ou crimes contra a humanidade

3. Relação entre a Convenção sobre Cibercriminalidade e o Protocolo Adicional

4. Disposições finais

O **primeiro capítulo** regula o objectivo do Protocolo Adicional e define o termo - material racista e xenófobo. De acordo com o Artigo 1 (1) do Protocolo Adicional, material racista e xenófobo significa "*qualquer material escrito, imagem ou outra expressão de ideias ou teorias que defenda, encoraje ou incite ao ódio, discriminação ou violência contra qualquer indivíduo ou grupo de indivíduos, com base na raça, cor, sexo ou origem nacional ou étnica, bem como religião, se usado como desculpa em vez de um destes atributos.* "

3.1.3 Documentos UE/CE utilizados para harmonizar a legislação na luta contra a cibercriminalidade

Em particular, devido à natureza específica da cibercriminalidade e à necessidade de uma cooperação internacional eficaz, a UE procura aproximar as legislações de cada Estado-Membro para que este fenómeno negativo possa ser processado de forma mais eficaz. As decisões-quadro, directivas e outros documentos da UE/CE são principalmente um meio de se alinharem com a legislação de cada país da UE. Do ponto de vista da luta contra o cibercrime, os documentos mais importantes são os seguintes:

- *Directiva 91/250/CEE do Conselho* relativa à protecção jurídica dos programas de computador
- *Decisão 92/242/CEE do Conselho* relativa à segurança dos sistemas de informação
- *Directiva 98/34/CE do Parlamento Europeu e do Conselho* relativa ao procedimento de informação no domínio das normas e regulamentações técnicas, com a redacção que lhe foi dada pela Directiva 98/48/CE
- *Directiva 2000/31/CE* relativa a certos aspectos legais dos serviços da sociedade de informação, em especial do comércio electrónico, no mercado interno ("Directiva sobre o comércio electrónico")
- *Decisão-quadro 2000/375/JAI do Conselho* relativa ao combate à pornografia infantil na Internet
- *Directiva 2002/21/CE do Parlamento Europeu e do Conselho* relativa a um quadro regulamentar comum para as redes e serviços de comunicações electrónicas (directiva-quadro)
- *Directiva 2002/19/CE do Parlamento Europeu e do Conselho* relativa ao acesso e interligação de redes de comunicações electrónicas e recursos conexos (Directiva Acesso)
- *Directiva 2002/20/CE do Parlamento Europeu e do Conselho* relativa à autorização de redes e serviços de comunicações electrónicas (Directiva "Autorização")
- *Directiva 2002/22/CE do Parlamento Europeu e do Conselho* relativa ao serviço universal e aos direitos dos utilizadores em matéria de redes e serviços de comunicações electrónicas (Directiva Serviço Universal)
- *Directiva 2002/58/CE do Parlamento Europeu e do Conselho* relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à protecção dos dados nas comunicações electrónicas)
- *Directiva 2002/77/CE da Comissão* relativa à concorrência nos mercados de redes e serviços de comunicações electrónicas (Directiva Concorrência)
- *Decisão-Quadro 2002/584/JAI do Conselho da UE* relativa ao mandado de detenção europeu e aos processos de entrega entre os Estados-Membros
- *Decisão-Quadro 2004/68/JAI do Conselho* relativa à luta contra a exploração sexual de crianças e a pornografia infantil
- **Decisão-quadro 2005/222/JAI do Conselho** relativa a ataques contra os sistemas de informação
- *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social e ao Comité das Regiões* - Luta contra o spam, o spyware e o software malicioso de 15 de Novembro de 2006
- *Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité Europeu das Regiões* sobre uma política geral de luta contra a cibercriminalidade, de 22 de Maio de 2007
- *Conclusões do Conselho* sobre uma estratégia de trabalho comum e medidas concretas para combater a cibercriminalidade, de 27 de Novembro de 2008
- *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões* sobre a protecção das infra-estruturas críticas da informação "Proteger a Europa contra os ciberataques e intrusões em grande escala: reforçar a preparação, a segurança e a resiliência", de 30 de Março de 2009
- *Comunicação da Comissão ao Conselho e ao Parlamento Europeu*, Combate à criminalidade na era digital: criação do Centro Europeu do Cibercrime. 2012

- *Regulamento (UE) n.º 526/2013 do Parlamento Europeu e do Conselho* relativo à Agência Europeia para a Segurança das Redes e da Informação (ENISA) e que revoga o Regulamento (CE) n.º 460/2004 de 21 de Maio de 2013
- *Directiva 2013/40/UE do Parlamento Europeu e do Conselho* relativa aos ataques contra os sistemas de informação e que substitui a Decisão-Quadro 2005/222/JAI do Conselho, de 12 de Agosto de 2013
- *Regulamento (UE) n.º 513/2014 do Parlamento Europeu e do Conselho* que estabelece, no âmbito do Fundo de Segurança Interna, um instrumento de apoio financeiro à cooperação policial, à prevenção e à luta contra a criminalidade e à gestão de crises e que revoga a Decisão 2007/125/JAI do Conselho, de 16 de Abril de 2014
- *Regulamento (UE) n.º 910/2014 do Parlamento Europeu e do Conselho* relativo aos serviços electrónicos de identificação e de confiança para transacções electrónicas no mercado interno e que revoga a Directiva 1999/93/CE de 23 de Julho de 2014 (Regulamento eIDAS, ou Regulamento eIDAS)
- *Regulamento (UE) 2016/794 do Parlamento Europeu e do Conselho* relativo à Agência Europeia de Cooperação Judiciária (Europol) e que revoga e substitui a Decisão 2009/371/JAI, 2009/934/JAI, 2009/935/JAI, 2009/936/JAI e 2009/968/JAI, de 11 de Maio de 2016
- *Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de Abril de 2016*, relativo à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Directiva 95/46/CE (Regulamento Geral sobre a Protecção de Dados)
- *Directiva do Parlamento Europeu e do Conselho (UE) 2016/1148*, relativa a medidas destinadas a assegurar um elevado nível comum de segurança das redes e sistemas de informação na União, de 6 de Julho de 2016 (Directiva SRI)
- *Directiva do Parlamento Europeu e do Conselho (UE) 2019/713* relativa ao combate à fraude e à contrafacção de meios de pagamento que não em numerário e que substitui a Decisão-Quadro 2001/413/JAI do Conselho, de 17 de Abril de 2019
- *Conclusões do Conselho sobre uma estratégia de trabalho comum e medidas concretas para combater a cibercriminalidade*, de 27 de Novembro de 2008
- *Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre a protecção das infra-estruturas críticas da informação "Proteger a Europa contra os ciberataques e intrusões em grande escala: reforçar a preparação, a segurança e a resiliência"* de 30 de Março de 2009

3.1.4 Normas legais da República Checa

Em relação ao cibercrime e à ciber-segurança, é necessário mencionar as normas legais da República Checa, que estão directamente relacionadas com esta questão:

- Lei n.º 40/2009 Sb., Código Penal
- Lei n.º 141/1961 Sb., sobre os procedimentos judiciais penais
- Lei n.º 218/2003 Sb., Lei sobre Justiça Juvenil
- Lei n.º 121/2000 Sb., Lei dos Direitos de Autor
- Lei n.º 127/2005 Sb., sobre Comunicações Electrónicas
- Lei n.º 480/2004 Sb., sobre certos serviços da sociedade da informação
- Lei n.º 273/2008 Sb., sobre a Polícia da República Checa
- Lei n.º 89/2012 Sb., Código Civil
- Lei n.º 110/2019 Sb., sobre o Tratamento de Dados Pessoais
- Lei n.º 14/1993 Sb., sobre Medidas para a Protecção da Propriedade Industrial
- Lei n.º 441/2003 Sb., sobre Marcas
- Lei n.º 527/1990 Sb., sobre Invenções, Desenhos Industriais e Propostas de Melhoramento
- Lei n.º 300/2008 Sb., sobre Leis Electrónicas e Conversão Autorizada de Documentos, com as alterações que lhe foram introduzidas
- Lei n.º 297/2016 Sb., sobre Serviços Criação de Confiança para Transacções Electrónicas
- Lei n.º 160/1999 Sb., sobre o livre acesso à informação
- Lei n.º 181/2014 Sb., sobre Ciber-segurança e emendas a leis conexas (Lei sobre Ciber-segurança)

3.1.5 Normas legais da Polónia

Na lei polaca, os principais regulamentos relativos ao cibercrime são:

- Acesso ilegal a um sistema (hacking) - Arte. 267 § 1 e 2 do Código Penal. Este crime é processado a pedido da parte lesada. São puníveis com uma multa, restrição da liberdade ou prisão até 2 anos.

- Quebra do segredo da comunicação (sniffing) - arte. 267 § 3 do Código Penal. Este tipo de crime consiste na obtenção de informações confidenciais, por exemplo através de sniffers, ou seja, programas que interceptam dados (palavras-passe e identificações de utilizadores). Tal acto é punível com uma pena de prisão até 2 anos.
- Violação da integridade dos dados (vírus, trojans), 268 do Código Penal, Arte. 268 a do Código Penal. Esta infracção diz respeito, nomeadamente, ao roubo de dados pessoais, à sua disponibilização a terceiros sem o consentimento do proprietário, bem como à sua utilização de forma não autorizada. Existem sanções financeiras (até PLN 100.000) pela prática destes actos.
- Violação da integridade do sistema - Arte. 269 do Código Penal. Um exemplo de tal crime são os ataques de inundaç  o Ping, que consistem em sobrecarregar a liga  o   Internet. Podem, por exemplo, levar   indisponibilidade de certos servi  os. O legislador polaco previu uma pena m  xima para este acto de at  8 anos de pris  o (em caso de viola  o da seguran  a do Estado).
- Artesanato "ferramentas de hacking" - Arte. 269 a do C  digo Penal, Art. 269 b do C  digo Penal. A pr  tica desta infrac  o   pun  vel com uma pena de 3 meses a 5 anos de pris  o.
- Lei de 5 de Julho de 2018 sobre o sistema nacional de ciber-seguran  a.

3.1.6 Normas legais de Portugal

Em rela  o   cibercriminalidade e   ciberseguran  a, em Portugal est  o em vigor os seguintes actos jur  dicos, v  rios deles repetidamente tentados:

- Lei n.  109/2009, a Lei sobre o Cibercrime
- Decreto-Lei n.  48/95, o C  digo Penal
- Lei n.  103/2015, sobre o registo criminal dos delinquentes condenados por delitos de autodetermina  o sexual de menores
- Lei n.  52/2003, sobre a luta contra o terrorismo
- Lei n.  58/2019, sobre a protec  o de dados, incluindo as jantes conexas
- Lei n.  59/2019, relativa ao tratamento de dados pessoais para efeitos de preven  o, detec  o, investiga  o ou repress  o de infrac  o  es penais ou de execu  o de san  o  es penais, incluindo crimes conexos
- Lei n.  32/2008, relativa   conserva  o dos dados gerados ou tratados no  mbito da presta  o de servi  os de comunica  o  es electr  nicas publicamente dispon  veis ou de redes p  blicas de comunica  o  es
- Decreto-Lei n.  131/2014, sobre a protec  o e confidencialidade da informa  o gen  tica, bases de dados gen  ticos humanos para fins de cuidados de sa  de e investiga  o sanit  ria
- Decreto-Lei n.  63/85, o C  digo dos Direitos de Autor e Direitos Conexos
- Decreto-Lei n.  252/94, sobre programas inform  ticos
- Decreto-Lei n.  110/2018, o C  digo da Propriedade Industrial
- Decreto-Lei n.  122/2000, sobre bases de dados
- Lei n.  46/2018, sobre a seguran  a do ciberespa  o
- Decreto-Lei n.  65/2021, que regulamenta a Lei n.  46/2018
- Decreto-Lei n.  62/2011, sobre infra-estruturas cr  ticas
- Lei n.  5/2004, sobre comunica  o  es electr  nicas
- Lei n.  41/2004, sobre privacidade e protec  o de dados nas comunica  o  es electr  nicas
- Lei n.  26/2016, sobre o acesso   informa  o administrativa
- Decreto-Lei n.  7/2004, sobre os servi  os da sociedade da informa  o
- Decreto-Lei n.  12/2021, sobre identifica  o electr  nica e servi  os de confian  a
- Lei n.  7/2007, sobre o cart  o de cidad  o
- Lei n.  37/2014, sobre a chave m  vel digital
- Decreto-Lei n.  91/2018, sobre servi  os de pagamento e dinheiro electr  nico
- Decreto-Lei n.  69/2014, que aprova a constitui  o do Centro Nacional de Ciber-Seguran  a

3.1.7 O cibercrime numa parte especial do C  digo Penal

Do ponto de vista da cibercriminalidade, o C  digo Penal cont  m elementos objectivos especiais de infrac  o  es penais, que se centram na cibercriminalidade, ou em alguns ciberataques.

O cibercrime é geralmente classificado em termos de utilização das tecnologias da informação e da comunicação em infracções penais quando estes elementos são utilizados como instrumento para cometer uma infracção penal e o elemento objectivo da infracção penal inclui a utilização destes meios como característica do elemento objectivo, e infracções penais quando elementos das tecnologias da informação e da comunicação são alvo de ataque de um infractor, ou seja, representam um objecto individual ou material objecto de ataque.

O legislador incluiu numa parte especial do Código Penal uma série de elementos objectivos de infracções penais, que ou contêm características relacionadas com as tecnologias de informação e comunicação ou podem ser preenchidas com um ataque cibernético. Estas infracções incluem:

- Secção 180 Manipulação ilícita de dados pessoais
- Secção 181 Violação dos direitos de outrem
- Secção 182 Violação do Sigilo da Correspondência
- Secção 183 Violação da confidencialidade de ficheiros e outros documentos privados
- Secção 184 Difamação
- Secção 191 Distribuição de Pornografia
- Secção 192 Produção e Manuseamento de Pornografia Infantil
- Secção 193 Abuso de uma Criança para Produção de Pornografia
- Secção 193b Estabelecimento de Contactos Ilegais com uma Criança
- Secção 205 Roubo
- Secção 206 Uso Não Autorizado de Propriedade de outrem
- Secção 209 Fraude
- Secção 213 Prática de Jogos e Apostas Desleais
- Secção 214 Participação
- Secção 216 Lavagem de dinheiro
- Secção 228 Danos a terceiros
- Secção 230 Acesso não autorizado a sistemas informáticos e meios de informação
- Secção 231 Obtenção e Posse de Dispositivos de Acesso e Senhas de Sistemas Informáticos e outros dados deste tipo
- Secção 232 Danos a Sistemas Informáticos e Registos de Meios de Informação e Interferência com Equipamento Informático por Negligência
- Secção 234 Obtenção Não Autorizada, Falsificação e Alteração de Meios de Pagamento
- Secção 236 Fabrico e Posse de Equipamento Falsificado
- Secção 264 Distorção de Dados e Falta de Registos de Exportação de Bens e Tecnologias de Dupla Utilização
- Artigo 268º Violação dos Direitos de Marca e Direitos a Outros Nomes
- Secção 267 Distorção de Dados e Falta de Registos de Comércio Externo com Material Militar
- Secção 269 Violação dos Direitos Económicos Protegidos
- Secção 270 Violação dos Direitos de Autor, Direitos Relacionados com os Direitos de Autor e Direitos a Bases de Dados
- Secção 272 Ameaça Pública
- Secção 276 Danos e Compromisso de Funcionamento de Facilidade Beneficiária Pública
- Secção 287 Propagação da Toxicodependência
- Secção 290 Ganho de Controlo sobre uma Aeronave, Embarcações Civis e Plataforma Fixa
- Secção 291 Pôr em perigo a segurança de um avião e de uma embarcação civil
- Secção 311 Ataque Terrorista
- Secção 316 Espionagem
- Secção 317 Informação Classificada em Perigo
- Secção 345 Acusação Falsa
- Secção 348 Falsificação e alteração de documentos públicos
- Secção 353 Ameaça Perigosa

- Secção 354 Perseguição Perigosa
- Secção 355 Difamação de Nação, Raça, Étnia ou outro Grupo de Pessoas
- Secção 356 Instigação do ódio contra um grupo de pessoas ou da supressão dos seus direitos e liberdades
- Secção 357 Disseminação de Hoaxes
- Secção 361 Participação em Grupo Penal Organizado
- Secção 364 Incitação à ofensa criminal
- Secção 365 Aprovação de Infracção Penal
- Secção 400 Genocídio
- Secção 403 Estabelecimento, Apoio e Promoção de Movimentos Destinados à Supressão dos Direitos Humanos e Liberdades
- Secção 404 Expressão de Simpatias para Movimentos em Busca da Supressão dos Direitos Humanos e Liberdades
- Secção 405 Negação, Concurso, Aprovação e Justificação do Genocídio
- Secção 407 Incitação de guerra ofensiva

Segundo o Código Penal, estes cibercrimes podem ser classificados de acordo com muitos critérios diferentes. Uma das classificações mais utilizadas de crimes cibernéticos é a classificação acima mencionada:[\[8\]](#)

a) infracções penais em cuja prática os meios de informação e comunicação são objecto de protecção (ou seja, que são alvo de um ciberataque):

- Secção 182 Violação do Sigilo da Correspondência
- Secção 183 Violação da confidencialidade de ficheiros e outros documentos privados
- Secção 206 Uso Não Autorizado de Propriedade de outrem
- Secção 228 Danos a terceiros
- Secção 230 Acesso não autorizado a sistemas informáticos e meios de informação
- Secção 232 Danos a Sistemas Informáticos e Registos de Meios de Informação e Interferência com Equipamento Informático por Negligência
- Secção 234 Obtenção Não Autorizada, Falsificação e Alteração de Meios de Pagamento
- Secção 264 Distorção de Dados e Falta de Registos de Exportação de Bens e Tecnologias de Dupla Utilização
- Secção 267 Distorção de Dados e Falta de Registos de Comércio Externo com Material Militar
- Secção 270 Violação dos Direitos de Autor, Direitos Relacionados com os Direitos de Autor e Direitos a Bases de Dados
- Secção 290 Ganho de Controlo sobre uma Aeronave, Embarcações Civis e Plataforma Fixa
- Secção 291 Pôr em perigo a segurança de um avião e de uma embarcação civil
- Secção 311 Ataque Terrorista
- Secção 317 Informação Classificada em Perigo

b) infracções penais em que os meios de informação e as tecnologias de comunicação são utilizados para cometer uma infracção penal:

- Secção 180 Manipulação ilícita de dados pessoais
- Secção 181 Violação dos direitos de outrem
- Secção 182 Violação do Segredo da Correspondência
- Secção 184 Difamação
- Secção 191 Distribuição de Pornografia
- Secção 192 Produção e Manuseamento de Pornografia Infantil
- Secção 193 Abuso de uma Criança para Produção de Pornografia
- Secção 193b Estabelecimento de Contactos Ilegais com uma Criança
- Secção 205 Roubo
- Secção 209 Fraude
- Secção 213 Prática de Jogos e Apostas Desleais

- Secção 214 Participação
- Secção 216 Lavagem de dinheiro
- Secção 230 Acesso não autorizado a sistemas informáticos e meios de informação
- Secção 231 Obtenção e Posse de Dispositivos de Acesso e Senhas de Sistemas Informáticos e outros dados deste tipo
- Secção 234 Obtenção Não Autorizada, Falsificação e Alteração de Meios de Pagamento
- Secção 236 Fabrico e Posse de Equipamento Falsificado
- Artigo 268º Violação dos Direitos de Marca e Direitos a Outros Nomes
- Secção 269 Violação dos Direitos Económicos Protegidos
- Secção 272 Ameaça Pública
- Secção 276 Danos e Compromisso de Funcionamento de Facilidade Beneficiária Pública
- Secção 287 Propagação da Toxicodependência
- Secção 316 Espionagem
- Secção 345 Acusação Falsa
- Secção 348 Falsificação e alteração de documentos públicos
- Secção 353 Ameaça Perigosa
- Secção 354 Perseguição Perigosa
- Secção 355 Difamação de Nação, Raça, Étnia ou outro Grupo de Pessoas
- Secção 356 Instigação do ódio contra um grupo de pessoas ou da supressão dos seus direitos e liberdades
- Secção 357 Disseminação de Hoaxes
- Secção 361 Participação em Grupo Penal Organizado
- Secção 364 Incitação à ofensa criminal
- Secção 365 Aprovação de Infracção Penal
- Secção 400 Genocídio
- Secção 403 Estabelecimento, Apoio e Promoção de Movimentos Destinados à Supressão dos Direitos Humanos e Liberdades
- Secção 407 Incitação de guerra ofensiva

Para além das disposições acima referidas de uma parte especial do Código Penal, a Secção 120 do Código Penal também se aplica à cibercriminalidade. Estipula que "*peças enganadoras ou que tirem partido do seu mal-entendido também podem ser feitas interferindo **com informações ou dados informáticos**, interferindo **com o equipamento informático de um computador ou realizando outra operação num computador**, interferindo com **um dispositivo electrónico ou outro dispositivo técnico**, incluindo a interferência com **objectos designados para controlar tal dispositivo**, ou utilizando tal operação ou interferência realizada por outra pessoa.*"

[1] Uma lista dos Estados que assinaram e ratificaram a Convenção sobre o Cibercrime pode ser encontrada em

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=F6wSLE5D.

[2] Esta obrigação está estabelecida nos artigos 14-21 da Convenção sobre o Cibercrime.

[3] O texto completo da Convenção pode ser encontrado em: <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>

[4] *ETS No. 189 Protocolo Adicional à Convenção sobre Cibercriminalidade, relativo à criminalização de actos de natureza racista e xenófoba cometidos através de sistemas informáticos*. [em linha]. [cit.20.8.2016]. Disponível a partir de:

<https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=090000168008160f>

[5] Uma lista dos Estados que assinaram e ratificaram o Protocolo Adicional pode ser encontrada em:

https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189/signatures?p_auth=F6wSLE5D

[6] Com excepção da pornografia infantil, que está directamente contida no artigo 9º da Convenção sobre o Cibercrime.

[7] É precisamente a questão do racismo e da xenofobia que é um tema da "zona cinzenta" nos EUA, uma vez que algumas declarações podem ser consideradas um crime e outras não. Por exemplo, nem todas as manifestações de racismo são consideradas crime nos **EUA**, ver a **Primeira Emenda à Constituição dos EUA** - *o Congresso não aprovará qualquer lei que ignore a liberdade de religião ou proíba o livre exercício (culto), ou que restrinja a*

liberdade de expressão ou de imprensa, ou o direito das pessoas a reunirem-se pacificamente e a apresentarem petições ao governo com vista a corrigir os erros. Para ser uma infracção ou uma infracção penal, a realidade da ameaça deve ser provada. Caso contrário, seria uma violação da primeira emenda. Em contraste, as expressões de racismo em **França** ou na **Alemanha**, bem como na **República Checa**, são consideradas um crime.

[8] Devido à dicção dos seus elementos objectivos, algumas infracções penais podem ser classificadas em ambas as categorias (estas disposições protegem os meios de informação e as tecnologias de comunicação, mas ao mesmo tempo contêm sinais de utilização abusiva destas tecnologias).

3.2. Aspectos substantivos da cibercriminalidade na Polónia

O legislador incluiu no Código Penal uma série de elementos objectivos de infracções penais, que ou contêm características relacionadas com as tecnologias de informação e comunicação ou podem ser satisfeitas por um ataque cibernético. Estas infracções incluem:

- Arte. 126a. Provocação pública para cometer um acto proibido
- Arte. 130. Espionagem
- Arte. 132. Desinformação da inteligência
- Arte. 133. Insulto à Nação ou à República da Polónia
- Arte. 135. Agressão ou insulto ao Presidente da República da Polónia
- Arte. 136. Agressão activa ou insulto a um representante de um estado estrangeiro
- Arte. 137. Insulto público a um sinal ou símbolo do Estado
- Arte. 151. Com o objectivo de cometer suicídio e dar assistência
- Arte. 165 Causando perigo público
- Arte. 190. Ameaça penal
- Arte. 190a. Perseguição
- Arte. 191. Forçar uma conduta específica, abandono ou supressão
- Arte. 191a. Gravação da imagem de uma pessoa nua
- Arte. 196. Ofensa contra os sentimentos religiosos dos outros
- Arte. 200a. Contacto electrónico com um menor para fins pedófilos
- Artigo 200b. Promoção pública de conteúdos pedófilos
- Arte. 202. Apresentação e distribuição de pornografia
- Arte. 212. Difamação
- Arte. 216. Difamação de uma pessoa
- Arte. 224a. Falso relato de uma ameaça
- Arte. 226. Insulto a um funcionário público ou a um órgão constitucional da República da Polónia
- Arte. 227. Apropriação indevida da função de um funcionário público
- Arte. 228. Suborno de um funcionário público
- Arte. 229. Suborno
- Artigo 230°. Patrocínio passivo pago
- Artigo 230°-A. Patrocínio activo pago
- Artigo 232. exercer influência sobre as actividades do tribunal
- Arte. 234. Acusação falsa
- Artigo 235. criação de provas falsas
- Arte. 236. Retenção de provas da inocência do suspeito
- Arte. 238. Falsa denúncia de uma infracção
- Arte. 239. Apoio e cumplicidade
- Arte. 240. Não denúncia penal de um acto criminoso
- Arte. 241. Divulgação ilegal das notícias do processo de instrução ou julgamento
- Arte. 244. Incumprimento das medidas penais ordenadas pelo tribunal
- Artigo 245 Utilização de violência ou ameaças para influenciar um participante no processo
- Artigo 246°. Extorsão por um funcionário público para dar testemunho, explicações, informações ou uma declaração

- Artigo 250º. Exercício ilegal de influência sobre uma pessoa com direito a voto
- Artigo 251º Violação do segredo do escrutínio
- Artigo 255º Incitação pública à prática ou elogio de uma transgressão ou infracção fiscal
- Artigo 255a. Divulgação de conteúdos que facilitem a prática de uma infracção terrorista
- Artigo 256 Propagação do fascismo ou outro regime totalitário
- Artigo 257. Racismo
- Arte. 265 Divulgação ou utilização de informações classificadas com a cláusula "secreto" ou "top secret".
- Arte. 266. Divulgação ou utilização de informações obtidas no âmbito do exercício de uma função ou actividade oficial
- Arte. 267 Obtenção de informações de forma ilegal
- Artigo 268 Obstrução à pessoa autorizada de apreender a informação
- Artigo 268a. Destruir, danificar, apagar, alterar ou obstruir o acesso aos dados informáticos
- Artigo 269º Destruir, danificar, apagar ou alterar dados informáticos sensíveis
- Artigo 269a. Interferência com o funcionamento de um sistema informático, sistema de comunicação de dados ou rede
- Artigo 269b. Produção, aquisição, eliminação ou fornecimento ilegal de programas informáticos
- Arte. 270. Falsificar um documento e utilizá-lo como autêntico
- Arte. 270a. Falsificação de uma factura e sua utilização para efeitos de autenticidade
- Arte. 271. Má representação
- Arte. 271a. Apresentação incorrecta numa factura
- Arte. 272. Utilização fraudulenta de declarações falsas num documento
- Arte. 273. Usando um documento que é falso Artigo 275.
- Arte. 275. Utilização do documento de identidade de outra pessoa
- Arte. 276. Destruir ou ocultar um documento sem o direito de dispor dele
- Arte. 277a. Falsificação de uma factura ou utilização de uma factura falsificada com o montante a indicar bens de grande valor
- Arte. 278. Roubo
- Arte. 282. Roubo
- Arte. 284. Apropriação indevida
- Arte. 285. Activação de impulsos telefónicos na conta de outra pessoa
- Artigo 286º. Fraude
- Arte. 287. Fraude informática
- Artigo 291. Recepção intencional
- Artigo 292. Recepção não intencional
- Artigo 293. Tomada de bens informatizada
- Artigo 296º. Causar danos nas transacções comerciais
- Artigo 296a. Suborno em posição de chefia
- Arte. 297. Extorsão do crédito
- Arte. 298. Extorsão da indemnização
- Artigo 299. Branqueamento de capitais
- Artigo 300º. Impedir a satisfação do credor
- Artigo 303. Falta de manutenção ou falsa manutenção de registos comerciais
- Artigo 304. Exploração da parte contratante
- Artigo 305. Interferência com concursos públicos

- Arte. 306. Remoção, contrafacção ou alteração de marcas de identificação
- Artigo 310. Falsificação de dinheiro, meios de pagamento ou títulos
- Artigo 311. Falsificação de informações no comércio de valores mobiliários
- Artigo 312. Circulação de dinheiro falso ou falsificado, meios de pagamento ou documentos de pagamento
- Artigo 313. Falsificação das marcas oficiais de títulos
- Artigo 314º. Falsificação de marcas oficiais com vista à sua utilização em transacções comerciais
- Arte. 346. Violência ou ameaça ilegal por parte de um soldado contra o seu superior
- Arte. 347. Insulto de um superior por um soldado

3.3. Aspectos substantivos da cibercriminalidade em Portugal

A principal característica das Fontes relativas ao cibercrime no sistema jurídico português é a sua dispersão. Mesmo estando em vigor uma *lei sobre o cibercrime*, na sequência da Convenção de Budapeste e da Decisão-Quadro 2005/222/JAI do Conselho de implementação, as infracções que implicam especificamente a utilização de sistemas TIC foram atribuídas a vários outros actos, incluindo o *Código Penal*. Além disso, desde 1991, os crimes relacionados com a protecção de dados pessoais são considerados diferentes dos cibercrimes em geral, quase com tipicidade paralela.

Assim, de acordo com o sistema jurídico português, os cibercrimes podem ser classificados de acordo com muitos critérios diferentes. Uma das classificações mais utilizadas de cibercrimes é a classificação acima mencionada:

a) infracções penais em cuja prática os meios de informação e as tecnologias da comunicação são objecto de protecção:

- Acesso ilegal (Art. 6 da Lei de Crimes Cibernéticos)
- Sabotagem informática [Interferência ilegal] (Art. 5 da Lei sobre o Cibercrime)
- Intercepção ilegal (Art. 7 da Lei de Crimes Cibernéticos)
- Danos a programas informáticos ou outros dados informáticos [Interferência de dados] (Art. 4 da Lei de Cibercriminalidade)
- Mau uso de dispositivos (Artes. 4(3), 5(2), 6(2) e 7(3) da Lei sobre o Cibercrime)
- Reprodução ilegal de programa informático protegido (art. 8º da Lei sobre a cibercriminalidade)
- Reprodução ou comunicação ilegal de uma base de dados protegida por direitos de autor (art. 11º do Decreto-Lei nº 122/2000)
- Remoção ou alteração de qualquer informação electrónica de gestão de direitos (Arts. 217 a 219 e 224-224 do Código dos Direitos de Autor e Direitos Conexos)
- Violação dos direitos exclusivos sobre topografias de produtos semicondutores (art. 318º do Código da Propriedade Industrial)
- Violação de correspondência ou telecomunicações (art. 194º do Código Penal)

b) infracções penais em que os meios de informação e as tecnologias de comunicação são utilizados para cometer uma infracção penal:

- Acesso indevido aos dados pessoais (art. 47º da Lei nº 58/2019)
- Utilização incompatível de dados pessoais com a finalidade de tratamento (Art. 46 da Lei n.º 58/2019)
- Apropriação indevida de dados pessoais (Art. 48º da Lei nº 58/2019)
- Violação ou destruição de dados pessoais (Art. 49 da Lei n.º 58/2009)
- Introdução de dados pessoais falsos (Art. 50 da Lei n.º 58/2009)
- Violação do segredo relacionado com dados pessoais (Art. 51 da Lei n.º 58/2009)
- Desobediência [à Comissão Nacional para a Protecção de Dados] (Art. 52 da Lei n.º 58/2009)
- Tratamento ilegal de dados pessoais sensíveis (artigo 193º do Código Penal)
- Violação agravada da privacidade (Artes. 191(1)(b) e 197(b) do Código Penal)
- Acesso indevido aos dados pessoais na justiça penal (art. 53º da Lei nº 59/2019)
- Apropriação indevida de dados pessoais na justiça penal (Art. 54º da Lei nº 59/2019)
- Utilização incompatível de dados pessoais com a finalidade de tratamento em justiça penal (Art. 55º da Lei nº 59/2019)
- Interligação ilegal de dados pessoais na justiça penal (art. 56º da Lei nº 59/2019)
- Desobediência qualificada [à Comissão Nacional de Protecção de Dados] na justiça penal (art. 57º da Lei nº 59/2019)
- Introdução de dados pessoais falsos na justiça penal (Art. 58º da Lei nº 59/2019)
- Vingança pornografia relacionada com violência doméstica (art. 152(2)(b) do Código Penal)
- Infracções relacionadas com a pornografia infantil (art. 176º do Código Penal)
- Solicitação de crianças para fins sexuais (Art. 176-A do Código Penal)
- Falsificação informática (Art. 3 da Lei sobre o Cibercrime)
- Contrafacção de cartões e outros meios de pagamento não monetários (Art. 3-A da Lei sobre o Cibercrime)
- Fraude informática [e telecomunicações] (art. 221º do Código Penal)
- Utilização de cartões falsificados e outros meios de pagamento não monetários (Art. 3-B da Lei de Crimes Cibernéticos)

- Aquisição de cartões falsificados e outros meios de pagamento não monetários (Art. 3-C da Lei de Crimes Cibernéticos)
- Utilização indevida de dispositivos relacionados com a falsificação de cartões e outros meios de pagamento não monetários (art. 3-D da Lei sobre o Cibercrime)
- Aquisição de cartões falsificados e outros meios de pagamento não monetários obtidos por crimes informáticos (art. 3-E da Lei de Crimes Cibernéticos)

Com ligações indirectas, estes delitos também podem ser mencionados:

- Assédio Sexual (Art. 170 do Código Penal)
- Insulto (Art. 181º do Código Penal)
- Difamação (Art. 180º do Código Penal)
- Violação da privacidade (art. 192º do Código Penal)
- Discriminação e incitação ao ódio e à violência (art. 240º do Código Penal)
- Contrafacção de obras protegidas por direitos de autor (art. 196º do Código dos Direitos de Autor e Direitos Conexos)
- Cópia, distribuição e venda de obras protegidas por direitos de autor (Art. 195 do Código dos Direitos de Autor e Direitos Conexos)

4. Manifestações de cibercriminalidade



O cibercrime manifesta-se normalmente através de ciberataques, mas os aspectos puramente não técnicos devem ser utilizados para levar a cabo com sucesso uma série de ataques.

Certas condutas ilegais no ciberespaço ou relacionadas com o cibercrime podem ser classificadas ao abrigo das disposições relevantes do actual Código Penal, mas existem certos tipos de conduta que podem ser significativamente mais complicados, ou mesmo impossíveis, de criminalizar (em muitos casos é bastante imoral).

Muito frequentemente o cibercrime é considerado um novo tipo de crime. No entanto, uma parte significativa dos crimes cibernéticos utiliza ou transfere tipos notórios de conduta ilegal (tais como fraude, violação de direitos de autor, roubo, intimidação, etc.) para o ambiente digital, onde podem ser cometidos "melhor, mais rápida e mais eficazmente" do que no mundo real. Entre os ataques puramente cibernéticos, poderiam ser incluídos, por exemplo, o hacking, ataques DoS e DDoS, botnets, etc.

É característico do mundo virtual que a maioria dos utilizadores tenha uma confiança incompreensível, quase ilimitada nele. Ao mesmo tempo, é preciso afirmar que o mundo virtual está a tornar-se cada vez mais importante para nós. Pessoalmente, sinto que ao utilizar os serviços prestados na Internet, muitas pessoas deixam de pensar em possíveis riscos ou ameaças. Estão principalmente cativadas pelas possibilidades aparentemente infinitas das "novas tecnologias"; de que outra forma é possível explicar a ausência de princípios e mecanismos básicos de defesa no mundo virtual, quando no mundo real nos comportaríamos de forma completamente diferente. Por vezes, o comportamento dos utilizadores no ciberespaço lembra-me o "Strange Case of Dr. Jekyll and Mr. Hyde" de Robert Louise Stevenson (1886). Pessoas aparentemente decentes no mundo real agem sem quaisquer restrições legais ou morais no ambiente "pseudo-anónimo" do ciberespaço. Assim, por exemplo, é possível encontrar um caso de um juiz que descarrega "pornografia infantil" [1], utilizadores que nunca roubaram nada no mundo real mas não têm qualquer problema em roubar no mundo virtual [2], ou violar outros direitos protegidos pela lei de um país.

Alguns dos principais peritos comentaram as previsões sobre o desenvolvimento da cibercriminalidade no passado, das quais gostaria de citar em particular Schneier, que previu em 2002 que a próxima grande tendência de segurança na Internet seria o crime. *"Não casos de vírus, Trojans e ataques DDoS por diversão ou a oportunidade de exibir as suas capacidades. Será um verdadeiro crime. Na Internet. Os criminosos tendem a ficar cinco ou dez anos atrasados em relação ao desenvolvimento tecnológico, mas acabam por realizar o seu potencial. Assim como Willie Sutton começou a roubar bancos "porque havia dinheiro", assim os criminosos modernos começarão a atacar através de redes informáticas. Cada vez mais valores (fundos) estão em linha do que em dinheiro real".* [3]

Em 2007, o FBI introduziu estatísticas que comparavam um "assalto a banco" comum com uma conduta que é um ataque de phishing. [4]

Parâmetro	Assalto à mão armada médio	Ciberataque médio
Risco	O infractor corre o risco de ser ferido ou morto.	Sem risco de danos físicos
Lucro	Em média, 3-5 mil dólares.	Em média, 50-500 mil dólares.
Probabilidade de apanhar	50-60% dos atacantes apanhados.	Cerca de 10% dos atacantes apanhados.
Probabilidade de condenação	95% dos atacantes apanhados foram condenados.	Dos atacantes apanhados, apenas 15% dos atacantes irão a julgamento e apenas 50% serão condenados.
Punição	Em média 5-6 anos, se o infractor não tiver ferido ninguém durante o roubo.	Em média 2-4 anos.

Em 2012, em relação às tecnologias de informação e comunicação, Goodman declarou que "a capacidade de um indivíduo influenciar as massas, devido a estas tecnologias, está a crescer exponencialmente. Está a crescer exponencialmente, tanto para bons como para maus fins". Ele apresenta claramente este crescimento no desenvolvimento do crime de roubo, para o qual uma faca ou pistola era originalmente suficiente no passado, e roubo significava essencialmente um acto entre indivíduos ou pequenos grupos. "Uma grande 'inovação' teve lugar na altura de um assalto a um comboio inteiro que transportava 200 pessoas". A Internet permite uma escala ainda maior de um ataque perpetrado por uma pessoa. O roubo de um grande número de utilizadores é claramente demonstrado pelo caso da Sony Playstation com aproximadamente 100 milhões de feridos. "Quando na história da humanidade poderia um indivíduo roubar 100 milhões de pessoas? Mas não se trata apenas de roubos..."[5].

No mesmo ano, Robert S. Mueller, Director do FBI, proferiu um discurso na RSA Cyber Security Conference (San Francisco, CA), onde declarou, entre outras coisas: "Creio que existem apenas dois tipos de empresas: as que foram invadidas e as que serão invadidas. E mesmo elas estão a convergir para uma categoria: as empresas que foram pirateadas e que serão pirateadas novamente".[6]

Actualmente, existe uma interconexão crescente e maciça de vários sistemas informáticos no ciberespaço, o que praticamente gera uma relação directa que consiste na seguinte afirmação "quanto mais dispositivos conectados, maior a sua vulnerabilidade e maior o número de ataques". Uma das representações gráficas dos ataques em curso pode ser encontrada em: <http://map.norsecorp.com/#/>; <https://cybermap.kaspersky.com/>; <https://map.lookingglasscyber.com/> etc.

Acreditamos que não há dúvida de que a cibercriminalidade está a aumentar, e é um problema global. Várias estatísticas mostram danos parcialmente diferentes causados pelo cibercrime, mas isto não altera o facto de que todos eles incluem danos primários (por exemplo, mau funcionamento de um sistema informático, suas partes, serviços oferecidos, falha de infra-estrutura, etc.) e danos secundários (por exemplo, recuperação de sistema, recuperação de dados, reconexão de utilizadores finais, etc.). A Europol informa no seu relatório de 2014[7] que o cibercrime custa à economia global cerca de 300 mil milhões de dólares por ano. A comunidade de atacantes mudou consideravelmente desde a expansão maciça da Internet. Em primeiro lugar, significa que já não existem indivíduos que tenham cometido delitos por diversão ou para contornar barreiras. Actualmente, estes são geralmente profissionais que fazem o seu trabalho para lucrar e estão frequentemente envolvidos em grupos organizados.

Esta mudança é compreensível e está indissociavelmente ligada a três aspectos:

- 1) **Dependência da sociedade na Internet** (ou serviços oferecidos, tecnologias, etc.),
- 2) **O cibercrime tornou-se um negócio global lucrativo** [os primeiros ataques cibernéticos já demonstraram o potencial de lucro, quer directamente (através de levantamento de fundos) ou indirectamente (por exemplo, pagando por danos ao serviço de outra pessoa)].
- 3) **Literacia mínima dos utilizadores** que utilizam tecnologias de informação e comunicação (o utilizador é um exemplo típico do elo mais fraco da cadeia).

Com o desenvolvimento de todos os tipos de serviços baseados no princípio "as-a-service"[8], surgiram várias plataformas (tipicamente subterrâneas, fóruns escuros) no ambiente do cibercrime, onde são oferecidos serviços que podem ser descritos **como crime como um serviço** (cibercrime- as-a-service). Assim, surge um "malware ou economia subterrânea" que fornece a quase todos os utilizadores os meios para cometer crimes cibernéticos. Os seguintes serviços são oferecidos como padrão dentro do serviço colectivamente referido como crime como um serviço:

- *Investigação como um serviço*, [9]
- *Crimeware-como-um-serviço*, [10].
- *Infra-estrutura como um serviço*, [11]
- *Hacking-as-a-service*, [12].
- *Dados como um serviço*, [13]
- *Spam como um serviço*, [14].
- *Ransomware-como-um-serviço*, etc.

A lista de serviços individuais não é exaustiva, e pode-se afirmar que o crime como serviço inclui a possibilidade de encomendar qualquer serviço ou mercadoria concebível que possa ser utilizada ou obtida no ciberespaço. O aumento destas actividades negativas está directamente ligado ao fenómeno da Internet das Coisas (IdC), que liga dispositivos (sistemas informáticos) com a Internet, representando assim outra ameaça significativa, que reside principalmente no desrespeito de um dos princípios básicos da segurança.

Muitos fabricantes ou distribuidores de sistemas informáticos que podem ser classificados como IdC não abordam a questão da segurança (o seu objectivo é trazer para o mercado e vender o maior número possível de dispositivos que possam ser descritos como um sistema informático), que os atacantes utilizam.

Os custos associados à evolução da segurança são geralmente a parte mais dispendiosa do desenvolvimento, mas esta é uma área que precisa de ser abordada tendo em conta as ameaças já conhecidas. Estes incluem, por exemplo: um canal de comunicação não seguro de um pacemaker[15]; um carro ou avião telecomandado[16]; um lar inteligente ou os seus componentes (frigorífico, caldeira, sistema de segurança, televisão, etc.), que pode ser controlado remotamente[17], etc.

"Como vai ser o mundo quando já estivermos a utilizar 6,4 mil milhões de dispositivos IoT **este ano**? Durante os próximos quatro anos, deverão ser 20,8 mil milhões de dispositivos. Além disso, muitos destes dispositivos terão uma duração de vida significativamente mais longa do que o ciclo de vida normal dos telemóveis, comprimidos, ou computadores portáteis. Como poderá um fabricante de automóveis proteger a segurança do modelo 2020 dez anos mais tarde? Ou um frigorífico que possa ficar em sua casa durante quinze anos ou mais? Quanto tempo demorou a Microsoft a aprender a actualizar o seu próprio sistema operativo"?[18]

Schneier afirma que quando se trata de dados, os atacantes podem fazer essencialmente três coisas básicas com eles: roubá-los (violando o princípio da **Confidencialidade**), alterá-los (violando o princípio da **Integridade**) ou impedir os proprietários de aceder a eles (violando o princípio da **Disponibilidade**). Schneier afirma que, com o advento da IOT, os dois últimos tipos de ataques tornar-se-ão extremamente eficazes. [19]

Na secção seguinte, irei introduzir alguns dos ataques que ocorrem no ambiente do ciberespaço. Não é possível definir todos os ataques, quer devido ao âmbito desta publicação, quer devido à impossibilidade de descrever todos os possíveis actos alternativos subsuficientes sob o termo cibercrime. Se possível, a qualificação penal específica de tal conduta será declarada para uma manifestação específica de cibercriminalidade.

2.

[1] Juiz, 69 anos, que descarregou pornografia infantil enfrentando 'humilhação catastrófica': [em linha]. [cit.1.9.2009]. Disponível a partir de: <http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo>

[2] HILL, Caxemira. *Estes dois jogadores de Diablo III roubaram armadura virtual e ouro - e foram processados pela IRL*. [online]. [cit.10.8.2015]. Disponível a partir de:

<http://fusion.net/story/137157/two-diablo-iii-players-now-have-criminal-records-for-stealing-virtual-items-from-other-players/>

[3] Para mais detalhes ver SCHNEIER, Bruce. *Crime: A Próxima Grande Coisa da Internet*. [online]. [cit.6.11.2007]. Disponível em: <https://www.schneier.com/crypto-gram/archives/2002/1215.html>

[4] JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praga: Grada, 2007, p. 30

[5] Para mais detalhes ver GOODMAN, Marc. *Uma visão dos crimes no futuro*. [em linha]. [cit.13.11.2014]. Disponível a partir de: https://www.ted.com/talks/marc_goodman_a_vision_of_crimes_in_the_future#t-456071

[6] MUELLER, Robert. [em linha]. [cit.3.4.2013]. Disponível a partir de:

<https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies>

[7] Ver *The Internet Organised Crime Threat Assessment (IOCTA) 2014*. [em linha]. [cit.10.8.2015]. Disponível em: <https://www.europol.europa.eu/content/internet-organised-crime-threat-assesment-iocta>

[8] É a prestação de serviços tipicamente associada a uma solução de nuvem. Exemplos são: infra-estrutura como serviço; plataforma como serviço; serviço como serviço; segurança como serviço, etc.

[9] Sob este serviço, é possível imaginar actividades que consistem na detecção de várias vulnerabilidades, ainda desconhecidas, do sistema informático ou software alvo. (Estas vulnerabilidades são conhecidas como vulnerabilidades de dia-zero).

A actividade real no âmbito da investigação como serviço não tem necessariamente de ser, na sua natureza, um acto criminoso ou ilegal. A detecção de vulnerabilidades e erros é realizada por vários peritos em segurança informática (por exemplo, testes de penetração, etc.). Normalmente, estes serviços são prestados com base nos termos contratuais entre o testador e o testador ou utilizando algumas das circunstâncias que impedem a ilegalidade.

[10] O crimeware-as-a-service oferece uma vasta gama de actividades desde a simples venda de malware, passando pela sua "personalização", bem como a entrega de exploits (vulnerabilidades), etc.

[11] A infra-estrutura como um serviço oferece então a oferta de sistemas informáticos físicos ou virtuais (botnets, serviços de alojamento, arrendamentos de rede, etc.).

[12] Este serviço pode incluir uma simples quebra de dados de acesso a e-mail, conta de rede social, etc., até ataques profissionais e sofisticados a uma vítima seleccionada. Esta área pode então incluir, por exemplo, a execução de ataques DoS e DDoS.

[13] Os dados como serviço oferecem a mercadoria mais procurada, que são os dados. Especificamente, estes são, por exemplo: dados de acesso (nome e senha) a várias contas, cartões de crédito, contas bancárias, cartões de crédito roubados, mas também informações sobre pessoas (residência, data de nascimento, números de telefone, e-mails, etc.).

[14] O nome implica que é possível encomendar e pagar por uma campanha de spam.

[15] Cf. TAYLOR, Harriet. *Como a "Internet das Coisas" pode ser fatal*. [em linha]. [cit.17.6.2016]. Disponível em: <http://www.cnn.com/2016/03/04/how-the-internet-of-things-could-be-fatal.html>

[16] Para mais detalhes ver REENBERG, Andy. *Os hackers matam remotamente um jipe na auto-estrada - comigo dentro dela*. [em linha]. [cit.4.5.2016]. Disponível a partir de: <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>

Na versão checka disponível, por exemplo, a partir de: http://auto.idnes.cz/hackeri-unesli-jeep-dalkove-ovladani-auta-f1l-/automoto.aspx?c=A150723_135910_automoto_fdv

Para mais detalhes ver ZETTER, Kim. *É Possível para Passageiros Hackear Aeronaves Comerciais?* [online]. [cit.5.5.2016]. Disponível em: <https://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/>

[17] É assim possível, por exemplo, contornar a segurança doméstica; aumentar a temperatura com o termostato controlado à distância e causar danos a outra pessoa; encomendar uma quantidade insignificante de alimentos através de um frigorífico "inteligente", etc.

[18] DOČEKAL, Daniel. Bruce Schneier: *Internet věcí přinese útoky, které si neumíme představit*. [online]. [cit.10.8.2016]. Disponível a partir de: <http://www.lupa.cz/clanky/bruce-schneier-internet-veci-prinese-utoky-ktere-si-neumime-predstavit/>

[19] SCHNEIER, Bruce. *A Internet das Coisas Transformará os Hacks de Grande Escala em Catástrofes do Mundo Real*. [online]. [cit.10.8.2016]. Disponível em: <https://motherboard.vice.com/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster>

4.1. Engenharia Social

A engenharia social não pode ser considerada directamente aplicável a um ataque cibernético, mas é um pré-requisito para que uma série de ataques cibernéticos sejam bem sucedidos.

Se quiséssemos definir o conceito de engenharia social, poder-se-ia dizer que se trata de influenciar, persuadir ou manipular as pessoas a fim de as obrigar a tomar uma determinada acção ou a obter delas informações que de outra forma não forneceriam. O objectivo é dar a uma vítima uma tal impressão de que a situação em que se encontra é diferente da que realmente é. Em termos mais simples, é a "arte do engano", com Mitnick a distinguir duas especializações na profissão de artista-manipulador. *"Aquele que ganha dinheiro com as pessoas é um vulgar burlão, enquanto aquele que usa manipulação e persuasão contra empresas - geralmente com a intenção de obter informações - é um engenheiro social".* [1].

Estou convencido de que esta reivindicação de Mitnick de 2003 não se manteria no mundo digital de hoje, pois muitos atacantes utilizam técnicas de engenharia social para obter informações ou dados e utilizá-los, por exemplo, no crime como um serviço. Além disso, estas técnicas são utilizadas não só para empresas mas também para indivíduos. Um ataque real não tem de assumir a forma de fraude, mas subsequentemente esta informação pode ser vendida ou mal utilizada para um ataque mais grave.

A ideia principal da engenharia social não é utilizar várias abordagens ou ferramentas puramente técnicas, por exemplo para quebrar uma palavra-passe, quando é muito mais fácil enganar uma vítima, que pode revelar voluntariamente a palavra-passe. O elo mais fraco do sistema de segurança é e será sempre uma pessoa (o utilizador). Uma vez que não pode haver um sistema informático no mundo que não dependa de seres humanos, pelo menos em algum momento (quer se trate da operação, configuração ou manutenção de um sistema informático), a forma mais fácil é obter a informação necessária das pessoas.

É a simplicidade de um ataque dirigido ao elo mais fraco de todo o sistema que normalmente o torna a forma mais eficaz. A engenharia social surgiu com o caso de Mitnick [2], que é considerado por muitos como sendo um hacker, mas que na realidade se considera a si próprio como um engenheiro social. Nos seus livros [3], Mitnick mostra como é fácil obter informação sensível e que representa um risco de segurança para indivíduos e organizações. Numa audiência perante a Comissão de Assuntos Governamentais do Senado dos EUA [4], na qual Mitnick testemunhou sobre a obtenção de senhas e informações sensíveis sobre os sistemas informáticos das empresas em que invadiu, Mitnick disse: *"Apresentei-me como outra pessoa e simplesmente perguntei por elas"*.

Para a engenharia social, um dos factores-chave é obter o máximo de informação possível sobre o alvo do ataque (seja um sistema informático, uma entidade jurídica ou uma pessoa singular). Existe frequentemente um efeito a longo prazo sobre uma pessoa chave e a construção de "confiança" entre um agressor e uma vítima antes de um ataque, enquanto o agressor tipicamente explora o descuido humano, confiança, vontade de ajudar os outros, preguiça, fraqueza, medo (por exemplo, para que a pessoa não se meta em problemas), irresponsabilidade, estupidez, etc.

As características humanas acima referidas ajudam muito um atacante a levar a cabo o seu ataque. Pergunte a si mesmo quanto verifica a sua contraparte, por exemplo, ao fazer uma chamada telefónica ou ao comunicar via TIC? Quanto verifica os meios de armazenamento (discos USB, cartões de memória, etc.) que recebeu como presente para o evento de apresentação?

Especialmente no campo das TIC, é possível observar ataques cada vez mais sofisticados e elaborados [por exemplo, e-mails fraudulentos bem preparados, instituições reais (utilizadas como um alegado remetente), redireccionamento para sites fraudulentos ou instalação de malware contido num documento anexo ou num meio de armazenamento, etc.].

Os ataques de engenharia social são geralmente conduzidos de três maneiras, e estes métodos são combinados uns com os outros:

1. **Recolha de dados livremente** (publicamente) **disponíveis** sobre um alvo de um ataque
2. **Ataque físico** (por exemplo, um atacante finge ser um empregado de uma agência de serviços - como um serviço de impressão, um trabalhador de manutenção, etc.), em que o atacante tenta obter tanta informação "de dentro" da empresa, ou informação sensível sobre empregados individuais (incluindo, por exemplo, procura de lixo, etc.)

3. Ataque psicológico

Os métodos mais comuns de ataques de engenharia social incluem:

1. **E-mail fraudulento** ou **site falso**
2. **Chamada telefónica**
3. **"Ataque "cara a cara"**
4. **Mergulho em contentores de lixo**, bem como "esforço de dados".
5. **Pesquisa de websites, redes sociais, etc.** (Esta é uma fonte aberta de dados de fácil acesso para atacantes de engenharia social, que ajuda a identificar ou verificar informações sobre um alvo potencial). **Informação pública disponível em linha** (por exemplo, CVs, teses, artigos, propostas, etc., publicados na Internet). **Relatórios anuais e outras informações publicamente disponíveis sobre uma empresa**
6. **Entrega de publicidade ou outros materiais em CD, DVD ou outros suportes de armazenamento**
7. **Deixar um meio de armazenamento** (USB, etc.) **numa área de interesse** (como empresa, casa do empregado, etc., tal meio contém normalmente malware)
8. **Oferta para experimentar um serviço online** (por exemplo, oferta de um armazenamento em nuvem, ou um serviço interessante gratuitamente, etc.)

9. Entrega ou descoberta de equipamento (sistema informático)

10. Técnico de serviço falso

11. Outros

Quanto a alvos de ataques de engenharia social dentro de uma organização, os possíveis alvos podem ser, por exemplo:

- posição de gestão,
- Departamento de TI,
- trabalhadores do helpdesk,
- recepcionistas (secretárias),
- pessoal de segurança,
- gestão de edifícios,
- limpeza, etc.

Um engenheiro social é capaz devido à sua capacidade de manipular pessoas; contudo, a simples manipulação não é suficiente em alguns casos e é necessário ligar esta informação aos conhecimentos técnicos no campo das TIC.

No final deste capítulo, dou um exemplo em que Mitnick demonstra a ligação entre as técnicas sociais e o conhecimento das TIC:[5]

Um jovem atacante a quem vou telefonar Ivan Peters preparou-se para recuperar o código fonte para um novo jogo electrónico. Ele não teve problemas em entrar na rede de área ampla da empresa porque um amigo hacker seu já tinha comprometido um dos servidores web da empresa. Depois de encontrar uma vulnerabilidade não corrigida no software do servidor web, o seu amigo tinha quase caído da cadeira. Quando se apercebeu que o sistema tinha sido configurado como um host *dual-homed*, o que significava que ele tinha um ponto de entrada na rede interna.

Mas uma vez que Ivan estava ligado, enfrentou então um desafio que era como estar dentro do Louvre e na esperança de encontrar a Mona Lisa. Sem uma planta do chão, podia vaguear durante semanas. A empresa era global, com centenas de escritórios e milhares de servidores informáticos, e não forneciam exactamente um índice de sistemas de desenvolvimento ou os serviços de um guia turístico para o guiar para o caminho certo. Em vez de utilizar uma abordagem técnica para descobrir qual o servidor de que precisava para atingir, Ivan utilizou uma abordagem de engenharia social. Fez chamadas telefónicas com base em métodos semelhantes aos descritos em outras partes deste livro. Na primeira chamada de apoio técnico informático, alegou ser um funcionário da empresa com um problema de interface num produto que o seu grupo estava a conceber. e pediu o número de telefone do líder do projecto para a equipa de desenvolvimento de jogos. Depois ligou para o nome que lhe tinha sido dado, fazendo-se passar por um tipo das TI. *"Mais tarde esta noite"*, disse ele, *"estamos a trocar um router e precisamos de garantir que as pessoas da sua equipa não percam a conectividade com o seu servidor"*. *Portanto, precisamos de saber quais os servidores que a sua equipa utiliza"*. A rede estava a ser actualizada a toda a hora. E dar o nome do servidor não prejudicaria nada de qualquer forma, pois não? Uma vez que estava protegido por palavra-passe, ter apenas o nome não podia ajudar ninguém a entrar. Então, o tipo deu ao atacante o nome do servidor. Nem sequer se deu ao trabalho de ligar ao homem para verificar a sua história ou escrever o seu nome e número de telefone. Ele apenas deu o nome dos servidores, ATM5 e ATM6.

Nesta altura, Ivan mudou para uma abordagem técnica para obter a informação de autenticação. O primeiro passo com a maioria dos ataques técnicos aos sistemas que fornecem capacidade de acesso remoto é identificar uma conta com uma senha fraca, que fornece um ponto de entrada inicial no sistema. Quando um atacante tenta utilizar ferramentas de hacking para identificar senhas remotamente, o esforço pode obrigá-lo a permanecer ligado à rede da empresa durante horas de cada vez.

Claramente, ele faz isto por sua conta e risco: quanto mais tempo permanece ligado, maior é o risco de ser detectado e apanhado. Como passo preliminar, Ivan faria uma enumeração, que revela detalhes sobre um sistema alvo. Mais uma vez, a Internet fornece convenientemente software para o efeito (<http://mtslenth.0catch.com>). Ivan encontrou várias ferramentas de hacking disponíveis publicamente na web que automatizaram o processo de enumeração, evitando a necessidade de o fazer à mão, o que levaria mais tempo e, assim, correria um risco maior. Sabendo que a organização implantou principalmente servidores baseados em Windows, descarregou uma cópia do NBTEnum, um utilitário de enumeração NetBIOS (sistema básico de entrada/saída)[6]. Introduziu o endereço IP (protocolo Internet) do servidor ATM5 e começou a executar o programa. A ferramenta de enumeração foi capaz de identificar várias contas que existiam no servidor.

Uma vez identificadas as contas existentes, a mesma ferramenta de enumeração tinha a capacidade de lançar um ataque de dicionário contra o sistema informático. Um ataque de dicionário é algo com que muitas pessoas e intrusos da segurança informática estão intimamente familiarizados, mas que a maioria das outras pessoas ficarão provavelmente chocadas por aprender é possível. Tal ataque visa descobrir a palavra-chave de cada utilizador no sistema através da utilização de palavras comumente utilizadas. Somos todos preguiçosos com algumas coisas, mas nunca deixa de me surpreender que quando as pessoas escolhem as suas palavras-passe, a sua criatividade e imaginação pareçam desaparecer. A maioria de nós quer uma palavra-passe que nos dê protecção mas que seja ao mesmo tempo fácil de lembrar, o que normalmente significa algo intimamente ligado a nós. As nossas iniciais, nome do meio, alcunha, nome do cônjuge, canção favorita, filme, ou cerveja, por exemplo. O nome da rua onde vivemos ou da cidade onde vivemos, o tipo de carro que conduzimos, a aldeia à beira-mar onde gostamos de ficar no Havai, ou aquele riacho favorito com a melhor pesca de trutas à nossa volta. Reconhece o padrão aqui? Estes são sobretudo nomes pessoais, nomes de lugares, ou palavras de dicionário. Um ataque de dicionário percorre palavras comuns a um ritmo muito rápido, tentando cada uma delas como senha em uma ou mais contas de utilizador.

Ivan dirigiu o ataque do dicionário em três fases. Na primeira, ele utilizou uma lista simples de cerca de 800 das palavras-passe mais comuns. A lista inclui *segredo*, *trabalho* e *palavra-passe*. Além disso, o programa permutou as palavras do dicionário para tentar cada palavra com um dígito anexo, ou anexando o número do mês corrente. O programa experimentou cada tentativa contra todas as contas de utilizador que tinham sido identificadas. Sem sorte. Para a tentativa seguinte, Ivan foi ao motor de busca do Google e escreveu "*dicionários de listas de palavras-chave*" e encontrou milhares de sites com extensas listas de palavras-chave e dicionários para inglês e várias línguas estrangeiras. Descarregou um dicionário electrónico inteiro de inglês. Depois melhorou-o descarregando uma série de listas de palavras que encontrou no Google. Ivan escolheu o site em www.outpost9.com/files/Wordlists.html. Este site permitiu-lhe descarregar (tudo isto gratuitamente) uma selecção de ficheiros incluindo nomes de família, nomes próprios, nomes e palavras do congresso, nomes de actores, e palavras e nomes da Bíblia. Outro dos muitos sítios que oferecem listas de palavras é na realidade fornecido através da Universidade de Oxford, em <ftp://ftp.ox.ac.uk/pub/wordlists>. Outros sites oferecem listas com nomes de personagens de desenhos animados, palavras usadas em Shakespeare, na Odisseia, Tolkien, e na série Star Trek, bem como na ciência e religião, e em

todo o lado. (Uma empresa on-line vende uma lista contendo 4,4 milhões de palavras e nomes por apenas 20 dólares). O programa de ataque pode ser definido para testar os anagramas das palavras do dicionário, bem como - outro método favorito que muitos utilizadores de computador pensam que aumenta a sua segurança.

Depois de Ivan ter decidido qual a lista de palavras a utilizar, e ter iniciado o ataque, o software funcionou em piloto automático. Ele foi capaz de voltar a sua atenção para outras coisas. E aqui está a parte incrível: Pensar-se-ia que um tal ataque permitiria ao hacker fazer uma soneca de Rip van Winkle e o software ainda teria feito poucos progressos quando ele acordasse. De facto, dependendo da plataforma a ser atacada, da configuração de segurança do sistema, e da conectividade de rede, o vocabulário inglês completo pode, incrivelmente, ser experimentado em menos de trinta minutos! Enquanto este ataque estava a decorrer, Ivan iniciou outro computador a executar um ataque semelhante no outro servidor utilizado pelo grupo de desenvolvimento, ATM6. Vinte minutos mais tarde, o software de ataque tinha feito o que a maioria dos utilizadores insuspeitos gostava de pensar ser impossível: Tinha quebrado uma senha, revelando que um dos utilizadores tinha escolhido a senha "*Frodo*", um dos Hobbits do livro O Senhor dos Anéis. Com esta palavra-chave em mãos, Ivan conseguiu ligar-se ao servidor ATM6 utilizando a conta do utilizador. Havia boas e más notícias para o nosso atacante. A boa notícia era que a conta que ele decifrou tinha privilégios de administrador, que seriam essenciais para o passo seguinte. A má notícia era que o código fonte do jogo não se encontrava em lado nenhum. Deve ser, afinal, na outra máquina, a ATM5, que ele já sabia que era resistente a um ataque de dicionário. Mas Ivan ainda não estava a desistir; ele ainda tinha mais alguns truques na manga. Em alguns sistemas operativos Windows e UNIX, os hashes de palavras-passe (palavras-passe encriptadas) estão abertamente disponíveis a qualquer pessoa que tenha acesso ao computador em que estão armazenados. O raciocínio é que as palavras-passe encriptadas não podem ser quebradas e, portanto, não precisam de ser protegidas. A teoria está errada. Utilizando outra ferramenta chamada *pwdump3*, também disponível na Internet, foi capaz de extrair os hashes das senhas da máquina ATM6 e descarregá-las. Um ficheiro típico de hashes de palavra-passe tem este aspecto:

```
Administrador:
500:95E4321A38AD8D6AB75E0C8D76954A50:
2E48927AQB04F3BFB341E266D6L
akaspe:1110:5A8D7E9E3C3954F642C5C736306CBFEF:393CE7F90A8357F157873D72D
digger:1111:5D15C0D58D0216C525AD3B83FA6627C7:17AD564144308B42B8403D01AE256
555
ellgan:1112:2017DA45D801383EFF17365FAF1FFE89:07AEC950C22CB89C2C734EB89j1
tafeeck:1115:9F5890B3FECCAB7EAAD3B435B51404EE:1F0115A728447212FC05E1D208203
35
vkantar:1116:81A6A5D035596E7DAAD3B435B51404EE:B933D36DD12258946FCC7BD153F1
CD6
vwallwick:1119:25904EC665BA30F44494F42E1054F192:15B2B7953FB632907455D2706A432
mmcdonald: 1121:
A4AED098D29A3217AAD3B435B51404EE:40670F936B79C2ED522F5ECA939c
kworkman:1141:C5C598AF45768635AAD3B435B51404EE:DEC8E827A121273EF084CDBF5F
D192
```

Com os hashes agora descarregados para o seu computador, Ivan utilizou outra ferramenta que executava um sabor diferente de ataque por senha conhecida como *força bruta*.^[2] Este tipo de ataque tenta todas as combinações de caracteres alfanuméricos e a maioria dos símbolos especiais.

Ivan utilizou um utilitário de software chamado *L0phtcrack3* (pronuncia-se loft-crack; disponível em www.atstake.com; outra fonte para algumas excelentes ferramentas de recuperação de senhas é www.elcomsoft.com). Os administradores de sistemas utilizam o L0pht-crack3 para auditar senhas "*fracas*"; os atacantes utilizam-no para decifrar senhas. A característica de força bruta em LC3 tenta senhas com combinações de letras, números, e a maioria dos símbolos incluindo @#%\$%^&. Tenta sistematicamente todas as combinações possíveis da maioria dos caracteres. (Note-se, contudo, que se forem utilizados caracteres não imprimíveis, LC3 será incapaz de descobrir a palavra-passe). O programa tem uma velocidade quase inacreditável, que pode chegar aos 2,8 milhões de tentativas por segundo numa máquina com um processador de 1 GHz. Mesmo com esta velocidade, e se o administrador do sistema tiver configurado correctamente o sistema operativo Windows (desactivando o uso de hashes LANMAN), quebrar uma palavra-passe pode ainda levar um tempo excessivo. Por essa razão, o atacante descarrega frequentemente os hashes e executa o ataque na sua ou noutra máquina, em vez de ficar online na rede da empresa alvo e arriscar-se a ser detectado. Para Ivan, a espera não foi assim tão longa.

Várias horas depois, o programa apresentou-lhe palavras-passe para cada um dos membros da equipa de desenvolvimento. Mas estas eram as senhas para os utilizadores da máquina ATM6, e ele já sabia que o código fonte do jogo que procurava não estava neste servidor. E agora? Ele ainda não tinha conseguido obter uma palavra-passe para uma conta na máquina ATM5. Usando a sua mentalidade de hacker e compreendendo os maus hábitos de segurança dos utilizadores típicos, ele pensou que um dos membros da equipa poderia ter escolhido a mesma palavra-passe para ambas as máquinas. Na verdade, foi exactamente isso que ele encontrou. Um dos membros da equipa estava a utilizar a palavra-passe "*gamers*" tanto no ATM5 como no ATM6. A porta tinha-se aberto de par em par para Ivan caçar até que ele encontrou os programas que procurava.

Assim que localizou a árvore de código fonte e a descarregou alegremente, deu mais um passo típico dos crackers do sistema: Ele alterou a palavra-passe de uma conta inactiva que tinha direitos de administrador, para o caso de querer obter uma versão actualizada do software em algum momento no futuro.

Para reduzir os riscos colocados pela engenharia social, é necessário aumentar a consciência de possíveis ameaças não só dentro da organização, mas na sociedade como um todo. Como mencionei anteriormente, a engenharia social ajuda a realizar um ataque, e cabe inteiramente ao agressor determinar quem será o seu alvo. É muito mais fácil para um agressor concentrar o seu ataque nas massas de pessoas inexperientes e ignorantes do que numa empresa relativamente bem protegida.

[1] MITNICK, Kevin D. e William L. SIMON. *A Arte da Enganação (Uměniklamu)*. Gliwice: Helion, 2003. ISBN 83-7361-210-6. p. 6

[2] Para mais detalhes, ver, por exemplo, *Kevin Mitnick Case: 1999*. [online]. [cit.2.11.2011]. Disponível a partir de: <http://www.encyclopedia.com/doc/1G2-3498200381.html>

[3] Para mais pormenores, ver:

MITNICK, Kevin D. e William L., SIMON. *A Arte da Enganação (Uměnilamu)*. Gliwice: Helion, 2003. ISBN 83-7361-210-6.

MITNICK, Kevin D. *A arte da intrusão: as histórias reais por detrás das explorações de hackers, intrusos e enganadores*. Indianápolis: Wiley, 2006. ISBN 0-471-78266-1.

MITNICK, Kevin D. e William L., SIMON. *Ghost in the Wires: as minhas aventuras como o hacker mais procurado do mundo*. Nova Iorque: Little, Brown & Co, 2012. ISBN 9780316037723.

[4] *O testemunho de um ex-hacker*. [em linha]. [cit.26.9.2008]. Disponível em:
<http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html>

[5] O exemplo é literalmente citado de: MITNICK, Kevin D. e William L. SIMON. *A Arte da Enganação (Uměnilamu)*. Gliwice: Helion, 2003. ISBN 83-7361-210-6, pp. 127-130

[6] **Enumeração** - um processo que revela o serviço activado no sistema alvo, a plataforma do sistema operacional, e uma lista de nomes de contas dos utilizadores que têm acesso ao sistema.

[7] **Ataque por força bruta** - uma estratégia de detecção de senhas que consiste em testar todas as combinações possíveis de caracteres alfanuméricos e especiais.

4.2. Botnet

Botnet pode ser simplesmente definida como uma rede de bots ligados por software^[1] que executam uma acção baseada num comando do "proprietário" (ou administrador) dessa rede. A rede construída desta forma pode ser utilizada para actividades legais (por exemplo, computação distribuída) ou para actividades ilegais (ver abaixo).

Foram os cálculos distribuídos que, de facto, inadvertidamente deram aos criminosos a ideia de construir botnets da forma como são entendidos hoje em dia. O texto seguinte é de um website sobre computação distribuída: **"A maioria dos computadores no mundo utiliza todo o seu potencial informático apenas durante uma parte muito pequena do seu tempo de funcionamento, mas o seu consumo de electricidade é apenas ligeiramente inferior ao que seria se fossem totalmente utilizados. É uma pena não utilizar este computador de lounging, e muito poucas pessoas se apercebem da quantidade de energia não utilizada que existe no mundo... Na computação distribuída, o ditado "Não há necessidade de um duche, algumas gotas também ajudam" aplica-se na totalidade, e gotas de milhões de computadores comuns no mundo excedem várias vezes o desempenho mesmo dos maiores supercomputadores do mundo... O envolvimento em qualquer projecto de computação distribuída consiste apenas na instalação do cliente, e este pode normalmente realizar todas as actividades necessárias e cuidar de aplicações específicas... A maioria dos projectos funciona de modo a que o trabalho total seja dividido em muitas partes e estas são depois enviadas para computadores individuais, que as solicitam. Depois de processar cada peça, os próprios computadores individuais enviam os dados resultantes de volta ao centro do projecto, onde os resultados são novamente combinados numa única unidade".**^[2]

A própria ideia de distribuição de recursos, ou a utilização de baixo poder computacional de outros sistemas informáticos, por exemplo para calcular algoritmos matemáticos complexos, etc., não é definitivamente má e é muito mais eficiente do que a utilização e construção de "supercomputadores". Contudo, como seres humanos somos muito inventivos, era óbvio que esta ideia seria utilizada para outros fins que não o altruísmo ou a caridade. A capacidade de distribuir diferentes tarefas entre diferentes computadores geograficamente localizados tem sido e é atractiva para os atacantes.

O actual sistema informático, por exemplo, sob a forma de servidor de correio, não tem qualquer problema em enviar dezenas de milhões ou biliões de mensagens de correio electrónico por dia. Se um utilizador decidir utilizar este sistema, por exemplo, para espalhar spam, este sistema informático (rastreador por identificadores como o endereço IP) realizará esta actividade apenas por um período muito curto, uma vez que será bloqueado muito em breve pelo ISP (por exemplo, devido a tráfego ilegítimo ou excessivo na rede, que pode ser marcado como spam); o seu endereço aparecerá nas "listas negras", e com base nesta informação o tráfego será bloqueado (por exemplo, correio de saída). No entanto, se um atacante usar energia distribuída sob a forma de uma botnet, terá milhares a centenas de milhares de computadores, cada um dos quais envia uma parte das mensagens (por exemplo, 1000-2000 mensagens por dia). Tal tráfego não será então considerado problemático e não será interrompido.

É típico para uma **botnet** que se **um sistema informático alvo for infectado, este sistema**, chamado "zombie" ou "bot", **liga-se a um servidor de controlo central** [chamado servidor de comando e controlo (C&C)]. **Todo o sistema** (contendo zombies e C&C) **é controlado por um atacante** (referido como botmaster ou botherder) **que controla os bots através de um servidor C&C.**^[3]

Os seguintes elementos são característicos (necessários) para o botnet:

1. Infra-estrutura de comando e controlo (C&C)

É uma infra-estrutura que consiste num elemento (ou elementos) de controlo e robots (controlados por sistemas informáticos).

2. Instalação e controlo de um bot

Trata-se na maioria das vezes de malware que é espalhado através de uma botnet ou de outra forma. O principal objectivo de tal malware é integrar outros sistemas informáticos numa botnet. O malware explora várias vulnerabilidades em sistemas informáticos.

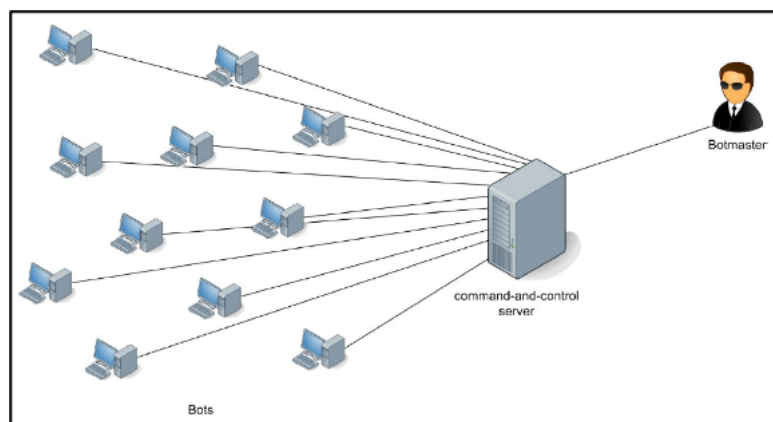
3. Controlo de robots através de infra-estruturas C&C

Um bot é um software que funciona secretamente e utiliza canais de comunicação comuns (IRC, IM, RFC 1459, etc.) para comunicar com um servidor C&C. Os novos bots tentam obter o máximo de informação possível do seu ambiente e promover-se a outros sistemas informáticos.

Com base na arquitectura, existem botnets com:

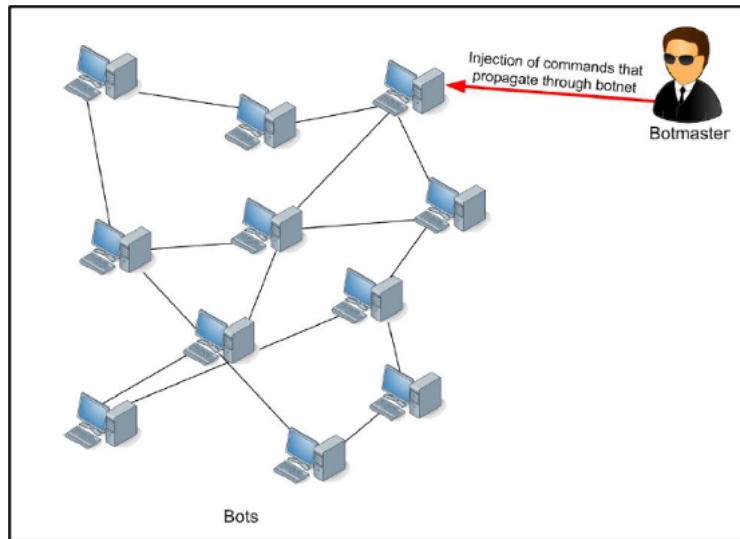
1. Arquitectura centralizada

Esta arquitectura é tipicamente construída sobre o princípio da comunicação cliente-servidor. Os sistemas informáticos finais (zombies/bots) comunicam directamente com o servidor C&C (elemento de controlo central) e seguem instruções e utilizam recursos deste servidor.

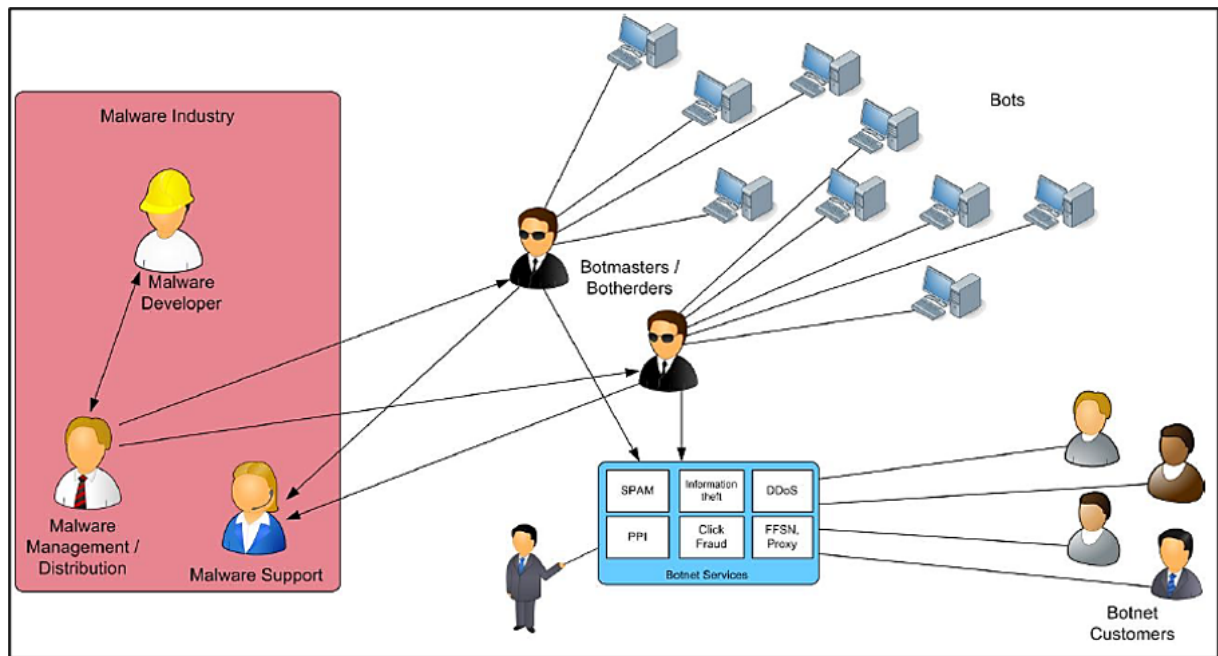


2. Arquitectura descentralizada

É tipicamente construído em arquitectura peer-to-peer (P2P). Esta arquitectura permite a partilha de recursos e comandos dentro de uma rede P2P. Não existe um elemento de controlo central na forma "clássica", o que torna este sistema mais resistente à tentativa de assumir o controlo através deste elemento de controlo.



As botnets podem ser utilizadas para muitas actividades, mas os ganhos financeiros estão principalmente em primeiro plano, o que consiste em gerar os seus próprios ataques (por exemplo, resgates, phishing, spam, roubo de informação, DDoS, etc.), bem como alugar os seus serviços ou toda a botnet aos clientes. Graças ao acima exposto, é possível incluir a botnet na estrutura do **crime como serviço** (onde o serviço é oferecido: **botnet-as-a-service**), ou na economia do malware[6], onde representa a plataforma técnica básica necessária para realizar uma série de ciberataques.



Economia malware

O sistema informático que se torna parte da botnet é então tipicamente utilizado para uma das actividades descritas na tabela seguinte. É de notar que estes ataques são normalmente combinados ou distribuídos dentro da rede de bots no que respeita à sua ocupação, procura por parte dos "clientes", etc.

Envio de	Roubo de Identidade	Ataques DoS	Clique Fraude
----------	---------------------	-------------	---------------

- spam - phishing - malware - adware - spyware	Os dados e informações pessoais e sensíveis são obtidos e enviados (de volta ao agressor). - Dados de acesso à conta Dados de acesso a e-mails, redes sociais, etc. - outros dados ou informações que possam ser utilizados ou vendidos pelo agressor	Lançamento de um ataque DoS contra um alvo (sistema informático) especificado pelo botmaster.	O sistema informático exibe (ou clica em) links publicitários no site sem o conhecimento do utilizador. Isto dá a impressão de que o site tem tráfego e os anunciantes estão a perder dinheiro. [7] .
--	--	---	---

No quadro abaixo resumo uma lista de algumas redes de botnets conhecidas[\[8\]](#) :

Data de criação	Data final	Nome	Número estimado de bots	Número de spam em milhares de milhões por dia	Alias (também conhecido por)	Mais informações
2002						
	2011	Coreflood	2,300,000			Porta traseira. Recolha de informações pessoais e sensíveis.
2004						
		Bagle	230,000 ^[16]	5.7	Beagle, Mitglieder, Lodeight	Envio maciço de spam. Concebido para sistemas informáticos com sistema operativo Windows.
		Marina Botnet	6,215,000 ^[16]	92	DamonBriant, BOB.dc, Cotmonger, Hacktool.Spammer, Kraken	
		Torpig	180,000 ^[17]		Sinowal, Anserin	Distribuição de malware e recolha de dados sensíveis e pessoais. Concebido para sistemas informáticos com sistema operativo Windows.
		Tempestade	160,000 ^[18]	3	Nuwar, Peacomm, Zhelatin	Envio de spam. Concebido para sistemas informáticos com sistema operativo Windows.
2006						
	Março de 2011	Rustock	150,000 ^[19]	30	RKRustok, Costrat	Envio de spam. Capaz de enviar até 25.000 mensagens de spam por hora a partir de um computador. Activo no sistema operativo Windows.
		Donbot	125,000 ^[20]	0.8	Buzus, Bachsoy	Envio principalmente de spam farmacêutico.
2007						

		Cutwail	1,500,000 ^[21]	74	Pandex, Mutant (relacionado com: Wigon, Pushdo)	Envio de spam. Por defeito, utiliza o Pushdo Trojan para infectar um sistema informático. Activo no sistema operativo Windows.
		Akbot	1,300,000 ^[22]			Backdoor, permitindo-lhe assumir o controlo de um computador infectado. Após a instalação, recolheu dados, parou processos, ou lançou ataques DDoS.
Março de 2007	Novembro de 2008	Srizbi	450,000 ^[23]	60	Cbeplay, Permutador	Enviando principalmente spam. O trojan Srizbi foi utilizado para infectar sistemas informáticos.
		Lethic	260,000 ^[16]	2	nenhuma	Envio principalmente de spam farmacêutico.
Setembro de 2007		dBot	10,000+ (Europa)		dentaoBot, d-net, SDBOT	
		Xarvester	10,000 ^[16]	0.15	Rlsloup, Pixoliz	Envio de spam.
2008						
		Salidade	1,000,000 ^[24]		Sector, Kuku	Grupo Malware. Os sistemas informáticos infectados com Sality comunicam através de P2P. A actividade consiste em: enviar spam, recolher dados sensíveis, atacar servidores web, efectuar cálculos distribuídos (por exemplo, para quebra de palavra-passe, etc.). Activo no sistema operativo Windows.
Abril de 2008		Kraken	495,000 ^[33]	9	Kracken	Distribuição de malwares. Ligação de outros computadores à botnet.
	Dezembro de 2009	Mariposa	12,000,000 ^[25]			Botnet principalmente envolvido em golpes e ataques DDoS. Foi uma das maiores redes de botnets de sempre.
Novembro de 2008		Conficker	10.500,000+ ^[26]	10	DownUp, DownAndUp, DownAdUp, Kido	Worm attacking computer systems with Windows OS. Os bugs deste SO foram utilizados para expandir ainda mais o botnet.
Novembro de 2008	Março de 2010	Waledac	80,000 ^[27]	1.5	Waled, Waledpak	Envio de spam e distribuição de malware. Rescindido pela acção da Microsoft.

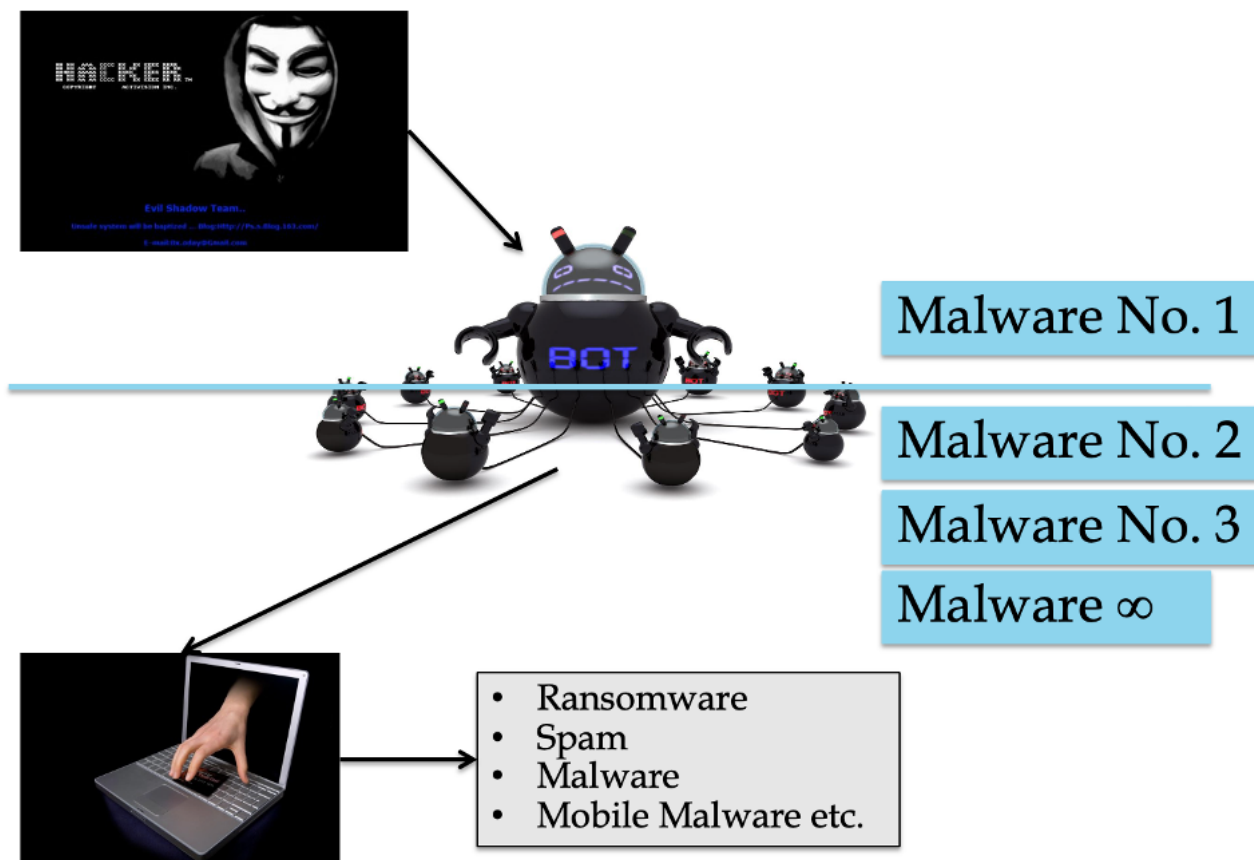
		Maazben	50,000 ^[16]	0.5	Nenhum	Envio de spam, malware, scam, phishing.
		OnewordSub	40,000 ^[28]	1.8		
		Gheg	30,000 ^[16]	0.24	Tofsee, Mondera	
		Nucrypt	20,000 ^[28]	5	Loosky, Locksky	
		Wopla	20,000 ^[28]	0.6	Pokier, Slogger, Cryptic	
		Asprox	15,000 ^[29]		Danmec, Hydraflux	Ataques de phishing, injeções SQL, propagação de malware.
		Spamthru	12,000 ^[28]	0.35	Spam-DComServ, Covesmer, Xmiler	Usando P2P
	19/07/2012	Grum	560,000 ^[31]	39.9	Tedroo	Envio principalmente de spam farmacêutico.
		Gumblar				
2009						
Maio de 2009	Novembro de 2010	BredoLab	30,000,000 ^[30]	3.6	Oficla	Envio de spam. Terminada por uma acção conjunta da polícia holandesa, Govcert NL, Europol. Kaspersky Lab, etc. Provavelmente o maior botnet conhecido.
	Novembro de 2009	Mega-D	509,000 ^[32]	10	Ozdok	Envio de spam.
Agosto de 2009		Festi	250,000 ^[34]	2.25	Spamnost	Envio de spam e realização de ataques DDoS.
2010						
Janeiro de 2010		LowSec	11,000+ ^[16]	0.5	LowSecurity, FreeMoney, Ring0.Tools	
		TDL4	4,500,000 ^[35]		TDSS, Alureon	
		Zeus	3,600,000 (apenas EUA) ^[36]		Zbot, PRG, Wsnpoem, Gorhax, Kneber	Centrado em actividades relacionadas com o roubo de informações de contas bancárias. Também instalou o CryptoLocker ransomware, etc. Activo no sistema operativo Windows.
	(Vários: 2011, 2012)	Kelihos	300,000+	4	Hlux	Maioritariamente envolvido no roubo de Bitcoin e no envio de spam.
2011						
	2015-02	Ramnit	3,000,000 ^[37]			Worm attacking computer systems with Windows OS. Encerrada por uma acção conjunta da Europol e da Symantec.

		Acesso Zero	2,000,000		Max+++ Sirefef	Botnet utilizado principalmente para mineração de bitcoins e fraude por clique. Activo no sistema operativo Windows.
2012						
		Camaleão	120,000		Nenhum	Clique Fraude
		Nitot				Botnet envolvida na propagação de malware e ataques DDoS. A maioria dos zombies (até 85%) estão localizados na China. O cliente botnet foi encontrado em sistemas informáticos entregues directamente a partir da fábrica.
2013						
		Boatnet	Mais de 500 computadores servidores	0.01	YOLOBotnet	
		Zer0n3t	Mais de 200 computadores servidores	4	FiberOptck, OptckFiber, Fib3rI0g1c	
2014						
		Semal	300,000+		Soundfrost	Envio de spam.
		Necurs	6,000,000			
2016						
		Mirai	380,000			DDoS, envio de spam.
		Methbot	6.000 domínios e 250.267 URLs distintos			
2018						
		3ve	1,7 milhões de computadores e um grande número de servidores			Roubo de dinheiro.

De facto, qualquer sistema informático pode ser ligado a uma rede de botnets. Entre outras coisas, estes são sistemas que satisfazem os requisitos da Internet das Coisas (IoT). Em 2014, foi relatado um caso em que uma rede de bots incluía um frigorífico que enviava mais de 750.000 e-mails de spam. [9].

O estudo da Nigam mostra [10] que existem dezenas de botnets directamente criados e principalmente centrados em sistemas informáticos, aos quais podemos chamar dispositivos móveis (por exemplo, smartphones, tablets, etc.). Devido à instalação de aplicações de fontes desconhecidas e à considerável ausência de produtos antivírus nos dispositivos móveis dos utilizadores, é também muito mais fácil instalar malware nestes dispositivos móveis e assim ganhar controlo sobre eles. Estes dispositivos são actualmente capazes de satisfazer plenamente os requisitos de um botmaster para o funcionamento de uma botnet, ou para as tarefas atribuídas aos "zombies".

O malware serve como um meio de obter acesso, controlo e maior disseminação de malware ou outras tarefas, tal como dirigido por um atacante, e não apenas no caso de botnets. No entanto, se o malware estiver actualmente infectado no sistema informático de um utilizador, é altamente provável que se tenha tornado parte da rede de botnets. Um atacante (botmaster) instala malware num sistema informático (zombie) que lhe permite manipular o sistema informático remotamente (malware N° 1 - enquanto este malware deixa o controlo ao botmaster mesmo que, por exemplo, parte ou a totalidade da botnet seja alugada). Só então é instalado outro software malicioso (malware 2. para malware ∞) para realizar outras tarefas (por exemplo, envio de spam, recolha de dados, extorsão utilizando ransomware, etc.). Toda a estrutura pode ser ilustrada como se segue:



Malware instalado num sistema informático ligado a uma botnet

De uma perspectiva legal, pode afirmar-se que as botnets representam redes inteiras de sistemas informáticos infectados sobre os quais um terceiro assumiu algum controlo sem autorização, sem o conhecimento dos utilizadores autorizados. Esses sistemas infectados servem na maioria das vezes como base para a ligação anónima de um atacante à Internet, para o envio de programas maliciosos, para a realização de ataques a outros alvos, para a realização de ataques DoS, para a difusão de spam, roubo de identidade ou outros ciberataques.

Possibilidades de sanções penais na República Checa

Quanto à própria actividade de um agressor, que consiste na instalação de malware para o controlo subsequente de um sistema informático, é possível avaliar esta conduta de acordo com a **Secção 230** do Código Penal (acesso não autorizado ao sistema informático e ao portador de informação). Se um atacante colocar malware num sistema informático com a intenção de causar danos ou outros danos a outro ou obter um benefício não autorizado para si próprio ou para outro, as suas acções poderão ser qualificadas de acordo com a Secção 230 (2) (d) do Código Penal.

Pode argumentar-se que é também uma utilização não autorizada da posse de outrem (porque o sistema informático em questão é a posse de outrem nestes casos) ao abrigo da **Secção 207 (1) al. (1)** do Código Penal. A aplicação da Secção 207 (1) al. (2) do Código Penal^[11], pode ser bastante problemática, pois a intensidade da intervenção e utilização do sistema informático é decisiva. Com base neste grau de intensidade, seria possível, se apropriado, quantificar os danos sofridos como expressão de depreciação no momento da utilização. Infelizmente, ao utilizar este cálculo, os danos causados não são pequenos.

A protecção real contra a ligação e utilização de computadores dentro da rede botânica pode ter dois níveis. O primeiro nível consiste em aumentar a protecção dos direitos de propriedade, complementando a Secção 207 do Código Penal com o elemento objectivo básico, cuja redacção poderia ser a seguinte: **"Quem utilizará um sistema informático sem o consentimento da pessoa habilitada".**

Esta disposição também definiria a circunstância que consiste em interferir com os direitos de propriedade de outro. No caso de utilização não autorizada da posse de outrem em relação a um sistema informático, a solução não é reduzir os danos de não pequenos para insignificantes (ver Secção 207 (1) al. (1) do Código Penal, uma vez que o preço de muitos sistemas informáticos é actualmente inferior a pelo menos 5.000 CZK) e, no entanto, estes sistemas informáticos são capazes de executar integralmente a actividade atribuída dentro da rede de bots.

O segundo nível, que descreve a gravidade das acções do agressor, consiste então na inclusão de uma nova circunstância de qualificação na Secção 230 (3) do Código Penal, enquanto que esta circunstância poderia ser a seguinte:

"liga intencionalmente um sistema informático a uma rede informática com a intenção de cometer um crime ou utiliza-o nessa rede com a mesma intenção,"

Possibilidades de sanções penais na Polónia

Acesso ilegal a um sistema (hacking) - Arte. 267 § 1 e 2 do Código Penal. Este crime é processado a pedido da parte lesada. São puníveis com uma multa, restrição da liberdade ou prisão até 2 anos.

Artigo 267º Obtenção ilícita de informações

§ Quem, sem autorização, obtém acesso a informações que não lhe são destinadas, abrindo uma revista fechada, ligando-se a uma rede de telecomunicações ou quebrando ou contornando a protecção electrónica, magnética, informática ou outra protecção específica da mesma, está sujeita a uma multa, a pena de limitação da liberdade ou de privação de liberdade por um período máximo de 2 anos.

§ 2. A mesma punição será imposta a qualquer pessoa que, sem autorização, obtenha acesso à totalidade ou a qualquer parte de um sistema informático.

§ 3. A mesma punição será imposta a qualquer pessoa que, a fim de obter informações a que não tenha direito, estabeleça ou utilize um dispositivo de escuta ou visual, ou outro dispositivo ou software.

§ 4. A mesma punição será imposta a quem divulgar a outra pessoa informações obtidas da forma especificada nos § 1-3.

§ A acusação da infracção especificada em § 1-4 ocorrerá mediante moção da pessoa lesada.

Possibilidades de sanções penais em Portugal

De acordo com a Arte. 6(2) da *Lei sobre o Cibercrime*, a introdução ilegal em um ou vários dispositivos informáticos de qualquer programa informático, instrução executável, código ou dados destinados a efectuar um acesso ilegal a um sistema informático é penalizada como sendo um acesso ilegal. O mesmo se aplica aos crimes de danos a programas informáticos ou outros dados informáticos [Interferência de dados] (art. 4(3), Sabotagem informática [Interferência ilegal] (art. 5(2) e também Intercepção ilegal (art. 7(3)).

Além disso, não existem quaisquer disposições relacionadas com a construção ou utilização de redes para a realização de qualquer uma das infracções declaradas.

[1] **Bot** (abreviatura da palavra robot). É um programa que pode executar os comandos de um atacante introduzidos a partir de outro sistema informático. Na maioria das vezes é uma infecção de um computador com um vírus como verme, cavalo de Tróia, etc. O sistema informático, que é assim remotamente controlado, é então referido como um **zombie**. No entanto, algumas fontes até se referem a um sistema informático infectado como um bot.

Um bot pode recolher dados, processar pedidos, enviar mensagens, comunicar com um elemento de controlo, etc.

[2] Para mais detalhes ver *Distribuvanévypočty*. [online]. [cit.2.11.2013]. Disponível em: <http://dc.czechnationalteam.cz/>

[3] Para mais pormenores, ver: PLOHMANN, Daniel, Elmar GERHARDS-PADILLA e Felix LEDER. *Botnets: Detecção, Medição, Desinfecção e Defesa*. ENISA, 2011. [online]. [cit.17.5.2015], p. 14. Disponível em: <https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence>

Outras definições e informações sobre os botnet podem ser encontradas, por exemplo, em:

Co je to botnet a jak se šíří? [online]. [cit.15.7.2016]. Disponível a partir de: <https://www.youtube.com/watch?v=ywXqDon5Xtg>

Botnety: nová internetová hrozba. [online]. [cit.15.7.2016]. Disponível a partir de: <http://www.lupa.cz/clanky/botnety-internetova-hrozba/>

Války síťových robotů - jak fungují sítě botnets. [online]. [cit.15.7.2016]. Disponível a partir de: http://tmp.testnet-8.net/docs/h9_botnet.pdf

Botnets. [online]. [cit.15.7.2016]. Disponível em: <https://www.youtube.com/watch?v=-8FUstzPixU&index=2&list=PLz4vMsOKdWVHb06dLjXS9B9Z-yFbzUWl6>

[4] Figura de um botnet centralizado. Para mais pormenores, ver: PLOHMANN, Daniel, Elmar GERHARDS-PADILLA e Felix LEDER. *Botnets: Detecção, Medição, Desinfecção e Defesa*. ENISA, 2011. [online]. [cit.17.5.2015], p. 16. Disponível em: <https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence>

[5] Figura de um botnet descentralizado. Ibidem, p. 18

[6] Economia malware. Para mais pormenores, ver: PLOHMANN, Daniel, Elmar GERHARDS-PADILLA e Felix LEDER. *Botnets: Detecção, Medição, Desinfecção e Defesa*. ENISA, 2011. [online]. [cit.17.5.2015], p. 21. Disponível em: <https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence>

[7] *Bots e Botnets - Uma Ameaça crescente*. [online]. [cit.11.8.2016]. Disponível em: <https://us.norton.com/botnet/>

[8] A tabela foi criada com base numa combinação de informações das seguintes fontes:

Botnet. [online]. [cit.15.7.2016]. Disponível a partir de: <https://en.wikipedia.org/wiki/Botnet>

Botnet - Lista histórica de Botnets. [online]. [cit.15.8.2016]. Disponível a partir de: http://www.liquisearch.com/botnet/historical_list_of_botnets

Botnet. [cit.8.7.2016]. Disponível a partir de: <http://research.omicsgroup.org/index.php/Botnet>

Lista histórica de botnets. [em linha]. [cit.15.8.2016]. Disponível em: <http://jpdias.me/botnet-lab/history/historical-list-of-botnets.html>

[9]Frigorífico apanhado a enviar e-mails de spam em ataque de botnet. [em linha]. [cit.17.5.2016]. Disponível em: <http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/>

[10] Para mais detalhes ver NIGAM, Ruchna. *Uma linha temporal de botnets móveis*. [online]. [cit.12.7.2016]. Disponível a partir de: <https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.2-A-Timeline-of-Mobile-Botnets-PAPER.pdf>

[11] Esta disposição prevê danos a bens de outras pessoas, enquanto que os danos não têm de ser pequenos (ou seja, pelo menos 25.000 CZK, ver Secção 138 (1) do Código Penal).

4.3. Malware

Malware (um composto de software malicioso) pode ser qualquer software utilizado para perturbar o funcionamento normal de um sistema informático, obter informações (dados) ou ser utilizado para obter acesso a um sistema informático. O malware pode assumir muitas formas, com muitos tipos de malware com o nome da actividade que executam.

Um malware é capaz de desempenhar várias funções (realizar várias actividades) ao mesmo tempo. Por exemplo, pode propagar-se ainda mais por correio electrónico (num anexo) ou como dados em redes P2P, e ao mesmo tempo pode obter, por exemplo, endereços de correio electrónico de um sistema informático infectado.

Historicamente, havia no início uma série de termos diferentes para este software, que é actualmente referido pelo termo colectivo malware. Os nomes reais de software malicioso específico eram geralmente criados de acordo com a actividade que o programa executava. Apesar da afirmação acima referida de que o termo malware é utilizado principalmente no presente, ainda é possível encontrar uma designação historicamente mais antiga de software malicioso. Estes são os seguintes grupos:

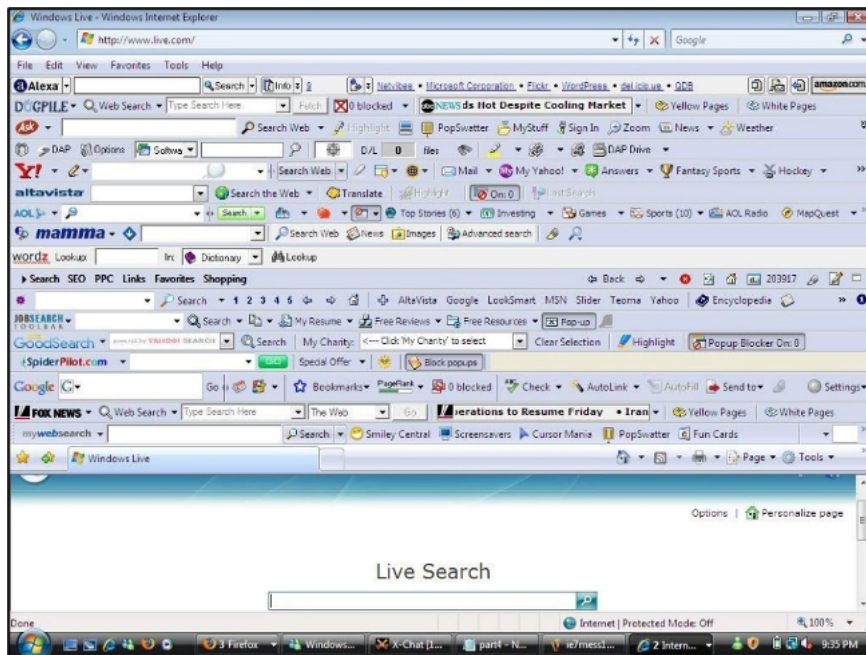
1. **Adware**
2. **Spyware**
3. **Vírus**
4. **Minhocas**
5. **Cavalos de Tróia**
6. **Backdoor**
7. **Rootkits**
8. **Keylogger**
9. **Resgate, etc.**[1]

Anúncio 1) Adware

O termo adware é uma abreviatura da frase inglesa "*advertising support software*". É a forma menos perigosa mas rentável de malware.[2]. O adware exhibe anúncios no sistema informático do utilizador (por exemplo, pop-ups no sistema operativo[3] ou em websites, anúncios exibidos juntamente com software, etc.). Embora na maioria dos casos sejam produtos que apenas incomodam o utilizador com mensagens publicitárias constantes que "aparecem" no ecrã, o adware também pode ser associado a spyware, cujo objectivo é monitorizar a actividade do utilizador e roubar informações importantes.



Adware



Exemplo de Adware e outros add ons instalados num web browser [4].

Anúncio 2) Spyware

O termo spyware é uma combinação das palavras inglesas "*spy*" e "*software*". O spyware é utilizado para obter dados estatísticos[5] sobre uma operação de um sistema informático e para o enviar para uma caixa de dados de um atacante sem o conhecimento e consentimento de um utilizador. Estes dados podem também incluir informações de natureza pessoal ou informações sobre uma pessoa de um utilizador, bem como informações sobre websites visitados, aplicações em execução, etc.

O spyware pode ser instalado como um malware autónomo, bem como muitas vezes como parte de outros programas, gratuitos e completamente seguros. Neste caso, a instalação e outras actividades do spyware são tipicamente tratadas nos termos do EULA, e o utilizador geralmente concorda voluntariamente, sem o saber, em monitorizar as suas próprias actividades. A adição de programas de spyware a outros programas (por exemplo, programas clientes P2P, vários programas shareware, etc.) é motivada pelos esforços do fabricante do programa para descobrir os interesses ou necessidades de um utilizador e utilizar esta informação, por exemplo, para publicidade dirigida.[6] Uma característica dos programas de spyware que fazem parte de um "pacote de programas" é que normalmente permanecem instalados no computador mesmo depois de o programa principal ter sido desinstalado, o que na maioria dos casos é ocultado ao utilizador.

O spyware representa uma ameaça tanto porque envia várias informações do sistema informático de um utilizador para um "atacante" (que é posteriormente processado e correlacionado com dados e informações obtidas de outras fontes), como porque o spyware pode conter outras ferramentas que afectam as actividades do próprio utilizador[7].

Anúncio 3) Vírus

É um programa ou código malicioso que se liga a outro ficheiro executável existente (por exemplo, software, etc.) ou documento. O vírus é reproduzido no momento em que este software é lançado ou em que um documento infectado é aberto. Na maioria das vezes, os vírus propagam-se através da partilha de software entre sistemas informáticos; não necessitam da cooperação de um utilizador para os difundir. Os vírus eram a forma dominante de malware, especialmente nas décadas de 1980 e 1990.[8]

Há um grande número de vírus cujo objectivo é destruir, enquanto outros são concebidos para "se instalarem" no maior número possível de sistemas informáticos e depois utilizá-los para um ataque direccionado. Típico para estes programas é a capacidade de propagação entre sistemas sem a necessidade de intervenção do utilizador num sistema informático. Os efeitos dos vírus podem ser multifacetados, tais como a reprodução inofensiva de uma melodia, congestionamento do sistema, alteração ou destruição de dados, ou a destruição total de um sistema infectado. Os vírus informáticos podem ser classificados de acordo com muitos aspectos diferentes, por exemplo, de acordo com o anfitrião (ou seja, de acordo com o tipo de programas que os vírus informáticos transmitem), de acordo com a forma como actuam no sistema, de acordo com a sua localização na memória, etc. [9]. Dependendo dos ficheiros em que os vírus infectam, podem ser divididos:

- § vírus de arranque (infectar apenas partições do sistema)
- § ficheiros de vírus (infectar apenas ficheiros)
- § vírus multipartidos (infectar ficheiros, bem como áreas do sistema)
- § macrovírus (aplicações de ataque usando macros)

Anúncio 4) Minhocas

Os chamados **worms informáticos** também são referidos como vírus. A razão para a ligação mais estreita com os vírus é o facto de os vermes não precisarem de nenhum hospedeiro, ou seja, nenhum ficheiro executável (semelhante aos vírus). Ao contrário dos vírus, que são anexados como parte de outro programa, estes programas geralmente propagam-se separadamente. Um sistema comprometido é então utilizado por um worm para enviar mais cópias de si mesmo a outros utilizadores através da comunicação em rede. Desta forma, espalha-se muito rapidamente, o que pode levar ao

Distribuição de malwares

Há uma série de formas através das quais o malware pode ser entregue a um sistema informático alvo. Aqui irei listar brevemente alguns métodos de propagação de malware. O malware pode ser distribuído através de:

- **Meios de armazenamento portáteis**

Por exemplo, utilizando CD, DVD, USB, drive externo, etc. Esta é a forma mais antiga mas ainda eficaz de distribuir malware, onde os utilizadores passam ficheiros infectados ou **redes informáticas** contendo **ficheiros infectados** (partilhando tais ficheiros dentro de redes informáticas, tipicamente redes P2P).

- **Drive-by-download**

Uma das formas mais comuns de infectar malware é descarregá-lo da Internet e depois executar um ficheiro, normalmente com uma extensão .exe (ficheiro executável), a partir de uma fonte desconhecida. Estes podem ser programas falsos ou falsificados (por exemplo, imitações de Flapp Bird, codecs de meios falsos, etc.), programas utilizados para contornar a protecção dos direitos de autor (rachaduras, keygens, etc.), programas infectados reais, etc.

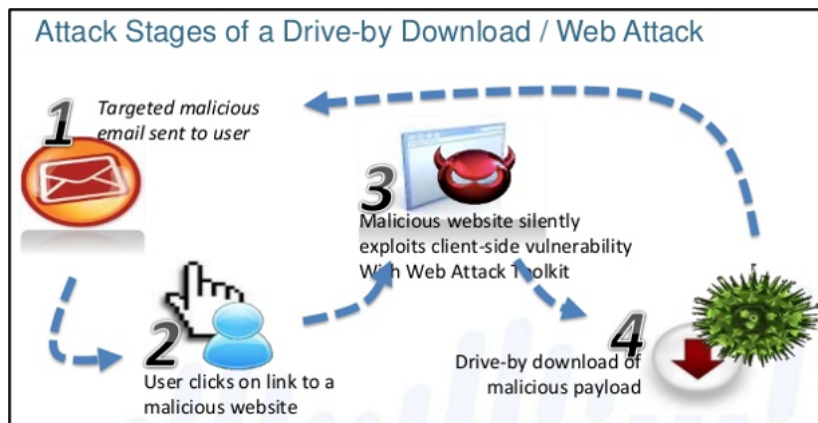
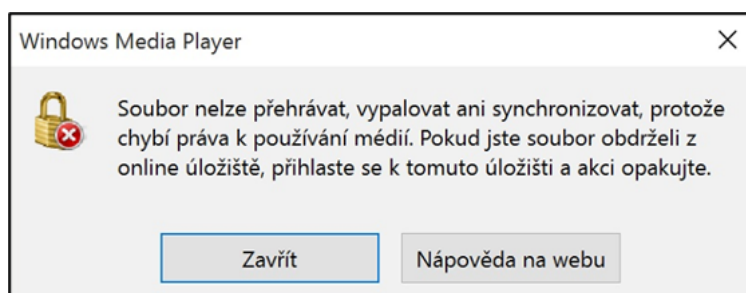
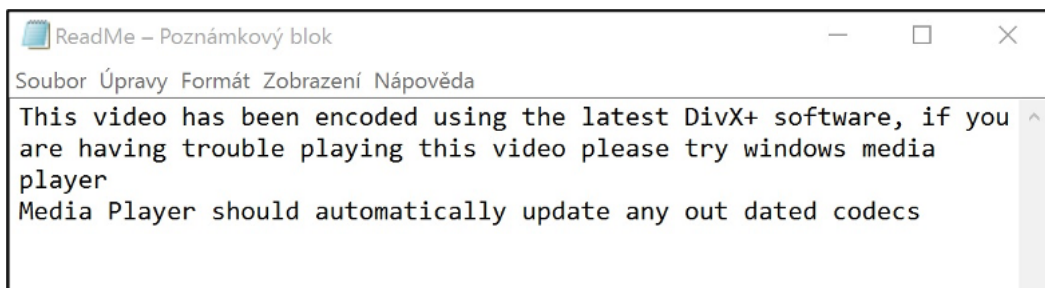
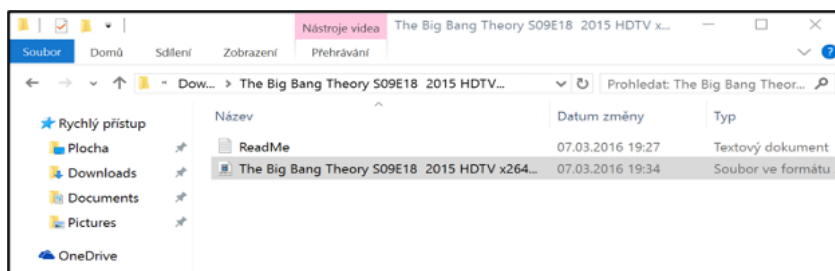


Ilustração de um dos possíveis princípios de condução por download.[\[20\]](#)

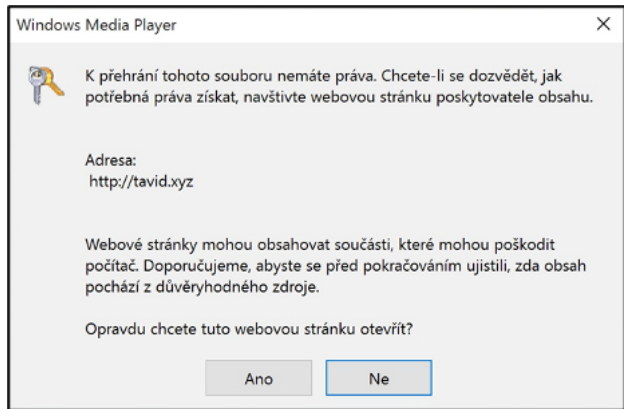
O exemplo seguinte mostra malware descarregado por um utilizador através de uma rede P2P (especificamente, um ficheiro com a *The Big Bang Theory -Season 9, Part 18*). Este malware levou os utilizadores a descarregar um novo codec através do Media Player para que o vídeo pudesse ser reproduzido. O media player começou a ligar-se ao site de um atacante e depois foi instalado um codec fictício, mas de facto foi instalado malware no computador (neste caso uma combinação de malware: backdoor, keylogger, bot), o que permitiu ao atacante controlar completamente o sistema informático do utilizador.

Neste caso, o facto de a parte oferecida da *The Big Bang Theory* ainda não ter sido transmitida nos EUA, onde estreia, foi muito impressionante, mas o número de downloads foi nas dezenas de milhares.



Texto sobre a figura: O ficheiro não pode ser reproduzido, queimado ou sincronizado porque faltam os direitos de utilização dos media. Se recebeu o ficheiro de um repositório online, inicie a sessão nesse repositório e tente novamente.

Fechar / Ajuda na web



Texto sobre a figura: Não tem permissão para reproduzir este ficheiro. Para saber como obter os direitos necessários, visite o website do fornecedor de conteúdos.

Endereço: <http://tavid.xyz>

Os sítios Web podem conter componentes que podem prejudicar o seu computador. Recomendamos que se assegure de que o conteúdo vem de uma fonte de confiança antes de prosseguir.

Tem a certeza de que quer abrir esta página web?

Sim / Não



· "Documentos de escritório"

Muito frequentemente, o malware espalha-se no corpo de ficheiros como, por exemplo: .doc, .xls, .avi, etc. Só os vírus macro podem ser distribuídos desta forma. Um utilizador assume que está a abrir um documento Word, mas ao mesmo tempo corre um ficheiro executável que se mascara como esse documento.

· Correio electrónico

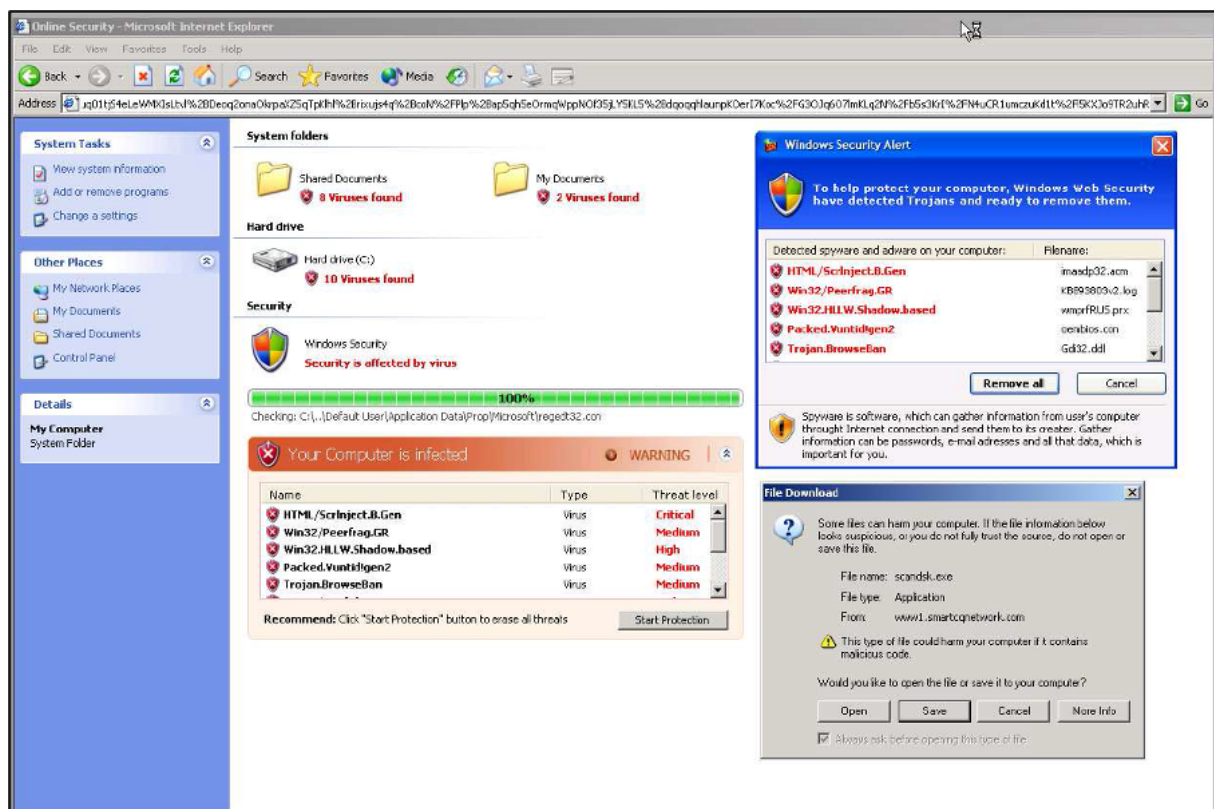
O malware pode ser armazenado num anexo a um e-mail, ou pode ser um script dentro de um corpo de e-mails HTML[21]. Esta é actualmente uma das formas mais comuns de distribuição de malware. Exemplos disso são as actuais campanhas de phishing, hoaxes, spam, etc.

· HTML

Os malwares podem ser colocados directamente num website ou em scripts individuais.

· Antivírus falso

Aos utilizadores é normalmente oferecido um antivírus gratuito - como adware. Este antivírus irá "scanear o seu computador" e detectar vulnerabilidades graves e malware que o antivírus de um utilizador não detectou. O falso antivírus combina um ataque de engenharia social (levantando preocupações sobre software malicioso) com a instalação de malware contido num falso antivírus.



Antivírus falso

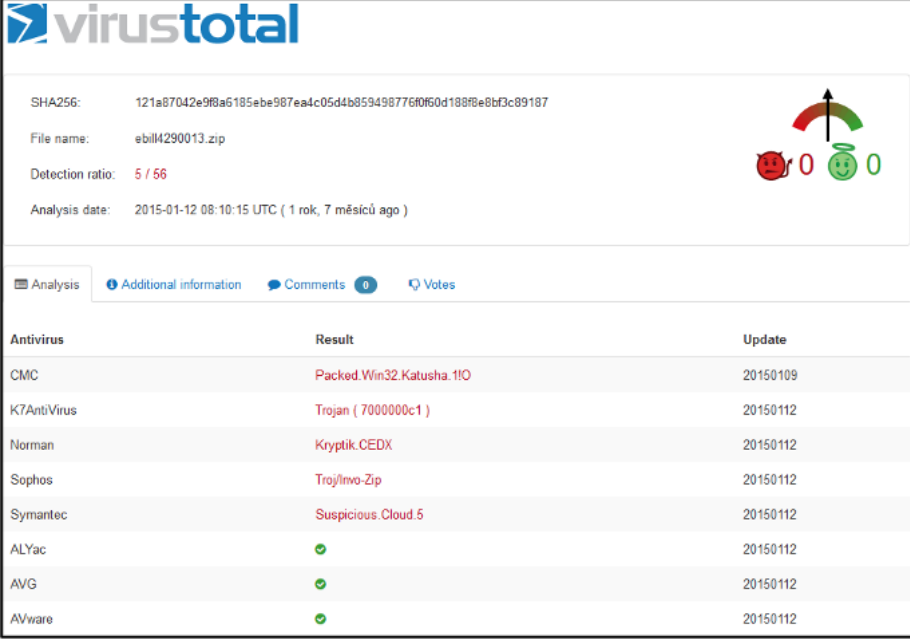


Antivírus falso[22]

Se um utilizador não tiver a certeza se um ficheiro ou website contém malware, pode usar uma variedade de ferramentas para o ajudar a verificar a existência de malware.

Um dos serviços comprovados é <https://www.virustotal.com/>. Nesta página web, um utilizador pode especificar uma digitalização de um ficheiro até 128 MB ou ter um sítio web a que pretende aceder verificado. (É aconselhável realizar esta digitalização, por exemplo, ao visitar sítios bancários na Internet ou sítios de pagamento. É preciso copiar o **URL completo da página que se visita**). O serviço Virustotal liga empresas que lidam com cibersegurança, desenvolvimento de produtos antivírus, etc., enquanto o pedido de um utilizador é testado pelas ferramentas de todas estas empresas, aumentando assim a probabilidade de detecção de software malicioso.

O seguinte ecrã de impressão mostra o resultado da digitalização de um ficheiro recentemente entregue, como parte de uma campanha de phishing. No dia seguinte ao início desta campanha, apenas 5 empresas identificaram malware num ficheiro anexo, e no prazo de uma semana todas as outras empresas conseguiram identificá-lo. Contudo, o tempo entre a entrega de actualizações aos antivírus dos utilizadores nos seus sistemas informáticos e o início do ataque é crucial para o eventual sucesso de um atacante.



SHA256: 121a87042e9f8a6185e9e987ea4c05d4b859498776f0f60d188f8e8bf3c89187

File name: ebill4290013.zip

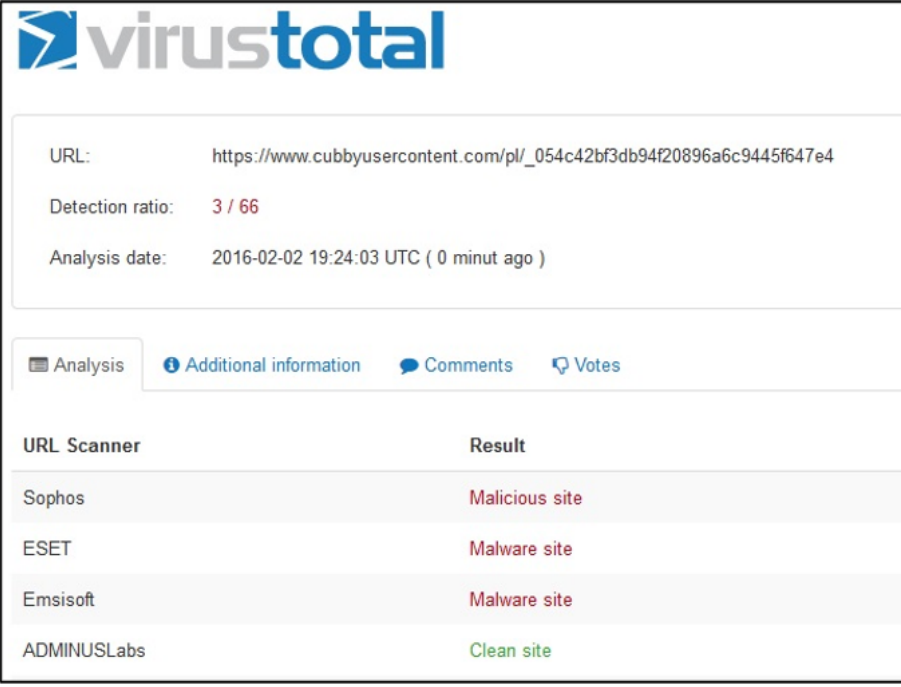
Detection ratio: 5 / 56

Analysis date: 2015-01-12 08:10:15 UTC (1 rok, 7 měsíků ago)

Analysis | Additional information | Comments (0) | Votes

Antivirus	Result	Update
CMC	Packed.Win32.Katusha.1!Q	20150109
K7AntiVirus	Trojan (7000000c1)	20150112
Norman	Kryptik.CEDX	20150112
Sophos	Trojan/Win32	20150112
Symantec	Suspicious.Cloud.5	20150112
ALYac	✓	20150112
AVG	✓	20150112
AVware	✓	20150112

Resultado do teste do ficheiro



URL: https://www.cubbyusercontent.com/pl/_054c42bf3db94f20896a6c9445f647e4

Detection ratio: 3 / 66

Analysis date: 2016-02-02 19:24:03 UTC (0 minut ago)

Analysis | Additional information | Comments | Votes

URL Scanner	Result
Sophos	Malicious site
ESET	Malware site
Emsisoft	Malware site
ADMINUSLabs	Clean site

Resultado do teste do website

O malware pode ser instalado em quase todos os sistemas informáticos. Os casos de instalação de **micromalware** são exemplos de instalações específicas. Trata-se de código malicioso que se espalha num número relativamente pequeno de sistemas informáticos. Este código apresenta um comportamento anormal e os programas de segurança falham frequentemente em responder. O caso mais conhecido de micromalware é o verme **STUXNET**^[23], ou a instalação de um cliente botnet no já mencionado frigorífico.

Um malware concebido para dispositivos móveis (**malware móvel**) é então um capítulo separado. O primeiro malware concebido para atacar telemóveis foi descoberto por volta de 2004. Hoje, Kaspersky Lab, que relatou a descoberta na altura, afirma que existem mais de **340.000 malwares**.^[24]

Se nos concentrarmos no sistema operativo mais vulnerável dentro de dispositivos móveis, então a maioria das ameaças visam o SO Android. A razão para isto é principalmente a variedade de versões de sistemas operativos usados e a sua desactualização. **A maioria dos dispositivos Android não permite actualizar o seu sistema operativo para a versão mais recente, que é normalmente modificada para suportar vulnerabilidades conhecidas e já corrigiu bugs de versões anteriores deste sistema operativo. De facto, estima-se que 77% das ameaças que atacam o sistema operativo Android poderiam ser eliminadas através da utilização da versão mais recente deste sistema operativo.**

No caso de dispositivos móveis, os atacantes utilizam principalmente:

- **Versão desactualizada de um sistema operativo de dispositivo móvel** (vulnerabilidades conhecidas de sistemas individuais);

- **Segurança mínima de um dispositivo móvel** por meios anti-vírus;
- **Ignorância do utilizador** (Muitos utilizadores instalam imprudentemente aplicações "a partir de uma fonte desconhecida" ou aplicações que requerem acesso e permissões excessivas dentro do dispositivo.);
- **Engenharia social e "ondas de interesse" em aplicações de um certo tipo.**

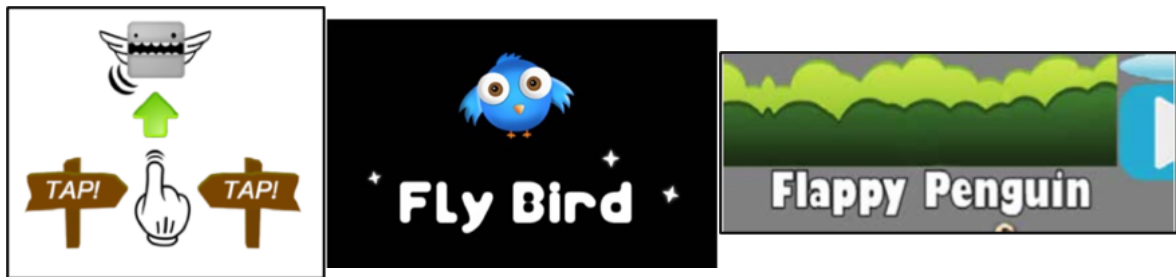
Uma das razões pelas quais o Android é atacado como sistema operativo principal é o facto de a segurança das aplicações não ser verificada dentro do canal de distribuição (Google Play) (ou se uma determinada aplicação não contém malware, por exemplo), como é o caso do sistema operativo iOS e do seu canal de distribuição (App Store).



Um exemplo do acima referido é o **Flappy Bird** e os seus "clones". Esta aplicação foi

desenvolvida por Nguyễn Hà Đồng e lançada para distribuição no iOS a 24 de Maio de 2013. Esta aplicação ficou disponível para o SO Android em 2014, e em Janeiro de 2014 tornou-se o jogo gratuito mais descarregado. O criador retirou o jogo do mercado a 10th de Fevereiro de 2014. O jogo registou mais de 50 milhões de descarregamentos.

Já na altura em que o jogo original Flappy Bird estava no mercado, vários clones deste jogo para o SO Android começaram a aparecer, muitos dos quais beneficiaram apenas do sucesso do original. Contudo, o malware foi deliberadamente colocado em várias outras versões, e estima-se que até 79% dos clones deste jogo tenham sido infectados com software malicioso.^[25] Os clones infectados incluem, por exemplo, os seguintes produtos:



A infecção de um telemóvel pode ser um dos alvos principais de um atacante, uma vez que estes dispositivos são tipicamente utilizados hoje em dia para autenticação de dois factores de autenticação de bancos ou compras pela Internet. Os atacantes tentam utilizar a informação obtida, por exemplo, para levantar fundos através do acesso directo à conta bancária de um utilizador através do serviço bancário da Internet ou para obter informação sensível.

Possibilidades de sanções penais na República Checa

Na República Checa, é possível punir um ataque com malware de acordo com a **Secção 230** (Acesso não autorizado a um sistema informático e a um portador de informação) do Código Penal. A **posse de malware, com a intenção de cometer uma infracção penal** nos termos da Secção 182 (Violação do sigilo das mensagens transportadas) ou uma infracção penal nos termos da Secção 230 do Código Penal, **é uma infracção penal nos termos da Secção 231** (Obtenção e posse de dispositivos de acesso e senhas de sistemas informáticos e outros dados deste tipo) do Código Penal. Se o **objectivo de um vírus** fosse obter, por exemplo, informações classificadas ou apoio de um grupo terrorista, um agressor poderia, por exemplo, cometer os crimes da **Secção 311** (Ataque terrorista), da **Secção 316** (Inteligência) ou da **Secção 317** (Ameaça de informações classificadas) do Código Penal **na fase de preparação**.

Possibilidades de sanções penais na Polónia

Violação da integridade dos dados (vírus, trojans), 268 do Código Penal, Arte. 268a do Código Penal. Esta infracção diz respeito, nomeadamente, ao roubo de dados pessoais, à sua disponibilização a terceiros sem o consentimento do proprietário, bem como à sua utilização de forma não autorizada. Existem sanções financeiras (até PLN 100.000) pela prática destes actos.

Artigo 268º Tornar difícil para uma pessoa com direito de se familiarizar com a informação

§ Quem, sem ter o direito de o fazer, destruir, danificar, apagar ou alterar um registo de informação importante ou de qualquer outra forma impedir ou obstruir consideravelmente uma pessoa com direito de tomar conhecimento da mesma, será sujeito a uma multa, a pena de limitação da liberdade ou privação de liberdade por um período até 2 anos.

§ 2 Se o acto especificado no § 1 disser respeito a um registo num suporte de dados informático, o autor do crime

será sujeito à pena de privação de liberdade por um período máximo de 3 anos.

§ 3. Quem, ao cometer o acto especificado nos § 1 ou 2, causar danos substanciais à propriedade, estará sujeito à pena de privação de liberdade por um período compreendido entre 3 meses e 5 anos.

Artigo 268a. Destruir, danificar, apagar, alterar ou impedir o acesso aos dados informáticos

§ Quem, sem ter o direito de o fazer, destruir, danificar, apagar, alterar ou obstruir o acesso aos dados informáticos ou interferir substancialmente ou impedir o processamento, armazenamento ou transferência automatizados de tais dados

será sujeito à pena de privação de liberdade por um período máximo de 3 anos.

§ 2. Quem, ao cometer o acto especificado no § 1, causar danos substanciais à propriedade,

está sujeita à pena de privação de liberdade por um período compreendido entre 3 meses e 5 anos.

§ 3 A acusação da infracção especificada nos § 1 ou 2 deve ocorrer com base numa moção dos feridos

Possibilidades de sanções penais em Portugal

De acordo com a Arte. 6(2) da *Lei sobre o Cibercrime*, a criação, distribuição ou difusão ilegal de qualquer programa informático, instrução executável, código ou dados destinados a efectuar um acesso ilegal a um sistema informático é penalizada como sendo um acesso ilegal. O mesmo se aplica aos crimes de danos a programas informáticos ou outros dados informáticos [Interferência de dados] (art. 4(3), Sabotagem informática [Interferência ilegal] (art. 5(2) e Intercepção ilegal (art. 7(3), uma vez que o legislador português decidiu não ter uma única disposição para a utilização indevida de dispositivos, como a Convenção de Budapeste (art. 6).

[1] Esta não é uma lista completa de diferentes tipos de malware. Trata-se antes de definir os tipos básicos de malware, incluindo uma explicação de como eles funcionam.

[2] Há empresas especializadas em "pagar por instalação" (PPI). "PPI causa então muitas actividades que levam à instalação de add-ons ou outro software indesejado, que (no caso menos prejudicial) troca anúncios em websites sem o conhecimento do utilizador ou insere-os onde não há anúncios no site... O PPI baseia-se no facto de que aqueles que oferecem estes serviços não prestam qualquer atenção a se o utilizador quer instalar algo. Recebem até 1,50 USD por instalação, pelo que é mais do que certo que instalações fraudulentas e automatizadas são um elemento essencial do seu "modelo de negócio".

[3] Figura destes pop-ups. Para mais detalhes, ver *Adware*. [online]. [cit.10.8.2016]. Disponível a partir de: <http://www.mhsaoit.com/computer-networking-previous-assignments/324-lesson-16-h-the-secret-history-of-hacking>

[4] [em linha]. [cit.10.8.2016]. Disponível em: <https://i.ytimg.com/vi/GcvlB-EpMwA/maxresdefault.jpg>

[5] Por exemplo, uma visão geral dos websites visitados, os seus endereços IP, visão geral dos programas instalados e utilizados, registos de downloads de ficheiros da Internet, dados sobre a estrutura e o conteúdo dos directórios armazenados no disco rígido, etc.

[6] [cit.8.1.2008]. Disponível a partir de: <http://www.spyware.cz/go.php?p=spyware&t=clanek&id=9>

[7] Estes podem ser, por exemplo: **Browser Helper Object** (biblioteca DLL, permitindo aos programadores mudar e monitorizar o Internet Explorer); **Hijacker** (software que altera uma página inicial de um navegador da web); **Dialers** [redirecciona a linha telefónica para tarifas telefónicas caras (actualmente, principalmente ataques a telemóveis e trocas VoIP)]; **Keystroke Logger / Keylogger** (monitorização de teclas); **Administração remota** (permite a um utilizador remoto controlar remotamente o sistema informático de um utilizador); **Tracer** (um programa que monitoriza o movimento de um sistema informático - tipicamente um dispositivo móvel), etc.

[8] Para mais detalhes ver The Malware Museum. *O Museu da Malware @ Internet Archive*. [online]. [cit.17.5.2016]. Disponível a partir de: <https://labsblog.f-secure.com/2016/02/05/the-malware-museum-internet-archive/>

[9] Mais detalhes, por exemplo, em PO`ÁR, Josef. Informační bezpečnost. Plzeň: Aleš Čeněk, 2005, p. 216 et seq.

[10] Para mais detalhes ver RAK, Roman e Radek KUMMER. Informačníhrozby v letech 2007-2017. *Security magazín*, 2007, vol. 14, No. 1, p. 4.

[11] Cf. JIROVSKÝ, Václav e Oldřich KRULÍK. Základní definice vztahující se k tématu. *Security magazín*, 2007, vol. 14, No. 2, p. 47.

[12] Uma visão geral dos Trojans mais comuns, juntamente com uma lista das suas funções e portas de comunicação, pode ser obtida a partir de vários websites disponíveis na Internet. Para mais pormenores ver, por exemplo, <http://www.test.bezpecnosti.cz/full.php>

[13] Cf. JIROVSKÝ, Václav. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praga: Grada, 2007, p. 63.

[14] Estes programas são por vezes referidos como programas de digitalização ou scanner.

[15] Para mais detalhes cf. BALIGA, Arati, Liviu IFTODE e Xiaoxin CHEN. Contenção Automatizada de Ataques de Rootkits. *Computers & Security*, 2008, vol. 27, No. 7-8, pp. 323-334.

[16] Cf. RAK, Roman e Radek KUMMER. Informačníhrozby v letech 2007-2017. *Security magazín*, 2007, vol. 14, No. 1, p. 5.

[17] Por exemplo, o Trojan DNS-Changer primeiro ataca programas de segurança, retirando-se da lista de programas maliciosos, o que torna impossível a sua detecção. Para mais detalhes: PLETZER, Valentin. Demaskovaný spyware. *CHIP*, 2007, No. 10, pp. 116-120.

[18] JIROVSKÝ, Václav. *Kybernetická kriminalita. Nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praga: Grada, 2007, p. 65

[19] Captura de teclas e informação sobre ficheiros em execução. [online]. [cit.10.8.2016]. Disponível em: <http://img.zerosecurity.org/files/2013/10/Keylogger-software-logfile-example.jpg>

[20] [em linha]. [cit.10.7.2016]. Disponível em: <https://image.slidesharecdn.com/delljointevent2014november-onur-141105074412-conversion-gate02/95/end-to-end-security-with-palo-alto-networks-onur-kasap-engineer-palo-alto-networks-23-638.jpg?cb=1415174438>

[21] Hyper Text Markup Language - Este é o nome da linguagem de marcação utilizada para criar páginas web.

[22] Duas versões de antivírus falso. [online]. [cit.10.8.2016]. Disponível a partir de: <http://www.cctslo.com/images/fake-personal-antivirus.jpg>

[23] Para mais detalhes, ver, por exemplo, *Stuxnet*. [online]. [cit.23.7.2016]. Disponível a partir de: <https://cs.wikipedia.org/wiki/Stuxnet>

[24] *O primeiro malware móvel: como Kaspersky Lab descobriu Cabir*. [online]. [cit.29.6.2015]. Disponível a partir de: <http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir>

Ver também, por exemplo:

kód cílí na mobily, šíří se jako lavina. [online]. [cit.17.5.2016]. Disponível a partir de: <https://www.novinky.cz/internet-a-pc/bezpecnost/401956-skodlivy-kod-cili-na-mobily-siri-se-jako-lavina.html>

Advertência! Mais de 900 milhões de telefones Android Vulneráveis ao Novo Ataque "QuadRooter". [online]. [cit.10.8.2016]. Disponível a partir de: <https://thehackernews.com/2016/08/hack-android-phone.html>

[25] Para mais detalhes, ver, por exemplo, *Flappy Bird Clones Help Mobile Malware Rates Soar*. [online]. [cit.14.8.2016]. Disponível a partir de: <http://www.mcafee.com/us/security-awareness/articles/flappy-bird-clones.aspx>

4.4. Ransomware

O grupo de malware também inclui o chamado malware extorsivo, para o qual o termo "**ransomware**" foi cunhado^[1] (por vezes também referido como rogueware ou scareware). Ransomware é um malware que impede ou restringe os utilizadores de utilizar correctamente um sistema informático até que um atacante receba um "resgate". O "ransomware" entra mais frequentemente no seu computador usando malware (um cavalo de Tróia ou worm) que está localizado num website ou é um anexo de e-mail. Uma vez que um malware esteja "estabelecido" em segurança num sistema informático, o seu próprio "ransomware" será descarregado.

Em geral, é possível distinguir dois tipos de resgates de acordo com o quanto interferem com o funcionamento real de um sistema informático. **O primeiro tipo é o de resgate que limita a funcionalidade de todo um sistema informático** e não permite que um utilizador utilize de todo este sistema (por exemplo, impedindo que o sistema operativo arranque ou bloqueando o ecrã do sistema). Um exemplo típico deste tipo é o "*Serviço de resgate da polícia*" - ver abaixo). **O segundo tipo é o "ransomware", que deixa um sistema informático funcional, mas bloqueia os dados do utilizador e torna-os inacessíveis.**

O objectivo deste malware é encriptar um disco rígido ou tipos de ficheiros seleccionados num sistema informático, visando principalmente encriptar os ficheiros privados de um utilizador, tais como imagens, documentos de texto ou de folha de cálculo, vídeos, etc. Após a encriptação, o utilizador recebe normalmente uma mensagem de que os seus ficheiros estão encriptados, e se quiser recuperá-los (decifrar), deve enviar uma certa quantia para a conta do atacante. Tipicamente, moedas virtuais como o Bitcoin ou vários serviços pré-pagos são utilizados para transacções. Na maioria dos casos, há um limite de tempo para o pagamento. Após este tempo, a chave que pode abrir os ficheiros encriptados é eliminada.

Evolução dos resgates

O Ransomware, como qualquer outro malware, está a evoluir, com o primeiro malware a ser classificado como ransomware a aparecer por volta de 2005. Foi essencialmente um **falso antivírus (screwware)** que, com a ajuda da engenharia social, tentou convencer um utilizador a pagar uma quantia pela limpeza de um sistema informático infectado. Este programa de resgate geralmente permitia ao utilizador utilizar um sistema informático (não estava bloqueado, ou dados encriptados), mas incomodava o utilizador com pop-ups e alertas sobre vírus inexistentes no computador. Este programa de resgate era muito fácil de remover.

O início massivo do resgate pode ser datado de cerca de 2011, quando um ataque de resgate bloqueando o acesso à conta de um utilizador do Windows começou a espalhar-se por todo o mundo, anunciando que o computador tinha sido bloqueado pela polícia do Estado.

O ataque real consistiu em o utilizador ficar infectado com malware (tipicamente um "cliente botnet" foi descarregado ao visitar alguns websites^[2]) e subsequentemente tornou-se parte de uma botnet através da qual o seu próprio "**resgate policial**" foi distribuído. Este "police ransomware" bloqueou subsequentemente o acesso a uma conta de utilizador do Windows^[3], notificando o utilizador de que foi encontrado no seu computador material que infringia a lei do país (por exemplo, violação dos direitos de autor, pornografia infantil, etc.). Ao mesmo tempo, o utilizador foi convidado pela "polícia" a pagar a quantia necessária, após o que o computador será desbloqueado e tudo será "resolvido". Neste caso, os atacantes utilizaram técnicas de engenharia social, especificamente as preocupações e a confiança de um utilizador, e ao referir-se às autoridades oficiais, tentaram obter dinheiro dele.

O que foi surpreendente em todo o caso foi o facto de uma grande parte dos utilizadores ter pago voluntariamente o montante exigido (na República Checa, este montante variou entre CZK 2000-4000), sem verificar se a polícia real está autorizada a bloquear computadores ou a "tratar" de quaisquer infracções do utilizador de tal forma.

Os seguintes ecrãs de impressão mostram "resgates policiais" em vários países e depois são mostradas as versões utilizadas na República Checa.



Resgate policial^[4]



Versão britânica do resgate da polícia[5].

Na Europa, várias versões (o aparecimento do site) de resgates da polícia foram aparecendo gradualmente. A primeira versão foi registada no final de 2011, mostrando o endereço IP da ligação, a ligação ISP e o local [onde foi dado o endereço IP de um fornecedor de ligação específico (ISP)], se um utilizador tivesse a webcam ligada, era criada e exibida uma fotografia.



Resgate da polícia - a primeira versão na República Checa

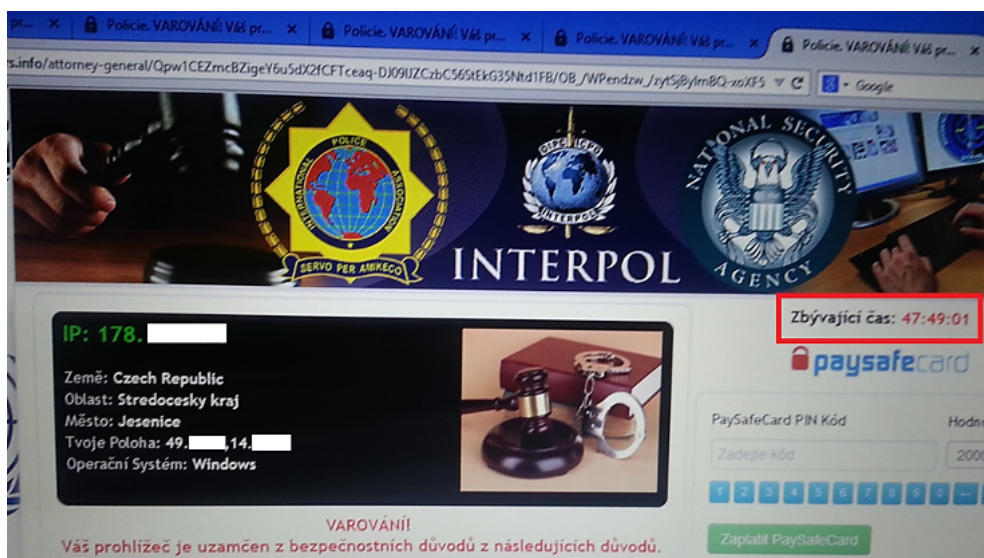
Versões mais recentes, para além de diferentes graficamente, também apresentavam a versão e o nome de utilizador do sistema operativo. A língua checa utilizada na página bloqueada também foi melhorada.



Resgate da polícia na República Checa - outras versões

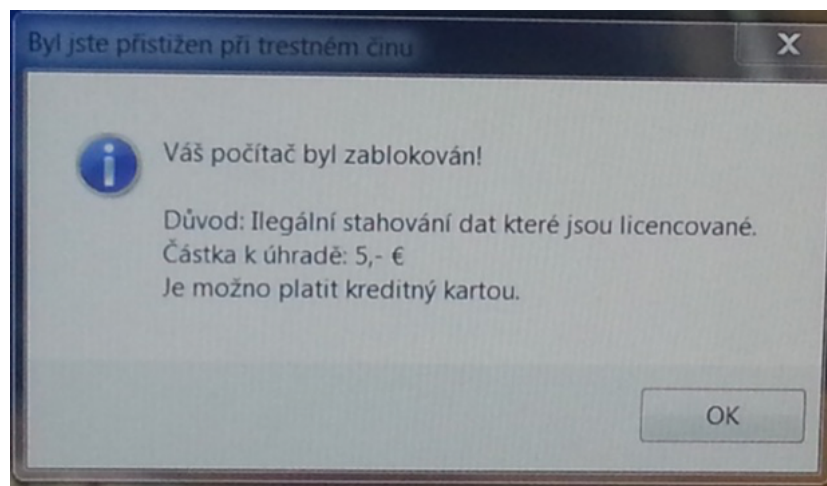
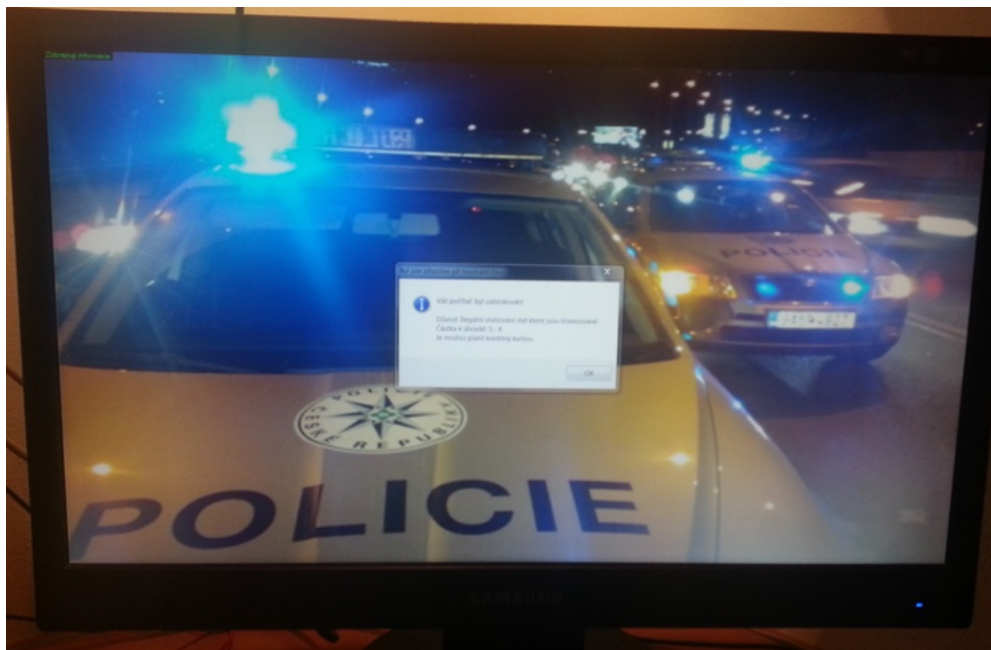
O "resgate policial" descrito acima experimentou a sua maior expansão em 2011-2013; contudo, outras variantes deste software malicioso apareceram com várias modificações mais tarde. Os ecrãs de impressão seguintes mostram as modificações do "police ransomware". Ambos os casos foram descobertos em 2015. O primeiro ecrã de impressão mostra um "ransomware" que bloqueia o browser dominante utilizado no computador infectado (enquanto outros browsers não foram infectados). O utilizador pôde utilizar todas as funções do sistema informático, excepto o programa de navegação infectado.

Para além das informações anteriormente mencionadas, é mostrada a posição GPS e o tempo restante até ao pagamento.



Resgate da polícia na República Checa (2015)

O segundo ecrã de impressão mostra um computador "bloqueado", enquanto que o software de resgate estava escondido na fenda de um jogo descarregado e instalado ilegalmente (neste caso, era um jogo Far Cry 4 descarregado de torrents checas).



Resgate da polícia na República Checa (2015)

Texto sobre a figura:

O seu computador foi bloqueado!

Motivo: Descarregamento ilegal de dados que são licenciados.

Montante a ser pago: 5,- €

É possível pagar com cartão de crédito.

Desde 2013, houve uma mudança significativa no caso do resgate de software. Os atacantes reduziram os ataques que consistiram em limitar a funcionalidade de todo o sistema informático, e concentraram-se principalmente no bloqueio de dados dos utilizadores. Os dados em discos locais, discos ligados dentro da rede informática e em todos os periféricos ligados (por exemplo, USB externo, HDD, etc.) são bloqueados. Os dados tornam-se um "refém", e quebrar a encriptação é quase impossível. Um dos primeiros resgates deste tipo foi o CryptoLocker (depois o CryptoWall, etc.).



CryptoLocker (2013)



Petya (2017)



Serviço de resgate móvel (2018)

Como parte das actividades de crime como serviço, o **resgate como serviço** tem sido oferecido desde 2016. Um utilizador (ou seja, um atacante) tem a oportunidade de definir o seu próprio "resgate" de acordo com as suas ideias. Ao mesmo tempo, é-lhe fornecido um conhecimento técnico sob a forma de servidores C&C, carteiras de bitcoin, suporte online 24/7, etc. Um exemplo de resgate como um serviço é o software **Ransom32**.



Ransomware (cliente)

Outras mudanças podem ser observadas nas actividades dos atacantes. Se for instalado um programa de resgate, este malware pode ser direccionado, por exemplo, para encriptar posições armazenadas em jogos, ou para "bloquear" televisões que utilizam o sistema operativo Android.^[6]

A prevenção e a resposta ao resgate podem ser resumidas nos pontos seguintes:

1. Imediatamente:

- Evitar sistemas de interligação que não sejam necessários
- Impedir a comunicação para a Internet, excepto quando necessário
- Alterar as palavras-passe das contas privilegiadas

2. Dentro de alguns dias:

- Mover cópias de segurança offline, verificar a funcionalidade das cópias de segurança
- Examinar os planos de continuidade de negócios e retirá-los dos sistemas
- Não apagar dados sobre incidentes de ciber-segurança
- Verificar indicadores de compromisso
- Alertar os empregados para o risco de phishing

3. No prazo de uma semana:

- Verificar se as cópias de segurança estão separadas para que mesmo um administrador privilegiado não as possa apagar
- Proibir a utilização de macros não assinadas, se possível.
- Verificar a segmentação da rede e o controlo entre segmentos
- Apertar as políticas de segurança das estações finais (proibição de executar aplicações não aprovadas, PowerShell não assinado...)
- Se a gestão da continuidade das actividades não for implementada - desenvolver planos de continuidade das actividades pelo menos para sistemas chave
- Instalar antivírus em todos os dispositivos relevantes
- Considerar a possibilidade de testar e implementar a actualização

4. Recomendações a longo prazo para resolver os ataques de resgate

- Formação regular do pessoal
- Segmentação significativa da rede
- Minimizar o uso de contas de administrador
- Cópias de segurança, testar regularmente as cópias de segurança, manter as cópias de segurança offline
 - o Regra 3 - 2 - 1 = Pelo menos 3 cópias em 2 dispositivos diferentes, 1 dos quais está fora da organização.
- Ter planos de continuidade de negócio (BCPs) e testá-los
- Verificar regularmente as aplicações acessíveis a partir da Internet e avaliar se ainda são necessárias

Possibilidades de sanções penais na República Checa

Na República Checa, é possível punir um ataque com malware, o qual é um resgate de acordo com a **Secção 230** (Acesso não autorizado a um sistema informático e a um portador de informação) do Código Penal. A **posse de malware, com a intenção de cometer uma infracção penal** nos termos da Secção 182 (Violação do sigilo das mensagens transportadas) ou uma infracção penal nos termos da Secção 230 do Código Penal, **é uma infracção penal nos termos da Secção 231** (Obtenção e posse de dispositivos de acesso e senhas de sistemas informáticos e outros dados deste tipo) do Código Penal.

No caso de resgate, é também possível aplicar as disposições do **artigo 230 (3)** do Código Penal, quando um agressor comete uma infracção penal deste tipo com a intenção de obter um benefício injustificado para si próprio ou para outro. A aplicação da Secção 175 (chantagem) do Código Penal também pode ser considerada, quando uma pessoa é obrigada a pagar um determinado montante ameaçando outros danos graves (por exemplo, ao ser apresentada com uma queixa criminal^[7]).

Possibilidades de sanções penais na Polónia

As leis que se aplicam na Polónia são as seguintes:

Arte. 267. Obtenção ilegal de informações

Arte. 269a. Interferência com o funcionamento de um sistema ou rede de informação ou de comunicação de dados

Possibilidades de sanções penais em Portugal

Como em quase todas as jurisdições, os ataques de resgates não são especificamente criminalizados. Contudo, tais acções podem ser perseguidas como extorsões (art. 223º do Código Penal). Uma alternativa, de uma perspectiva rigorosa do Cibercrime, seria a fraude informática (art. 221º do Código Penal), uma vez que o seu âmbito material é bastante amplo, seguindo a redacção do crime equivalente no texto da *Convenção de Budapeste* (art. 8º).

No entanto, outros crimes também estariam presentes, dependendo do *modus operandi* dos atacantes. Nomeadamente, por meios técnicos, sendo puníveis como acesso ilegal (Art. 6 da Lei de Crimes Cibernéticos), ou por *engenharia social*, com a inerente falsificação informática (Art. 3 da Lei de Crimes Cibernéticos).

Além disso, por si só, a encriptação dos dados da vítima equivaleria a sabotagem informática [interferência ilegal] (Art. 5 da Lei sobre o Cibercrime), de forma agravada se as infra-estruturas críticas ou serviços essenciais fossem perturbados (Art. 5(5)(b) da Lei sobre o Cibercrime).

Finalmente, se a decifragem não for possível, um Dano a programas informáticos ou outros dados informáticos [Interferência de dados] (Art. 4 da Lei de Cibercriminalidade) estaria em vigor.

[1] Por exemplo, Reventon, CryptoLocker, CryptoWall, Loky, Petya, Cerber, SamSam, JigSawetc. Para mais detalhes, ver, por exemplo

Ransomware. [online]. [cit.14.8.2016]. Disponível em: <https://www.trendmicro.com/vinfo/us/security/definition/ransomware>

[2] Muito frequentemente era um site com pornografia ou outro material sexual. Um utilizador podia também ser redireccionado para estas páginas a partir de outra página com uma "isca".

[3] A candidatura foi definida para "StayOnTop". Um utilizador não vê outras aplicações escondidas sob este "diálogo de resgate" e não é capaz de chamar o gestor de tarefas. O próprio Ransomware foi registado nos registos Run e RunOnce e efectuava uma verificação a cada 500 ms e escondia o gestor de tarefas no mesmo intervalo de tempo. A única outra aplicação em execução era a comunicação com o servidor C&C (mascarada no processo do navegador).

[4] *Resgate de bens da polícia*. [online]. [cit.14.8.2016]. Available from: https://www.f-secure.com/documents/996508/1018028/multiple_ransomware_warnings.gif/8d4c9ca2-fc77-433d-ac16-7661ace37f88?t=1409279719000

[5] [em linha]. [cit.14.8.2016]. Disponível a partir de: https://sophosnews.files.wordpress.com/2012/11/cool_ransom_uk_full.png

[6] Cf. por exemplo. *O novo Ransomware codifica os seus ficheiros de jogo*. [online]. [cit.14.8.2016]. Disponível a partir de: <https://techcrunch.com/2015/03/24/new-ransomware-encrypts-your-game-files/>

Android Ransomware agora também targeerts a sua Smart TV, Too! [online]. [cit.14.8.2016]. Disponível a partir de: <https://thehackernews.com/2016/06/smart-tv-ransomware.html>

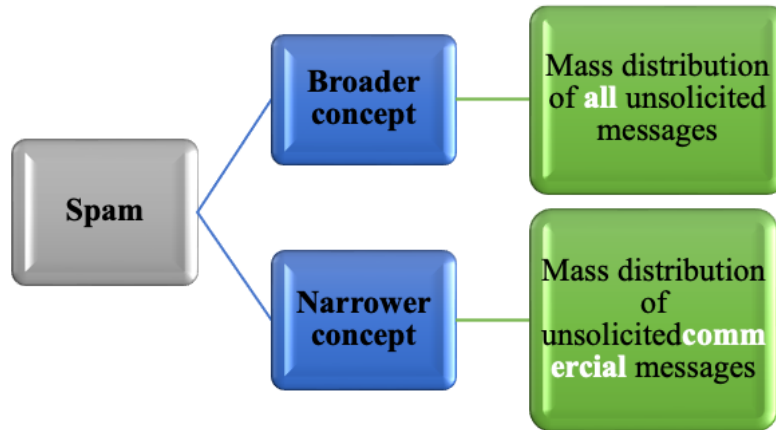
FLocker Mobile Ransomware Crosses to Smart TV. [online]. [cit.14.8.2016]. Disponível a partir de: <http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/>

[7] O conceito de outros danos severos, ver Stámaal, Pavel et al. *Trestní zákoník II. § 140 až 421. (Código Penal II. Secções 140 a 421). Komentář. (Comentário.)* 2ª Edição. Praga: C. H. Beck, 2012, pp. 1752-1753

Especificamente, "*uma ameaça de outros danos graves pode consistir numa ameaça de danos materiais, danos graves à honra ou reputação, etc. Outro tipo de dano grave pode consistir no início de um processo penal em resultado da denúncia de um crime pelo qual o perpetrador ameaça a parte lesada, forçando-a a fazer, negligenciar ou tolerar algo. Ao mesmo tempo, é indeciso se a parte lesada cometeu um crime, cuja notificação é ameaçada ou não (cf. R 27/1982).*"

4.5. Spam

Do ponto de vista das tecnologias de informação e comunicação, o conteúdo do termo spam pode, em princípio, ser compreendido a dois níveis. Num **sentido restrito**, é a difusão em massa de comunicação não solicitada, na maioria das vezes de natureza publicitária através da Internet, e na maioria das vezes através da comunicação electrónica. Num **sentido lato**, todas as mensagens não solicitadas recebidas, ou seja, também mensagens contendo vírus, cavalos de Tróia, etc.^[1] são spam.



Esquema - Divisão de spams

É característico do spam ser uma **mensagem** que é **enviada electronicamente, em massa e especialmente sem pedido**.

O spam utiliza vários canais de comunicação para enviar mensagens não solicitadas:

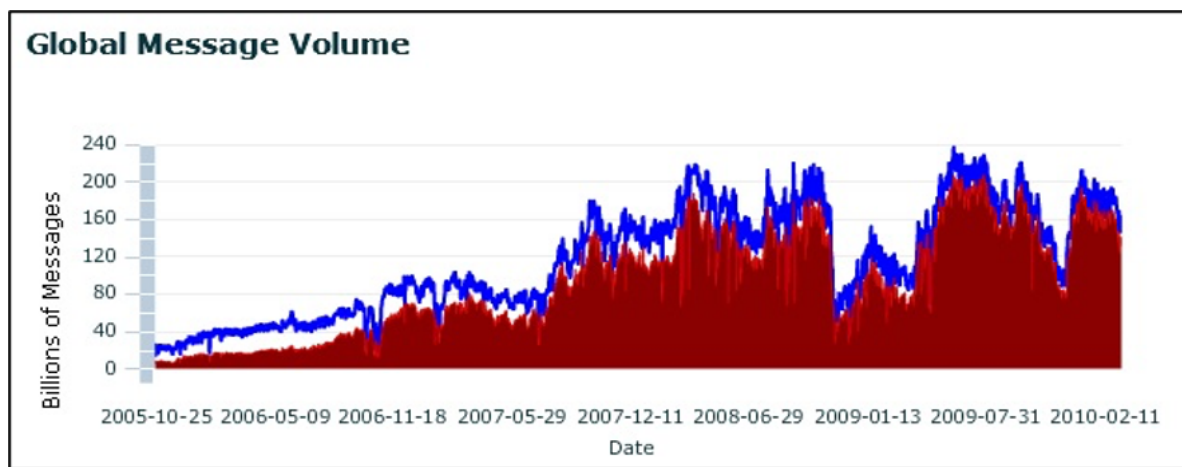
- e-mail;
- outro mensageiro (ICQ, Skype, etc.);
- SMS, MMS;
- fóruns de discussão, blogs, redes sociais, etc..;
- plataformas de jogo, etc.

O Spam pode conter informação:

- **comercial ou publicitário;**
- **sobre saúde e medicina** (Esta categoria inclui spam que oferece produtos de perda de peso, cosméticos, medicina não tradicional, medicamentos não disponíveis na região, etc.);
- **financeiros** (em particular, são ofertas de vários empréstimos, a possibilidade de rendimentos extra, etc.).);
- **pornográfico** (Este spam ou oferece vários produtos farmacêuticos para aumentar a potência sexual, ou links para sites com conteúdo pornográfico.);
- **educacional** (ofertas de vários cursos, formações, etc.);
- **embuste** (carta em cadeia);
- **político;**
- **religioso;**
- **criminal (esta categoria inclui mensagens contendo, por exemplo, malware, ou ligações a sites com código malicioso, etc.)**

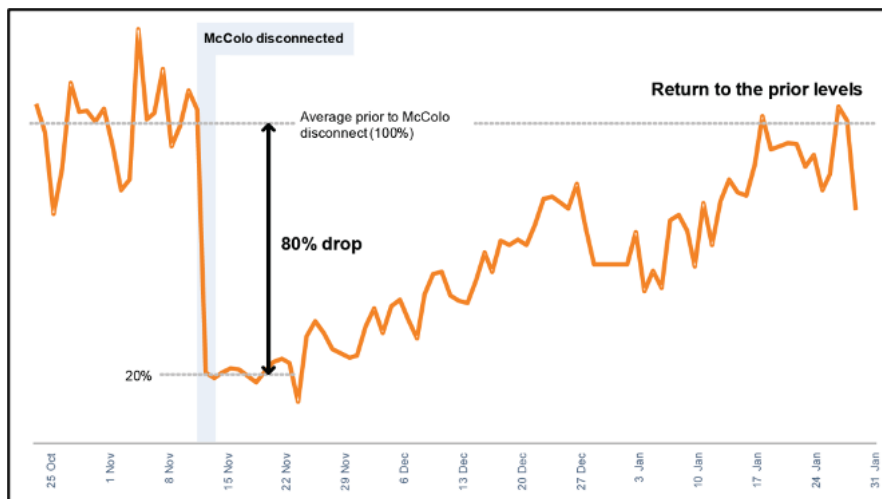
Existe actualmente um grande número de estatísticas que mostram diferentes números de spam em e-mails. Por exemplo, Jirovský afirma que mais de 90% do spam no correio electrónico pode ser esperado. Em 2006, foi enviada uma média de 14,5 mil milhões de mensagens de spam por dia.^[2] Devido a este facto, surgiram muitas organizações que lidam com spam e fornecem ferramentas de protecção contra o mesmo. Uma destas empresas foi a Trusted Source^[3], de onde provém o seguinte gráfico. Ele mostra a parte de spam em e-mails de 2005 a 2010. A linha azul mostra o número de mensagens de correio electrónico, e o campo vermelho reflecte o número de spams de correio electrónico (ambos são dados em milhares de milhões).

Independentemente das percentagens exactas, este tipo de mensagens não solicitadas constitui actualmente a maioria de todas as mensagens de correio electrónico recebidas.^[4] No entanto, devido a uma série de medidas técnicas por parte de cada ISP, o utilizador recebe um mínimo de mensagens que representam spam.



Desenvolvimento de Spam de 2005 a 2010

A queda significativa do spam no final de 2009 deve-se ao encerramento do negócio de spam na Internet do **McColo**.^[5]

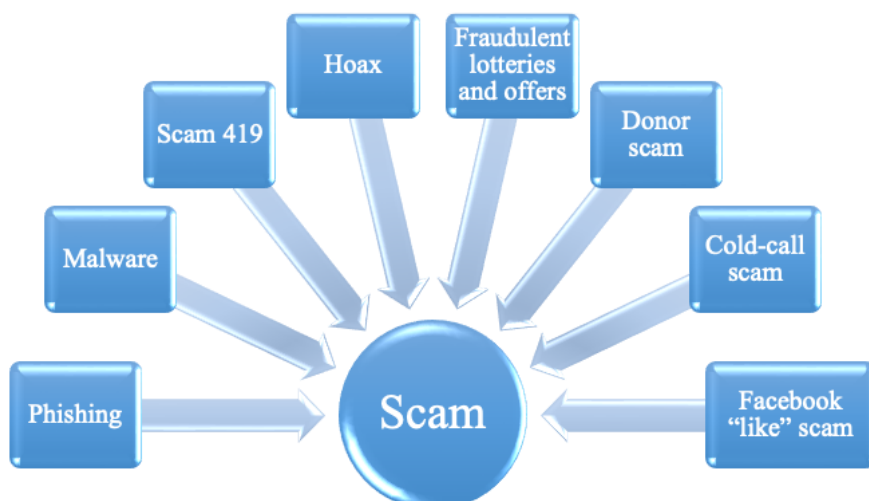


Desenvolvimento do spam após o McColo ter cessado as operações em Novembro de 2008

O spam interfere com a comunicação electrónica, muitas vezes tornando-a completamente impossível (a estrutura de informação é sobrecarregada) e reduzindo assim a confiança da sociedade nas tecnologias de informação. No entanto, se o spam for restringido, o direito à liberdade de expressão é praticamente restringido em favor do direito à protecção da integridade pessoal.

Mesmo pela razão acima descrita, a sanção legal de um spammer é bastante complicada e actualmente são utilizados os institutos de direito civil e administrativo, uma vez que o direito penal não permite punir um spammer.

O spam contendo conteúdo criminoso ou outro conteúdo fraudulento é referido como **fraude**. As burlas constituem actualmente uma parte significativa do spam e o seu objectivo é, tipicamente utilizando engenharia social, ganhar a confiança de um utilizador e forçá-lo a realizar algumas acções necessárias (por exemplo, abrir um anexo de e-mail, visitar o URL exibido, etc.). As burlas incluem *phishing*, *malware*, *419*, *hoax*, *lotarias* e *ofertas fraudulentas*, *burla de doadores*, *burla de chamadas a frio*, *burla no Facebook* como a *burla*, etc.



Tipos de esquema de esquema fraudulento

Nesta altura, concentrar-me-ei principalmente em três tipos de esquema, nomeadamente o **Esquema 419**, **Hoax** e **Fraudulent Offers**.

4.5.1. Esquema 419

O esquema 419 é uma designação para e-mails, mais conhecido como **cartas nigerianas**. Estas burlas são um exemplo da transmissão do crime normal (fraude) do mundo real para o mundo virtual.

Por uma questão de interesse, apresentamos três relatórios muito diferentes com a natureza do esquema 419.

Relatório Nº 1 - "Herdou uma enorme quantidade de dinheiro".

Olá, querida,

Sou uma advogada Victoria Josef, tenho uma mensagem para si sobre o meu cliente falecido que tem o mesmo apelido que você, estou ciente, pode não estar relacionado com o seu sangue, mas é uma cidadã do seu país que perdeu a sua vida ao lado da sua família imediata durante um acidente aqui no motor do Togo.

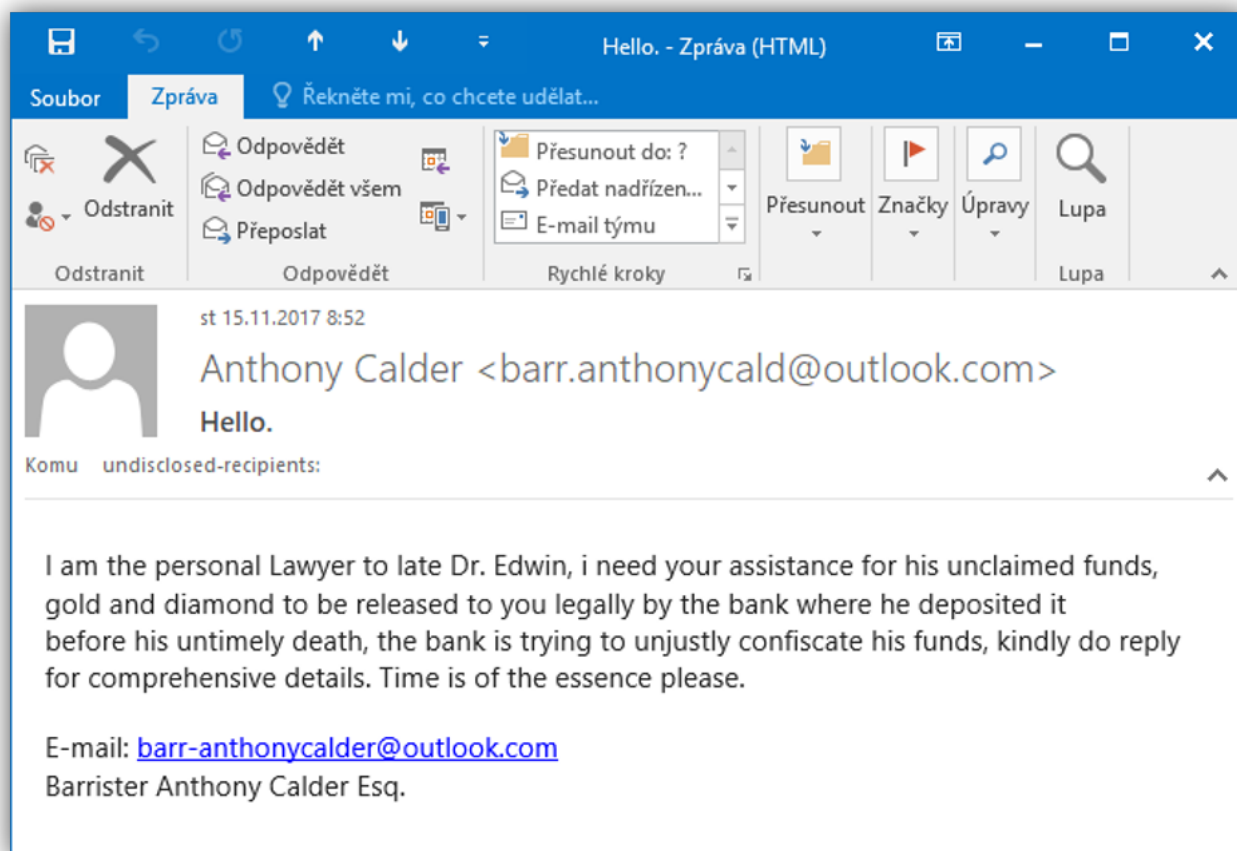
Partiu por um montante de \$ 2,700,000, entretanto, o seu banco quer transferir os benefícios para um dos membros da sua família alargada, uma vez que a apresentação pode ser feita através do meu escritório. Para ser honesto, este dinheiro pertence ao meu cliente falecido, que tem o mesmo apelido e nacionalidade que viveu consigo e trabalhou aqui no Togo durante mais de 20 anos como empreiteiro, mas morreu num acidente de carro fatal juntamente com todos os membros da sua família em 2009 e, recentemente, o banco onde este dinheiro está armazenado deu-me um mandato para fornecer algum membro da sua família para exigir este dinheiro ou então será passado para a conta do tesouro do governo como dinheiro abandonado.

Não quero que isso aconteça, mas o problema é que os seus supostos familiares mais próximos morreram neste mesmo acidente de carro e todos os seus esforços para localizar os seus familiares desde a sua morte não tiveram sucesso em disputar quando nunca me apresentou alguns deles enquanto estava vivo.

Amigo, foi por isso que embarquei nesta missão para encontrar alguém para trabalhar de mão em mão comigo reclamando este fundo para ajudar as nossas famílias e os necessitados, em vez de permitir que estes funcionários corruptos do governo tomassem conta deste dinheiro tão arduamente ganho, sem mais nem menos, e o espalhassem, deixando as massas pobres a sofrer. Para mim, para vos apanhar entre os milhões de pessoas no Facebook; só quer dizer que foi Deus que nos perturbou o caminho, por isso vamos trabalhar em conjunto com uma mente enquanto partilhamos o dinheiro da forma como ele o reivindicou.

Por favor, indique o seu interesse nesta declaração para que eu lhe possa fornecer no que diz respeito a trabalho e orientações.

Advogada Victoria Joseph Esq.



Mensagem nº 2 - "Apaixonei-me"

Olá querida,
O meu nome é Joe Anita
Sou uma mulher, descobri a sua identidade de lado, e quero aprender que sabemos
mais um sobre o outro e partilhamos a vida social com a cultura, e não tenho
nada a dizer, por isso, por favor, responda-me, por isso envio-lhe os meus dados
e direi mais sobre mim nos meus quadros. Muito obrigado.
A sua alegria Anita



ne 05.06.2016 21:29

MojzeszlGAnselm@gmail.com

You love sports and girls wish to meet a man.

Komu MojzeszlGAnselm@gmail.com

V této zprávě byly odebrány nadbytečné konce řádků.



hfrij3hfk.jpg
23 KB

Hi, my name is Narmina I'm a girl from Azerbaijan. Azerbaijan It's an independent country, you can find it on maps.

I find your address in dating marriage agency. This service is in our town. This is a dating agency has many connections with most online dating sites, and they have a common list of the forms and e-mail addresses. I come to this agency, pay some money and they give me your e-mail address.

So I very much hope that you will answer my letter soon.

I'm very interesting, soft and tender girl. But I'm very lonely in my life. I want to find good man for serious relations.

I'm ready to spend all my life with such man! I hope you like my picture, I send you with this letter.

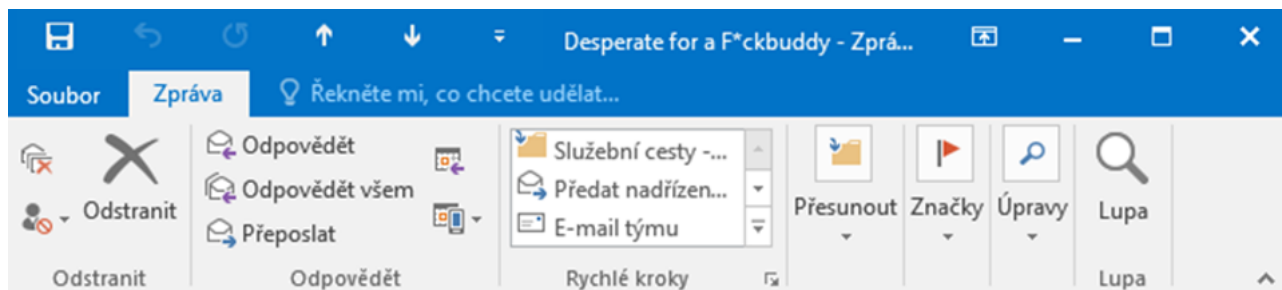
And if you still free from serious relations, just let me know and send the answer, may be it's our chance to escape from loneliness.

I would like to see yours picture also, and find out more about you.

Looking forward for your answer.

Narmina

Mensagem n.º 3 - "Sexo instantâneo"



pá 15.07.2016 16:01

Bryony Roark <Roark_Jayda@e.amexpub.com>

Desperate for a F*ckbuddy

i'm so hungry for s*x that i will do anything for it!

you can just f*ck me and leave, i dont mind ;)

r u ready? my wet pu**y is waiting...

my username is SkankiSlut7, look at my n3w plcs [***here***](#)



5 engines detected this URL

URL <http://6url.ru/iWTI>
Host 6url.ru
Downloaded file [c0b6418dce31ded4e3408dc1d7857ca315f0197804ba94780b87084381062168](#)
Last analysis 2016-07-11 08:35:44 UTC
Community score -7

5 / 68

Detection

Details

Community

Avira

Malware

BitDefender

Phishing

CLEAN MX

Phishing

Dr.Web

Malicious

Fortinet

Malware

Websense ThreatSeeker

Suspicious

ADMINUSLabs

Clean

AegisLab WebGuard

Clean

AlienVault

Clean

Antiy-AVL

Clean

Mensagem Nº 4 - Um astronauta nigeriano foi esquecido no espaço e precisa de regressar a casa

A notícia começou a espalhar-se em 2004, altura em que o "primeiro astronauta africano" se encontrava no espaço há 14 anos sem uma pausa. É de notar que a duração da sua estadia ultrapassou todos os tempos dos astronautas (talvez no total). Recebi a última versão deste Esquema 419 em 2016. Embora lamente muito por este astronauta imaginário (26 anos no espaço e sozinho), não pretendo certamente contribuir para os autores de fraudes. Infelizmente, apesar do conteúdo completamente inútil e da informação não fundamentada contida neste e-mail, há um grande número de pessoas que querem ajudar uma pessoa necessitada (graças a esta ajuda, este esquema poderia ser incluído no grupo de *doadores do esquema*).

Subject: Nigerian Astronaut Wants To Come Home
Dr. Bakare Tunde
Astronautics Project Manager
National Space Research and Development Agency (NASRDA)
Plot 555
Misau Street
PMB 437
Garki, Abuja, FCT NIGERIA

Dear Mr. Sir,

REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL

I am Dr. Bakare Tunde, the cousin of Nigerian Astronaut, Air Force Major Abacha Tunde. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989. He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progrez supply flights to keep him going since that time. He is in good humor, but wants to come home.

In the 14-years since he has been on the station, he has accumulated flight pay and interest amounting to almost \$ 15,000,000 American Dollars. This is held in a trust at the Lagos National Savings and Trust Association. If we can obtain access to this money, we can place a down payment with the Russian Space Authorities for a Soyuz return flight to bring him back to Earth. I am told this will cost \$ 3,000,000 American Dollars. In order to access the his trust fund we need your assistance.

Consequently, my colleagues and I are willing to transfer the total amount to your account or subsequent disbursement, since we as civil servants are prohibited by the Code of Conduct Bureau (Civil Service Laws) from opening and/ or operating foreign accounts in our names.

Needless to say, the trust reposed on you at this juncture is enormous. In return, we have agreed to offer you 20 percent of the transferred sum, while 10 percent shall be set aside for incidental expenses (internal and external) between the parties in the course of the transaction. You will be mandated to remit the balance 70 percent to other accounts in due course.

Kindly expedite action as we are behind schedule to enable us include downpayment in this financial quarter.

Please acknowledge the receipt of this message via my direct number 234 (0) 9-234-2220 only.

Yours Sincerely, Dr. Bakare Tunde
Astronautics Project Manager
tip@nasrda.gov.ng

<http://www.nasrda.gov.ng/>

Devido à natureza da fraude, seria possível, em alguns casos, rotular ou subordinar o esquema 419 a actos que tenham a natureza de phishing.

4.5.2. Hoax

Um embuste (uma ficção, uma partida, um boato de imprensa) é outra forma de spam ou fraude. O rótulo "embuste" é utilizado para mensagens em cadeia (como por exemplo: "*passem-na*", "*se não a enviar a outras 20 pessoas... acontece*", etc.), que contêm informações distorcidas, falsas, enganosas ou outras informações falsas. Um embuste contém frequentemente avisos sobre ataques, descrições de perigos, pedidos de ajuda, chamadas, petições, declarações de celebridades, cartas em cadeia de felicidade, mensagens engraçadas, imagens e vídeos em apresentações, brincadeiras com gatos e outros animais, etc.

4.5.3. Ofertas fraudulentas

Uma forma muito bem sucedida de esquema é várias ofertas fraudulentas, que podem ser enviadas em massa ou de uma forma direccionada. Actualmente, tais ofertas são enviadas não só através de e-mails, mas também através de quaisquer mensageiros instantâneos, redes sociais, portais de leilões, etc.

No que respeita à **distribuição em massa** de ofertas fraudulentas, é possível imaginar uma série de actividades sobre o princípio de "pirâmide" ou "avião", ofertas de trabalho vantajoso a partir de casa^[6], métodos "garantidos" de valor para o dinheiro (com as taxas de juro mais elevadas), ofertas de empréstimo (com as taxas de juro mais baixas), "grandes" oportunidades de emprego, etc.

O **envio direccionado** de ofertas fraudulentas deve também incluir uma conduta que não seja meramente spam, mas que seja, por exemplo, uma combinação de licitação sobre um tipo específico de bens dentro de portais de leilões e subsequente comunicação com utilizadores que tenham aceite esta licitação. Estas são as chamadas "fraudes em leilão".

NAJRÝCHLEJŠIE RASTÚCE PODNIKANIE Z DOMOVA VO SVETE!

POĎTE NA PREHLIADKU ZADARMO!



PÁČILO BY SA VÁM ZARÁBAŤ VIAC AKO 8.847,00 \$ ZA MESIAC PRÁCOU Z DOMU?

STIFORP CZECH

TISÍCE OBYČAJNÝCH LUDÍ SI ZARÁJ SLUŠNÉ ŽIVOBYTÍ

PRÁVE TERAZ MÁTE PRÍSTUP ZADARMO!

Stačí vyplniť krátky formulár na tejto strane a môžete sa vydať na cestu k finančnej stabilite

MENO

PRIEZVISKO

TELEFÓN

E-MAIL

POTVRDIETE

Irresistível oferta de trabalho a partir de casa (distribuição em massa dentro da rede social Facebook)

Actualmente, já não é certamente a regra que as ofertas em massa ou dirigidas são escritas em checo suspeito ou quebrado (ou são escritas em inglês ou russo), pelo contrário, o esforço de um agressor é convencer uma vítima de absoluta correcção, seriedade e "honestidade" das suas acções. Portais de leilões oferecem, muitas vezes de forma fraudulenta, vários tipos de electrónica, especialmente telemóveis e computadores. A verdadeira fraude pode então consistir, por exemplo, na alteração de informação essencial [por exemplo, país de origem do telemóvel; informação de que se trata de uma cópia (falsificação) do telefone] ou na não entrega da mercadoria enquanto tal. (O atacante solicita muito frequentemente o pagamento do montante total ou adiantamento).

A imaginação dos atacantes é considerável no ambiente da Internet, e no caso de quaisquer ofertas, anúncios, e especialmente o envio de adiantamentos ou pagamentos, é aconselhável ser paranóico e não confiar em pessoas desconhecidas.

No caso de ofertas fraudulentas, quando um agressor tenta obter vários adiantamentos ou outros pagamentos adiantados, tal conduta pode ser punida de acordo com a **Secção 209** (Fraude) do Código Penal.

Possibilidades de sanções penais na República Checa

No que diz respeito à sanção penal de spam e spammers, esta não está actualmente totalmente (re)resolvida na República Checa. Não existe protecção legal nacional ou internacional contra este comportamento indesejável. Mesmo a Convenção sobre o Cibercrime não inclui a definição de spam como um delito criminal.

Por exemplo, nos **EUA**, os spammers^[2] foram condenados por enviar spam no passado. Por exemplo, **Jeremy Jaynes** foi condenado em 2007 por um tribunal da Virgínia a 9 anos de prisão. Foi acusado em 2003, como evidenciado por 53.000 spams enviados no prazo de três dias. No entanto, o procurador disse acreditar que Jaynes era responsável pelo envio de mais de 10.000.000 de spams por dia, o que lhe deveria ter valido aproximadamente 750.000 dólares por mês.

Devido ao facto de apenas uma forma de conduta prejudicial não poder ser incluída no termo spamming, é muito difícil punir o spamming ao abrigo do direito penal. Isto só pode ser feito para os seus tipos individuais. Em certos casos, é possível punir a recolha de endereços de correio electrónico se essa recolha satisfizer os elementos objectivos da infracção penal de tratamento não autorizado de dados pessoais ao abrigo da **Secção 180** (Tratamento não autorizado de dados pessoais) do Código Penal. Se o spam contiver malware ou se destinar a cometer fraude, é possível punir as actividades de um spammer de acordo com as disposições relativas a malware ou phishing.

Possibilidades de sanções penais na Polónia

Na Polónia, o envio de informação comercial não solicitada por meios de comunicação electrónicos é considerado uma infracção e está sujeito a uma multa. Isto é regulamentado pelo Acto de 18 de Julho de 2002 sobre a prestação de serviços electrónicos (Diário Oficial de 2002 n.º 144, item 1204):

Arte. 24. 1. Quem enviar, por meio de comunicação electrónica, informações comerciais não solicitadas, está sujeito à pena de multa.

(2) A acusação da infracção, referida na secção 1, deve ocorrer a pedido da parte lesada.

Artigo 25 Os julgamentos em casos relacionados com as infracções especificadas nos artigos 23º e 24º serão conduzidos em conformidade com as disposições sobre processos em casos de infracções menores.

Possibilidades de sanções penais em Portugal

Também em Portugal, em termos gerais, o spam em si não é considerado como um crime. No entanto, seguindo a Arte. 14(1)(f)(g)(h)(i)(j) da Lei n.º 41/2004, sobre protecção de dados e privacidade nas comunicações electrónicas, os spammers para fins comerciais devem pagar multas administrativas, desde um mínimo de 1500 euros até um máximo de 5000000 euros.

Contudo, como excepção, sendo o conteúdo de mensagens no âmbito da Lei n.º 52/2003, sobre a luta contra o terrorismo, pode ser considerado como uma infracção penal (arts. 2 e 4).

[1] Para classificar spam, cf. forexample GONZÁLES-TALAVÁN, Guillermo. Um filtro SMTP Anti-spam simples e configurável: Greylists. *Computers & Security*, 2006, vol. 25, No. 3, pp. 229-236.

[2] Cf. por exemplo: *Estatísticas de Spam*. [em linha]. [cit.14.8.2016]. Disponível a partir de: <https://www.spamcop.net/spamstats.shtml>

Estatísticas e Fatos sobre Spam. [online]. [cit.14.8.2016]. Disponível em: <http://www.spamlaws.com/spam-stats.html>

[3] Fonte online original:<http://www.trustedsource.org/TS?do=homehttp://spam-filter-review.toptenreviews.com/spam-statistics.html> [cit.12.2.2010].

[4] Não é possível determinar exactamente que percentagem de todos os e-mails são spam. As diferentes fontes disponíveis dão números diferentes, por vezes muito diferentes. Por exemplo, um dos fornecedores de soluções anti-spam, POSTINI, registou em Março de 2005, no espaço de 24 horas, que 10 das 12 mensagens de correio electrónico eram spam. A frequência do envio de spam, cf. p. ex. LANCE, James. *Phishing bez záhad*. Praga: Grada, 2007, p. 22, SCHRYEN, Guido. The Impact that Placing Email Addresses on the Internet Has on the Receipt of Spam: An Empirical Analysis (O Impacto que a Colocação de Endereços de Correio Electrónico na Internet Tem na Recepção de Spam: Uma Análise Empírica). *Computers & Security*, 2007, vol. 26, No. 5, pp. 361-372.

[5] *Malware, mayhem, e a tomada de McColo*. [em linha]. [cit.14.8.2016]. Disponível a partir de: <http://betanews.com/2008/11/13/malware-mayhem-and-the-mccolo-takedown/>

[6] Por um lado, estas ofertas podem consistir de um pedido como por exemplo: "envie-nos \$10 para a nossa conta e enviar-lhe-emos instruções sobre como ganhar \$8.847 por mês." A segunda possibilidade é que estas ofertas de emprego não requerem qualquer taxa prévia, apenas requerem o registo do utilizador. Ao registar-se, um atacante recebe dados pessoais sobre um utilizador. Um e-mail desta empresa, contendo, por exemplo, malware, etc., pode então ser enviado para o endereço de e-mail do utilizador.

[7] *Condenado spammer a desafiar a lei Va*. [online]. [cit.14.8.2016]. Disponível a partir de: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htm

Top Spammer Sentenciado a Quase Quatro Anos. [online]. [cit.14.8.2016]. Disponível a partir de: <http://www.pcworld.com/article/148780/spam.html>

Buffalo Spammer jde na 7 let za mříže kvůli rozesílání nevyžádané pošty. [online]. [cit.14.8.2016]. Disponível a partir de: http://technet.idnes.cz/buffalo-spammer-jde-na-7-let-za-mrize-kvuli-rozesilani-nevyzadane-posty-13i-/tec_reportaze.aspx?c=A040528_28629_tec_aktuality

4.6. Phishing, Pharming, Spear Phishing, Vishing, Smishing

4.6.1. Phishing

O termo phishing é mais frequentemente referido como conduta fraudulenta ou enganosa, cujo objectivo é obter informações sobre um utilizador, tais como nome de utilizador, palavra-chave, número de cartão de crédito, PIN, etc.

Num **sentido restrito**, o phishing é uma acção que requer que um utilizador visite um site fraudulento (exibindo, por exemplo, um site bancário na Internet, loja online, etc.) e depois preencha "informação de login", ou esta informação é necessária directamente (por exemplo, ao preencher um formulário, etc.).

Num **sentido lato**, o phishing pode ser definido como qualquer conduta fraudulenta destinada a inspirar confiança num utilizador, reduzir a sua vigilância ou forçá-lo a aceitar um cenário preparado antecipadamente por um atacante. Neste sentido lato, o utilizador já não é obrigado a preencher os dados, mas recebe uma mensagem (ou o utilizador é redireccionado para uma página) tipicamente contendo malware que recolhe os dados. Além disso, os esquemas de doadores, etc., podem ser incluídos neste sentido mais lato.

Em ambos os casos, um utilizador que é alvo de um ataque de phishing é enganado. A diferença reside principalmente no grau de interacção exigido ao utilizador.

O Phishing na sua essência é a utilização da engenharia social. O phishing também pode ser feito no mundo real (ver esquemas, etc.), mas o mundo virtual permite que um atacante envie mensagens fraudulentas a um enorme número de potenciais vítimas com um esforço mínimo. Phishing pode, com muito exagero, ser comparado ao "*bombardamento de tapetes*". Tal como nos bombardeamentos, o phishing visa um número relativamente indeterminado de vítimas para que um atacante tenha esperança de sucesso. Por exemplo, em 2014, o Google declarou que um esquema com phishing realmente bom tem uma taxa de 45% de sucesso na obtenção de dados de utilizadores.^[1]

O phishing não é apenas uma questão de e-mails. É possível encontrar phishing em mensagens instantâneas (Skype, ICQ, Jabber, etc.), redes sociais, mensagens SMS e MMS, salas de chat, fraudes (ofertas fraudulentas de emprego ou bens, etc.), falsas aplicações de browser^[2], etc.

Phishing num sentido restrito

O princípio de um ataque "*clássico*" de phishing consiste mais frequentemente no envio do chamado e-mail de phishing a uma parte lesada, o que, à primeira vista, não levanta qualquer suspeita de que se trate de uma mensagem fraudulenta. Um tal e-mail inclui normalmente um link que um utilizador é levado a clicar.

Depois de clicar no link em anexo, o utilizador chega a um website fraudulento, o que é quase impossível de distinguir em termos de aparência e função da caixa web original correcta. Se for uma imitação de um sítio web, através do qual é possível fazer pagamentos, aceder a contas seguras, gerir tais contas, etc., então os dados introduzidos pelo utilizador são automaticamente enviados para o agressor.^[3] Desta forma, o atacante pode obter dados de identificação de utilizadores de serviços bancários na Internet, acesso a contas bancárias individuais de utilizadores de sistemas infectados, números de identificação e outros dados em cartões de pagamento com a ajuda dos quais é então possível efectuar pagamentos no ambiente da Internet, etc.

Um verdadeiro ataque de phishing tem lugar em várias etapas.^[4]

1. Planeamento de um ataque de phishing

Nesta fase de um ataque de phishing, é seleccionado um alvo (grupo de utilizadores) e o método a ser utilizado para o ataque é seleccionado. É avaliado o tipo de segurança técnica que o alvo utiliza, quais são os riscos de o atacante revelar a sua identidade, etc.

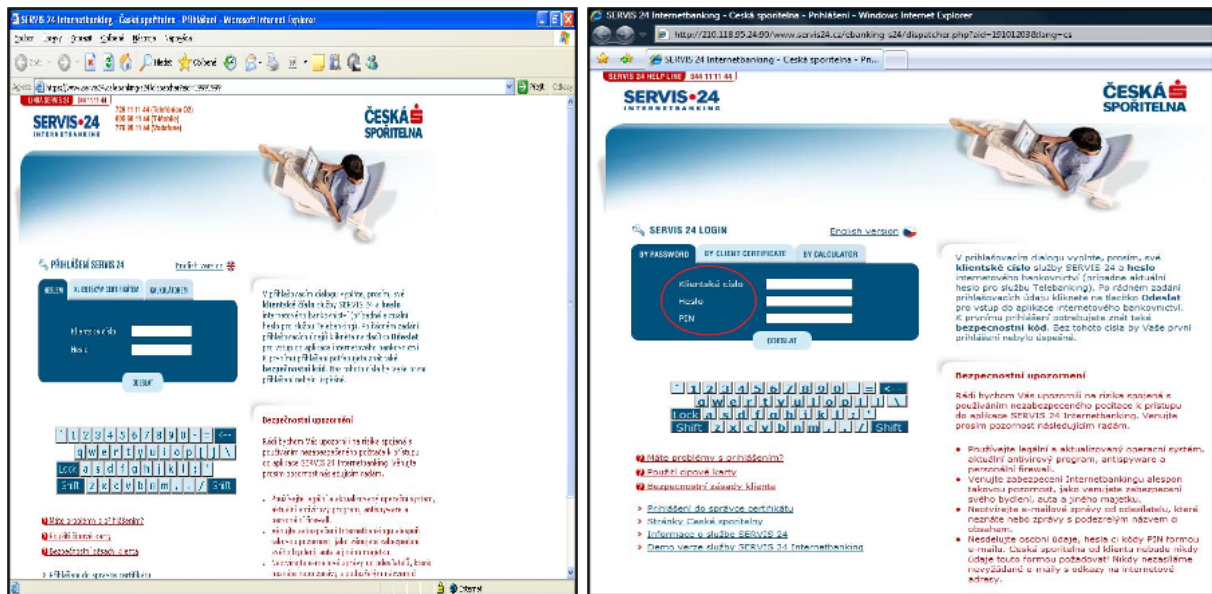
2. Criação de condições para um ataque de phishing

Nesta fase, está a ter lugar uma solução técnica para um ataque de phishing. Um atacante obtém listas de endereços de correio electrónico de utilizadores a quem deve ser enviado um correio electrónico de phishing, é criada uma caixa de dados, onde o sistema envia os dados de utilizador adquiridos, é criada uma mensagem de confiança, que é depois distribuída aos utilizadores.

3. Ataque de Phishing

Um e-mail de phishing é entregue a utilizadores individuais e, dependendo da qualidade de processamento deste e-mail e de outros factores (experiência do utilizador, sensibilização do utilizador para questões de phishing, software anti-phishing do alvo, etc.), os dados são enviados para a caixa de dados do atacante. Nesta fase de um ataque de phishing, o utilizador encontra pela primeira vez um e-mail de phishing.

Como pretexto, é frequentemente utilizada informação sobre um bug no sistema de segurança da empresa ou outro aviso, o que deve fazer com que o utilizador confie na autenticidade desta mensagem. Após activar o link interactivo, a pessoa é redireccionada para um website criado pelo agressor, copiando fielmente a página original da instituição financeira. O utilizador é solicitado a preencher os detalhes de login, geralmente incluindo o número do cartão e o código PIN. Os dados preenchidos são enviados para o endereço do phisher, que então retira alguns ou todos os fundos da conta, causando assim uma perda para o cliente (ver a figura seguinte).



Página original (esquerda) e página fraudulenta (direita)

4. Recolha de dados

O atacante obtém dados que foram introduzidos por utilizadores individuais do sistema comprometido num ambiente de site falso.

5. Retirada de fundos ou outros lucros de um ataque de phishing

Utilizando os dados obtidos, o atacante entra nas contas bancárias reais de utilizadores individuais e retira fundos. Ao transferir para outras contas, especialmente estrangeiras, diluindo estes fundos e utilizando outras técnicas, os fundos levantados tornam-se praticamente indetectáveis.

É muito difícil determinar quantos ataques de phishing são levados a cabo em todo o mundo todos os dias. É também problemático determinar quantos clientes de empresas comprometidas respondem a um e-mail de phishing. A taxa de retorno é estimada entre 0,01 e 0,1%.

As previsões em 2007 estimavam que os esquemas ou campanhas "clássicas" de phishing iriam aumentar no futuro.^[5] Estas previsões foram cumpridas em parte, uma vez que o número de campanhas "clássicas" de phishing está a diminuir, mas o phishing em sentido lato está a aumentar^[6], especialmente as suas novas modificações ou ligando o phishing a outros tipos de ataques (malware, botnet, etc.).

Phishing em sentido lato

Como parte da demonstração de phishing em sentido lato, apresentarei quatro campanhas que tiveram lugar na República Checa e foram mais ou menos bem sucedidas. É claro que estes ataques não são os únicos ataques de phishing em sentido lato que tiveram lugar na República Checa. A razão para escolher estes quatro ataques específicos é o facto de eu querer salientar em particular a abordagem inovadora do atacante e a combinação apropriada de ataque técnico com engenharia social. Especificamente, os ataques são:

1. Dívida/Banco/Execução
2. Correio Checo (Česká pošta)
3. Natal e prendas
4. Seznam.cz - Palavra-passe única

4.6.1.1. Dívida/Banco/Execução^[7]

Uma campanha de phishing chamada profissionalmente DBE atingiu a República Checa em grande escala em 2014 (com as reverberações desta campanha a durar pelo menos até ao final de 2015). O ataque em si foi preparado com muita precisão e incluiu tanto um phishing como uma distribuição de malware (para computadores e dispositivos móveis). Todo o ataque pode ser dividido nas seguintes fases:

1. Campanha de Phishing
2. Instalação de malware num computador
3. Acesso à banca em linha
4. Instalação de malware para um dispositivo móvel
5. Transferência e levantamento de fundos

Anúncio 1) Campanha de Phishing

O primeiro pré-requisito para que os atacantes pudessem obter dinheiro com sucesso foi uma grande campanha de phishing à qual um número suficiente de pessoas responderia. A distribuição efectiva de e-mails fraudulentos foi dividida em três ondas sucessivas de mensagens de phishing:

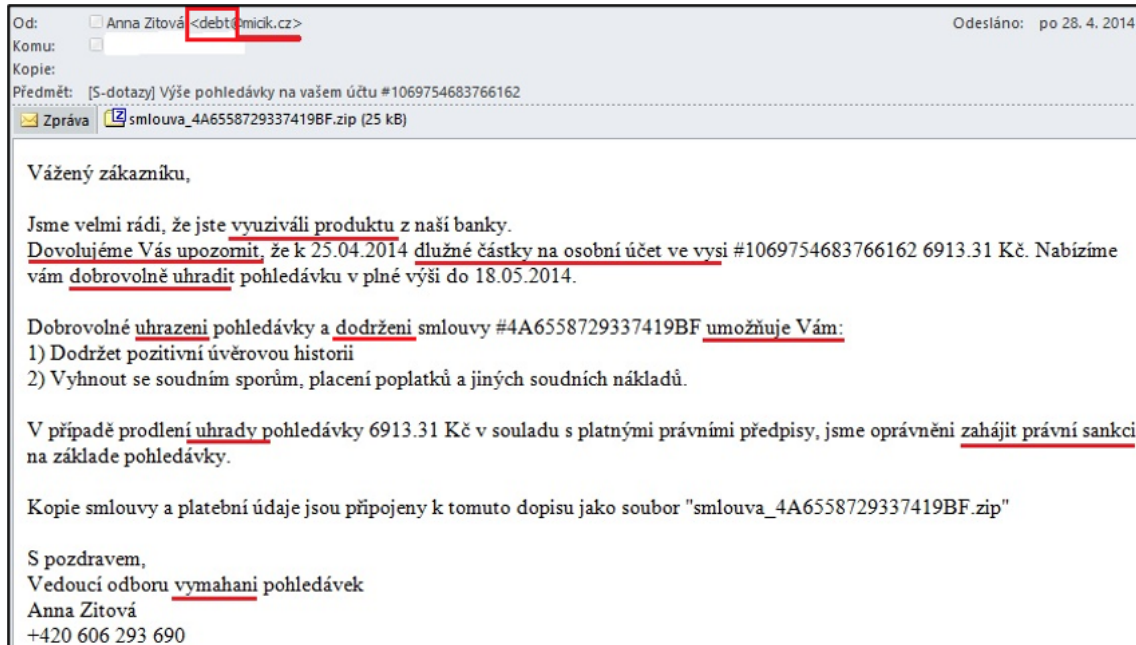
- I. Dívida (debt@....); Março-Abril de 2014

II. Banco (bank@...); Maio-Junho de 2014

III. Execução (emissões@...); Julho-Setembro 2014

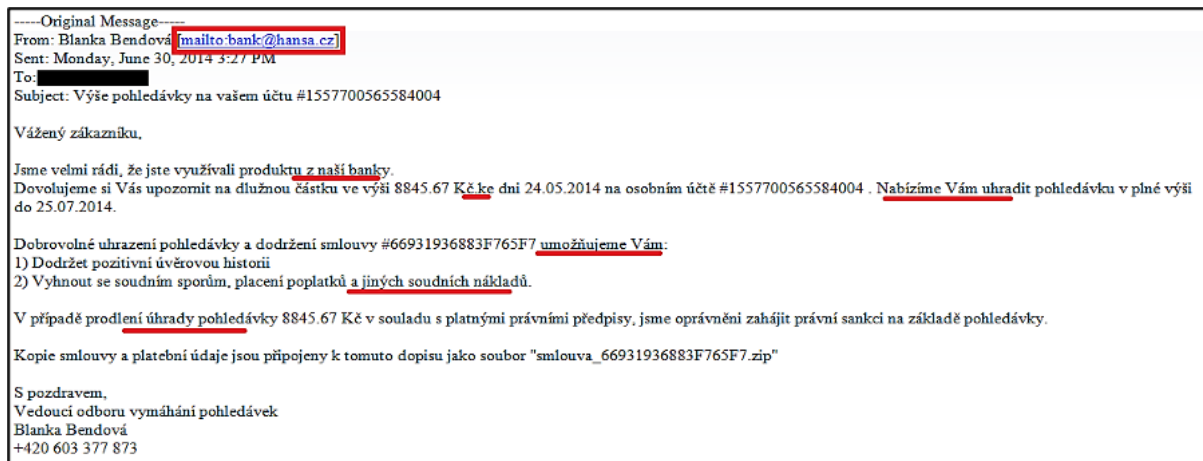
Dentro das campanhas individuais, houve um aumento na "qualidade" das suas próprias mensagens de correio electrónico e, em particular, uma melhor utilização da engenharia social em relação às presumíveis vítimas na região alvo, ou seja, a República Checa. No entanto, todas as referidas campanhas de phishing tinham pelo menos duas características em comum. Primeiro, era o facto de o anexo no e-mail enviado conter sempre um ficheiro que parecia um documento de texto mas que era um ficheiro executável, especificamente malware: Trojan.[8] A segunda característica comum era que a engenharia social tirava partido das preocupações dos indivíduos visados de possíveis litígios, neste último caso, da execução.

A primeira vaga de ataques de phishing foi enviada de vários domínios, não inteiramente confiáveis, quando se trata de cobrança de dívidas, registados na República Checa (por exemplo micik.cz ou dhome.cz, etc.). Foram utilizados vários nomes de pessoas e números de telefone existentes, rastreáveis na Internet (a pessoa proprietária deste número acabou por não ter nada a ver com o ataque).



E-mail fraudulento enviado como parte da onda de endividamento

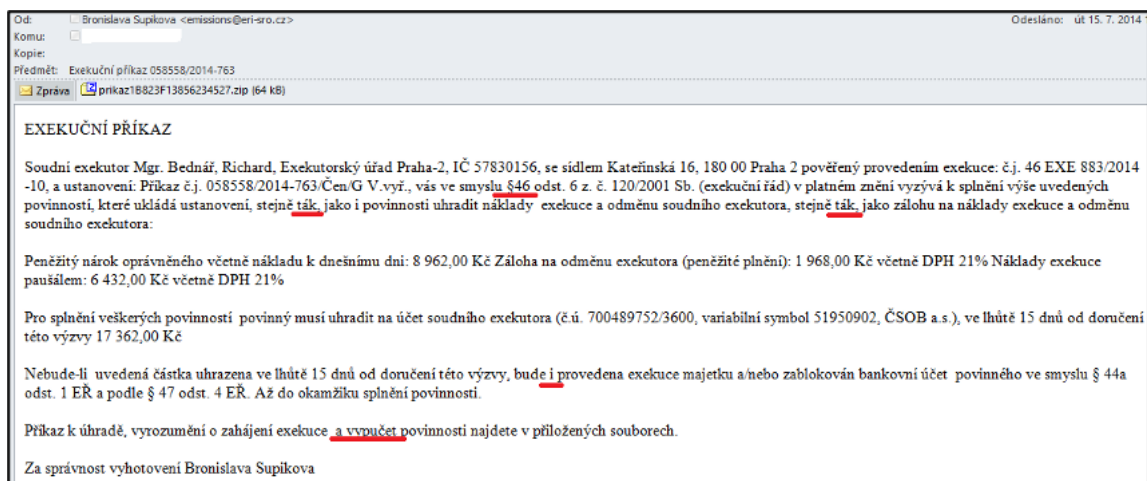
Na segunda vaga, a língua checa utilizada melhorou.



E-mail fraudulento enviado como parte da onda do Banco

Quando estes ataques de phishing começaram a aparecer, várias organizações de segurança e equipas CSIRT[9], bem como os meios de comunicação social, publicaram avisos incluindo instruções sobre como lidar com tais relatórios.[10]

Ambas as campanhas foram relativamente bem sucedidas, mas a mais bem sucedida foi o ataque em que o e-mail fraudulento foi um aviso (chamada) de um executor.



E-mail fraudulento enviado como parte da onda de execução

A língua checa utilizada na "ordem de execução" continha especialmente erros na utilização de diacríticos, ou algumas frases foram formuladas num estilo menos que natural. (Os erros mais óbvios estão sublinhados.) No entanto, foram utilizados os nomes de executores reais, rastreáveis na Internet (o referido executor não teve nada a ver com o ataque), bem como o número real de execuções.

Ad2) Instalação de malware para um computador

Como mencionado anteriormente, todas as campanhas de phishing incluíram malware no anexo do e-mail enviado: TrojanDownloader (ou seja, malware concebido para descarregar outro malware). Este malware foi principalmente criado e dirigido ao sistema operativo Windows XP, que foi descontinuado em Março de 2014.

Název	Velikost
 smlouva_26.06.2013-signed_893589F59975811EF.exe	85 504

Název	Velikost	Komprimovan...	Změněn
 prikaz-15.07.2014-signed_6F532B472446324E.exe	120 832	64 350	2014-07-15 11:00

Ficheiro executável (malware) contido no anexo aos e-mails fraudulentos

Depois de executar o anexo, foi instalado malware "Tinba" (cavalo de Tróia do banco), que foi descarregado da Internet em segundo plano, enquanto um contrato ou uma ordem de execução num editor de texto era mostrado a um utilizador.^[11]

O malware foi escrito para o directório: *Utilizadores/utilizador específico/AppData/Roaming/brothel*. Neste directório, foi possível encontrar o *ate.exe*, que é um ficheiro que foi criado após a abertura do ficheiro executável no e-mail de phishing. Ao mesmo tempo, foi criada uma chave apropriada no registo no ramo **HKEY_CURRENT_USERSoftwareMicrosoftWindowsCurrentVersionRun**. Desta forma, foi possível verificar se se tratava de malware resultante deste ataque.

Ad3) Acesso à banca online

O passo seguinte do agressor era esperar pelo momento em que a vítima entrasse na banca online. O malware no computador é capaz de gravar a comunicação entre o utilizador e a banca em linha, e um agressor tem a capacidade de monitorizar esta comunicação. O utilizador mal teve oportunidade de detectar o ataque porque o URL no navegador pertencia ao banco e a comunicação era segura (HTTPS).

"O roubo efectivo de dados sensíveis tem lugar através da inserção de código malicioso nos sítios oficiais dos bancos na Internet. Os scripts de configuração são descarregados de servidores C&C (máquinas pertencentes a atacantes, utilizadas para controlar a botnet) e descriptados como descrito acima. O que é interessante é a reutilização do mesmo formato de ficheiros de configuração dos conhecidos Trojans Carberp e Spyeye do banco. Para cada botuid (um valor único que identifica o ambiente do utilizador), uma lista de nomes de utilizador e palavras-passe é armazenada no servidor C&C. Os scripts adicionais são descarregados dependendo do banco utilizado, ou **hXXps://andry-shop.com/gate/get_html.js;hXXps://andry-shop.com/csob/gate/get_html.js**; ou **hXXps://yourfashionstore.net/panel/a5kGcvBqtV**, que será descarregado se a vítima visitar os sítios web de Česká spořitelna, ČSOB, ou Fia".^[12]

Anúncio 4) Instalação de malware para um dispositivo móvel

O passo seguinte do atacante foi convencer os utilizadores da necessidade de aumentar a segurança no acesso à banca online. A razão para o aviso emitido pelo alegado banco (na realidade um website controlado pelo atacante) era "aumentar" a segurança da ligação. Foi oferecida à vítima uma página com uma escolha de sistemas operativos de dispositivos móveis (Android, Windows Phone, Blackberry e iPhone OS), mas apenas a versão Android permitia o download de malware para o telefone. Os atacantes escolheram várias formas de distribuir malware para um telefone, desde o simples envio de uma mensagem SMS com uma ligação a partir da qual um utilizador pretendia descarregar o programa, até ao envio de uma mensagem SMS e de um código QR.^[13]

The text of the message:

CS-S24

Download a security from

Bit.ly/Tp9JjU

Vážení kliente!

SMS byla odeslána na číslo: +. Doručení SMS do 5 minut.

Pokud Vám nepřišel SMS, naskenujte QR kód



Je třeba nainstalovat aplikace OTPdirekt. Stiskněte tlačítko "Zobrazit instrukce".

Zobrazit instrukce

Pozor! Nemůžete pokračovat dále bez OTP hesla.

OTP heslo: **Pokračovat**

Descarregar malware para o telefone

O malware descarregado e instalado no dispositivo móvel foi detectado pelo Avast! como Android: *Perkele-T*.

O objectivo deste malware era obter acesso e controlo total sobre os meios de autenticação secundários (autenticação de dois factores), que na maioria dos casos é o telefone móvel. Se um utilizador estivesse a utilizar um sistema operativo que não o Android, recebia uma mensagem: *"Por favor, tente novamente mais tarde"*.

Ad5) Transferência e levantamento de fundos

O passo seguinte do atacante era retirar fundos da conta atacada e enviá-los para a conta dos cavalos brancos, que deveriam então levantar dinheiro ou transferi-lo para outras contas. Devido ao controlo total (utilizando malware) tanto dos dados de acesso bancário à Internet (ver computador infectado) como do controlo do dispositivo de autenticação secundário (ver telemóvel infectado - quando as mensagens de autenticação eram enviadas ao atacante sem serem vistas pela vítima), o atacante podia introduzir uma ordem de transferência de dinheiro "legítima".

De acordo com um relatório da Avast!, os atacantes de língua russa estavam por trás deste ataque. As mensagens SMS do telefone infectado foram encaminhadas para o número 79023501934, que foi registado na região de Astrakhan, Rússia. [\[14\]](#)

4.6.1.2. Correio Checo (Česká pošta)

O segundo grande ataque de phishing começou em Novembro de 2014 e continuou até Dezembro de 2014. No início do ataque, houve um e-mail de phishing com uma notificação de "Correio Checo" (Česká pošta) de que não foi encontrado como destinatário de uma remessa e que deveria descarregar a informação da remessa. A língua checa utilizada neste e-mail de phishing é uma das piores que se pode encontrar no phishing. Aparentemente, um dos tradutores automáticos da Internet foi utilizado para gerar este e-mail.

Os e-mails fraudulentos foram enviados a partir de endereços que não pertencem aos Correios checos. Estes eram, por exemplo, endereços: upport@cs-post.net, tracktrace@cs-post.net, cpost@cs-post.net, post@cs-post.net, zasilka@cs-post.net, que devido ao domínio **cs-post** poderia despertar a crença de um utilizador de que este é um sítio dos Correios checos. No entanto, é de notar que o **cs-post** foi registado no domínio **.net**, enquanto que as páginas reais do Correio Checo (Česká pošta) estão registadas no domínio **.cz** (ver <https://www.ceskaposta.cz>).

Ceská pošta (post@cs-post.info)
Jan Mráček Informace o Vaší zásilce
Dnes 18. 11. 2014, 11:21:28



Jan Mráček

Vaše zásilka **DR490714563C** dorazila na 14. listopadu 2014. Courier nebyl schopen doručit zásilku pro vás. Vytisknout informace o Vaší zásilce a ukázat, že v nejbližší poště, aby si zásilku.

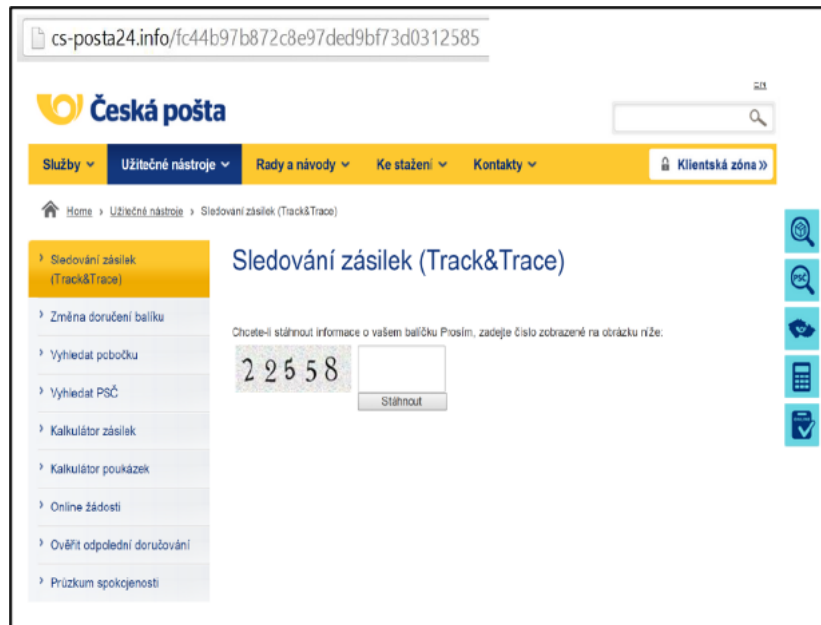
Stáhněte si informace o zásilce

Pokud je zásilka neobdrží do 15 pracovních dnů Česká pošta bude mít právo nárokovat odškodnění od si pro své udržení ve výši 52,5 Kč za každý den vedení. Můžete si najít informace o postupu a podmínkách při pozemku chov v nejbližší kanceláři.

Toto je generován automaticky zprávu, pokud nechcete přijímat zprávy od nás prosím [odhlásit](#)

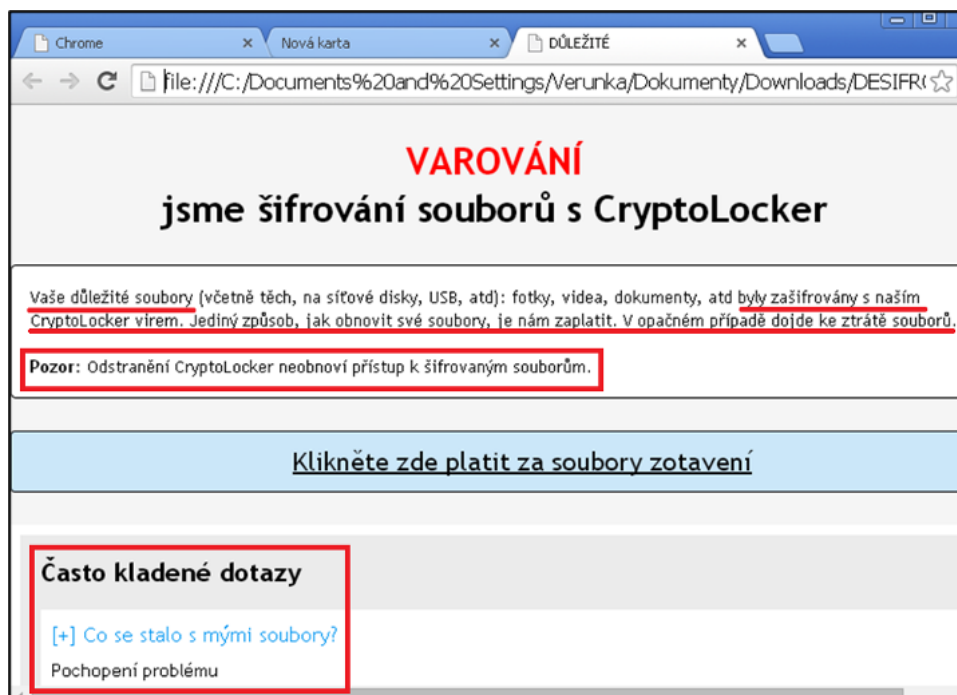
Figura64 - E-mail fraudulento de "Česká pošta"

Se um utilizador clicou na caixa: *Descarregar informação sobre o envio*, foi redireccionado para páginas que se assemelhavam às páginas reais do Correio Checo (Česká pošta). Aqui, foi pedido a um utilizador que introduzisse um código de segurança (Captcha) e foi-lhe então permitido descarregar um ficheiro .zip que continha "informação sobre o envio rastreado". Tal como na campanha anterior de phishing, um ficheiro executável (ransomware) foi armazenado no anexo, mas o objectivo era encriptar os dados de um utilizador.



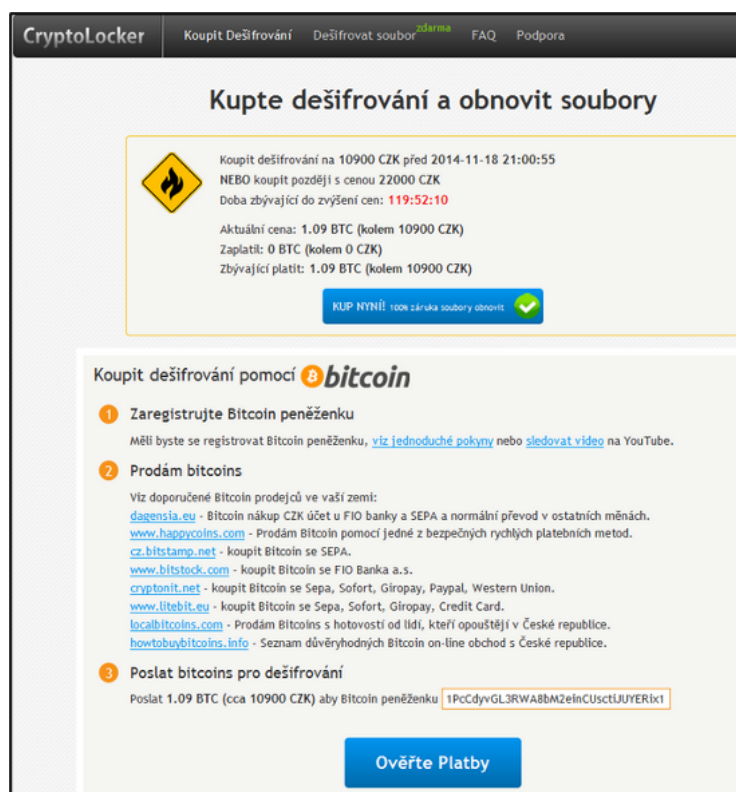
Sítio fraudulento do "Correio Checo" (Česká pošta)".

Após encriptar os dados, um utilizador foi solicitado a pagar por uma chave que fosse capaz de desencriptar os ficheiros encriptados. O pedido já foi escrito numa versão muito melhor do checo. O utilizador pode também aprender algumas respostas a algumas perguntas que o possam ter incomodado.



Informação que foi apresentada ao utilizador depois de encriptar os seus dados

A recuperação de dados nesse momento custou 1,09 BTC, e para além da conversão para coroas checas, foram mostradas ao utilizador instruções detalhadas sobre como criar uma carteira de bitcoin, onde e como comprar bitcoins e para onde os enviar.



Instruções sobre como decifrar os seus ficheiros[15].

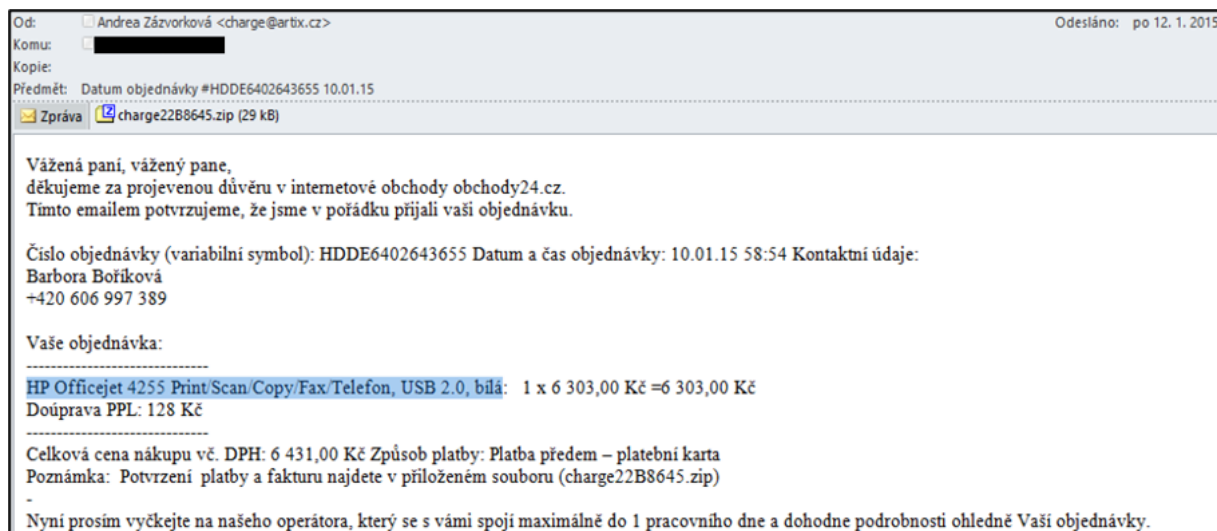
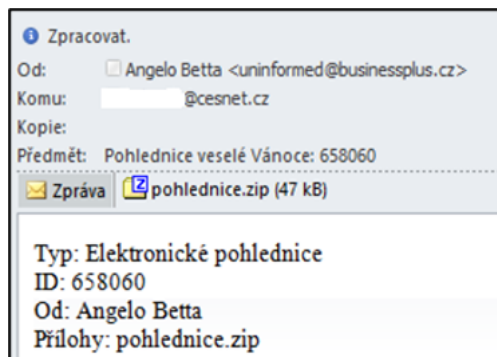
O ataque é específico, na medida em que acrescentou um programa de resgate a uma campanha de phishing, que começou imediatamente a encriptar os dados de um utilizador, e na medida em que foi utilizado um período pré-natalício para levar a cabo o ataque, no qual muitas pessoas esperam que os envios sejam entregues. Devido a estes dois factores, o ataque foi muito bem sucedido.

4.6.1.3. Natal e prendas

Outro grande ataque de phishing começou em Dezembro de 2014 (especificamente durante o período de Natal) e continuou em Janeiro de 2015. Este ataque foi dividido em duas fases. Na primeira fase, os utilizadores receberam um e-mail de desejos com um Feliz Natal através de um postal electrónico. Na segunda fase, foram enviadas mensagens confirmando uma encomenda de electrónica durante o mês de Janeiro. A mensagem informava um utilizador que este tinha adquirido bens (por exemplo, impressora, disco rígido, máquina fotográfica, etc.) pelos quais tinha pago antecipadamente com um cartão de pagamento, referindo-se à factura em anexo.

Ambos os ataques têm um elemento em comum, que é o malware contido num anexo de correio electrónico. Especificamente, foi um cavalo de Tróia (*Kryptik*), que foi apresentado como um protector de ecrã. Este malware era, como no caso do ataque mencionado no capítulo.

4.6.1.1 Debt/Bank/Execution comprimido num ficheiro .zip. Depois de desempacotar o ficheiro .zip, muitos utilizadores não consideraram o ficheiro .scr[16] executável e assim infectaram o seu próprio computador.



Amostras de cartões postais e mensagens de phishing de loja

O ataque é específico na medida em que utilizou um tipo de ficheiro que muitos utilizadores não consideram perigoso, e o momento do ataque. Graças a vários e-mails em cadeia, os utilizadores habituaram-se a abrir cartões postais electrónicos ou anexos com este aspecto, sem uma verificação mais completa do conteúdo. O segundo ataque foi planeado para que um utilizador verificasse se não tinha realmente encomendado qualquer mercadoria que não lhe tivesse sido entregue devido às férias de Natal.

4.6.1.4. Seznam.cz - Palavra-passe única

O último ataque de phishing demonstra uma mudança significativa nas táticas de ataque dos atacantes. Um atacante ainda tira partido do facto de o malware ter infectado um computador. Um atacante pode controlar ele próprio esse computador ou alugá-lo, por exemplo, como parte de uma botnet. A infecção real poderia ter ocorrido, por exemplo, através de outro correio electrónico recebido, ao visitar sites infectados, ou de outra forma. O objectivo do atacante no caso do Seznam - One Time Password[17] era obter o controlo do telemóvel do utilizador.

O malware que foi instalado num computador levou um utilizador a entrar na caixa de correio electrónico do Seznam.cz para instalar uma ferramenta para um trabalho mais fácil e seguro com a sua caixa de correio no seu telemóvel. Um utilizador é então guiado passo a passo através da instalação da aplicação SeznamOTP a partir de uma fonte não confiável. No final da instalação, é fornecida a um utilizador a sua "chave de licença única". Na realidade, contudo, um utilizador instalou malware no seu telemóvel.

Nastavení

One-Time-Password

Vážení uživatele Seznam

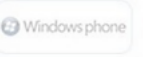
Jsm rádi, že vám můžeme oznámit, že teď autorizace ve vašem accountu (účtu) se stává jednodušší a bezpečnější. Seznam zavádí technologii One-Time-Password. Co to znamená?

One-Time-Password je to systém generace jednorázových hesel pro vstup do accountu uživatele, které jsou platné během 1 minuty. Pro vaše pohodlí jsme připravili jednoduchou a pohodlnou aplikaci pro váš chytrý telefon. Nyní pokaždé při vchodě do vašeho accountu, potřebujete otevřít naši aplikaci, generovat jednorázové heslo a uskutečnit vstup. Pro pokračování instalace postupujte podle návodu systému:

Mobilní telefon:

Obržíte SMS-zprávu s adresou webové stránky této aplikace na toto telefonní číslo

Vyberte operační systém vašeho mobilního telefonu:

Pokračovat

Ecrã de boas-vindas da instalação do SeznamOTP [18]

O **risco** deste último ataque de phishing é que a "mensagem de phishing" não foi entregue via correio electrónico ou outro meio de comunicação, mas foi exibida a um utilizador apenas numa situação específica (neste caso, após o login na caixa de correio seznam.cz) e o iniciador desta mensagem foi um malware encontrado num computador já infectado. O segundo factor de risco é o facto de o pedido de segurança não estar ligado a uma conta bancária. Por conseguinte, um utilizador pode não estar consciente dos perigos da instalação desta aplicação.

Na República Checa, é possível punir a conduta que tem a natureza de "phishing clássico", de acordo com a **Secção 209** (Fraude) do Código Penal. A fraude é completada por um enriquecimento. A criação de uma réplica de um website e a aquisição de nomes de login e palavras-passe poderia então ser qualificada como preparação ou tentativa de uma infracção penal de acordo com a Secção 209 do Código Penal. A obtenção de dados de acesso, incluindo números de conta, números de cartões de pagamento e códigos PIN sem a sua utilização posterior, não será considerada uma infracção penal.

Possibilidades de sanções penais na República Checa

No caso de formas combinadas de ataques de phishing, em que o malware é utilizado para infectar um computador, tal conduta de um infractor deve também ser punida de acordo com a **Secção 230** (Acesso não autorizado ao sistema informático e portador de informação) do Código Penal. Se o objectivo do ataque de phishing for obter um benefício injustificado para si próprio ou para outro, é também possível aplicar as disposições do **Artigo 230 (3)** do Código Penal.

Em casos específicos, seria possível utilizar as disposições da **Secção 234** (Medidas não autorizadas, contrafacção e alteração dos meios de pagamento) do Código Penal.

Possibilidades de sanções penais na Polónia

Quebra do segredo da comunicação (sniffing) - arte. 267 § 3 do Código Penal. Este tipo de crime consiste na obtenção de informações confidenciais, por exemplo através de sniffers, ou seja, programas que interceptam dados (palavras-passe e identificações de utilizadores). Tal acto é punível com uma pena de prisão até 2 anos.

Artigo 267º Obtenção ilícita de informações

§ 1 Quem, sem autorização, obtiver acesso a informações que não lhe sejam destinadas, abrindo uma carta fechada, ligando-se a uma rede de telecomunicações ou quebrando ou contornando uma protecção electrónica, magnética, informática ou outra protecção específica da mesma, será sujeito a uma multa, à pena de limitação da liberdade ou de privação de liberdade por um período até 2 anos.

§ 2. A mesma punição será imposta a qualquer pessoa que, sem autorização, tenha acesso à totalidade ou a qualquer parte de um sistema de informação.

§ 3. A mesma punição será imposta a qualquer pessoa que, a fim de obter informações a que não tenha direito, estabeleça ou utilize um dispositivo de escuta ou visual, ou outro dispositivo ou software.

§ 4. A mesma punição será imposta a qualquer pessoa que revele informações obtidas da forma especificada nos § 1-3 a outra pessoa.

§ 5. A acusação da infracção especificada em § 1-4 deve ocorrer com base na moção da pessoa lesada.

Possibilidades de sanções penais em Portugal

Sendo a disseminação de malware criminalizada (art. 6(2) da Lei sobre o Cibercrime), como mencionado, por si só, a criação de dados não autênticos seria considerada uma infracção como falsificação relacionada com a informática (art. 3 da Lei sobre o Cibercrime). Além disso, se a finalidade de tal criação tiver a intenção fraudulenta ou desonesta de obter, sem direito, um benefício económico para si próprio ou para outra pessoa, sobre as despesas da vítima, também seria considerada uma fraude informática (art. 221(1) do Código Penal).

Além disso, a contrafacção de cartões e outros meios de pagamento que não em numerário, incluindo a utilização indevida de dispositivos, é punida como infracções agravadas (artigos 3-A a 3-F da Lei sobre o Cibercrime).

Por outro lado, estando no âmbito de aplicação da Lei nº 52/2003, relativa à luta contra o terrorismo, a falsificação informática e a fraude informática seriam consideradas infracções agravadas.

4.6.2. Pharming

O **Pharming**^[19] é uma forma mais sofisticada e perigosa de phishing. Trata-se de um ataque a um servidor DNS (Domain Name System), que traduz um nome de domínio para um endereço IP. O ataque ocorre quando um utilizador introduz um endereço de um servidor web ao qual pretende aceder num navegador da Internet. No entanto, não se ligará ao endereço IP apropriado do servidor web original, mas a um endereço IP diferente, falsificado. Os sítios web com um endereço falso imitam geralmente muito fielmente as páginas originais. São praticamente indistinguíveis deles. Um utilizador introduz então as suas credenciais que um atacante obtém. Este ataque é geralmente efectuado quando um utilizador acede a sites bancários na Internet.

"Os sites falsos podem ser utilizados para instalar vírus ou cavalos de Tróia no computador de um utilizador, ou podem ser utilizados por atacantes para tentar obter informações pessoais ou financeiras, que podem depois ser indevidamente utilizadas para roubar identidade. O Pharming é uma forma particularmente perigosa de cibercrime, porque no caso de um servidor DNS infectado, um utilizador pode tornar-se uma vítima, mesmo que não esteja instalado qualquer malware no seu computador. Mesmo que utilize medidas de precaução, tais como introduzir manualmente endereços de Internet ou utilizar apenas marcadores de confiança, não está protegido contra este tipo de ataque, porque o redireccionamento indesejado só ocorre depois de o computador enviar um pedido de ligação".^[20]

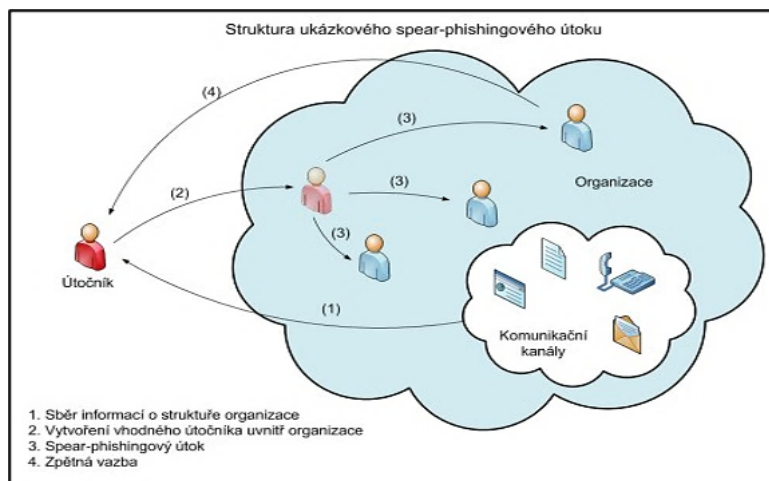
A outra forma típica de farming é atacar o computador de um utilizador final com malware, onde se pode esperar um nível de segurança mais baixo. Este malware altera o ficheiro anfitrião para desviar o tráfego do destino pretendido e redireccionar os utilizadores para um site falso.

As sanções penais são semelhantes às que se aplicam no caso de phishing. O mesmo, de acordo com a lei portuguesa e polaca.

4.6.3. Spear Phishing

O phishing de lança é uma das formas de ataque de phishing, mas com a diferença de que o phishing de lança é um ataque precisamente direccionado, ao contrário do phishing, que é um ataque (aleatório) bastante generalizado. O alvo de um ataque é geralmente um grupo, organização ou indivíduo específico, especificamente informação e dados contidos nesta organização (por exemplo, propriedade intelectual, dados pessoais e financeiros, estratégias empresariais, informação classificada, etc.).

A diferença entre phishing de lança e phishing clássico está em quem é o remetente das mensagens em questão. No início de um ataque, é o atacante que utiliza fontes abertas para descobrir o máximo de informação possível sobre a organização atacada, a sua estrutura, etc. Ele também cria um e-mail ou outra mensagem de alta qualidade e começa a comunicar com uma pessoa de dentro da organização como um colega. O atacante utilizará então essa pessoa como meio de difundir outras mensagens (por exemplo, malware infectado) dentro da organização. Como a pessoa que é "conhecida" pelas vítimas, não tem qualquer problema em comunicar com as vítimas, que verifica menos as mensagens do agressor, se é que o faz de todo.^[21]



Estrutura de um ataque com lança^[22]

Texto sobre a figura: A estrutura de uma amostra de ataque de pesca submarina

Atacante - Organização - Canais de comunicação

1. Recolha de informação sobre a estrutura de uma organização
2. Criação de um atacante adequado dentro da organização
3. Ataque de pesca com lanças
4. Feedback



O curso de um ataque de phishing de uma lança[23].

Possibilidades de sanções penais na República Checa

Um castigo de phisher de lança é semelhante ao de phishing. Por exemplo, uma organização terrorista pode estar por detrás de um ataque de phishing com uma lança. Neste caso, não está excluída a responsabilidade por uma infracção penal ao abrigo da **Secção 311** (Ataque terrorista) do Código Penal.

Possibilidades de sanções penais na Polónia

Aplicam-se as mesmas leis que se aplicam ao phishing.

Possibilidades de sanções penais em Portugal

Sendo a conclusão a mesma do phishing em geral, incluindo as relacionadas com o terrorismo.

4.6.4. Vishing

O termo vishing[24] refere-se ao phishing telefónico, no qual um atacante utiliza uma técnica de engenharia social e tenta atrair informação sensível de um utilizador (por exemplo, números de conta, detalhes de login - nome e palavra-passe, números de cartões de pagamento, etc.). O atacante está deliberadamente a tentar falsificar a sua identidade. Os atacantes apresentam-se frequentemente como representantes de bancos reais ou outras instituições, a fim de suscitar a menor suspeita possível num utilizador. O Vishing é utilizado na telefonia VoIP (Voice over Internet Protocol).

4.6.5. Smishing

Smishing[25] funciona com base num princípio semelhante ao vishing ou phishing, mas utiliza mensagens SMS para distribuir mensagens. Como parte do smishing, é principalmente uma tentativa de forçar um utilizador a pagar uma quantia (por exemplo, ligar para uma linha gratuita, enviar um SMS doador, etc.) ou clicar em ligações URL suspeitas. Se um utilizador visita o URL, é redireccionado para uma página que explora certas vulnerabilidades no sistema informático, ou o utilizador é alertado para informações sensíveis ou malware.[26]

Exemplo de smishing:

"Aviso - esta mensagem é gerada automaticamente a partir de (nome do banco local), o seu cartão de crédito foi bloqueado. Para reactivar, ligue 866 ### ####".

Possibilidades de sanções penais na República Checa

As sanções penais de vishing e smishing são semelhantes às aplicadas no caso de phishing.

Possibilidades de sanções penais na Polónia

Aplicam-se as mesmas leis que se aplicam ao phishing.

Possibilidades de sanções penais em Portugal

Também neste caso, as conclusões relativas à criminalização são as mesmas que para o phishing em geral, incluindo as relacionadas com o terrorismo.

[1] Ver, por exemplo, *Google diz que os melhores esquemas de phishing têm uma taxa de sucesso de 45 por cento*. [online]. [cit. 14.8.2016]. Disponível em: <https://www.engadget.com/2014/11/08/google-says-the-best-phishing-scams-have-a-45-percent-success-r/>

Phishing pelos Números: Must-Know Phishing Statistics 2016. [online]. [cit. 14.8.2016]. Disponível a partir de: <https://blog.barkly.com/phishing-statistics-2016>

[2] Ver por exemplo, *Beware of Fake Android Prisma Apps Running Phishing, Malware Scam* [online]. [cit.14.8.2016]. Disponível a partir de: <https://www.hackread.com/fake-android-prisma-app-phishing-malware/>

[3] LANCE, James. *Phishing bez záhad*. Praga: Grada Publishing, 2007. p. 45.

[4] WILSON Tracy, V. *Como funciona a Phishing*. [online]. [cit.14.8.2016]. Disponível em: <http://computer.howstuffworks.com/phishing.htm>

[5] As tendências de desenvolvimento do phishing – ver também, por exemplo, DODGE, Ronald. C., Curtis CARVE e Aaron J. FERGUSON. Phishing for User Security Awareness. *Computers & Security*, 2007, vol. 26, No. 1, pp. 73–80.

[6] De acordo com o estudo seguinte, o phishing aumentou em 250% nos últimos 6 meses. Ver *Relatório de Tendências da Actividade de Phishing*. [em linha]. [cit.14.8.2016]. Disponível a partir de: https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf

[7] A seguir referido como DBE.

[8] Para mais detalhes ver os resultados da Virustotal. [online]. [cit. 15.8.2016]. Disponível a partir de:

<https://www.virustotal.com/cs/file/62170532b1f656c6917fa66d0ed98462e106f3aa139273c9f2c3a370a67d265f/analysis/1471330723/>

[9] Equipa de Resposta a Incidentes de Segurança Informática. Para mais detalhes, ver, por exemplo: <https://www.csirt.cz/>

[10] Ver, por exemplo, *Pozor na zprávu o údajné neuhrazené pohledávce – jedná se o podvod*. [online]. [cit.15.8.2016]. Disponível em: <https://www.csirt.cz/page/2073/pozor-na-zpravu-o-udajne-neuhrazene-pohledavce---jedna-se-o-podvod/>
Znovu se objevily podvodné zprávy. [online]. [cit.15.8.2016]. Disponível a partir de: <https://www.csirt.cz/news/security/?page=97>

PODVODNÉ EMAILY hrozí exekucí, nic neplatte a neotvírejte! [online]. [cit.15.8.2016]. Disponível a partir de:

<http://tn.nova.cz/clanek/zpravy/cernakronika/podvodne-emaily-hrozi-exekuci-nic-jim-neplatte-a-neotvirejte.html>

Pozor na zprávu o výzvě k úhradě před exekucí – jedná se o podvod. [online]. [cit.15.8.2016]. Disponível a partir de: <https://www.csirt.cz/news/security/?page=87>

Čo sa skrýva v prílohe podvodných e-mailov? [online]. [cit.15.8.2016]. Disponível a partir de: <https://blog.nic.cz/2014/07/23/co-sa-skriva-v-prilohe-podvodnych-e-mailov-2/>

[11] Para mais detalhes ver a análise da funcionalidade do malware Tinba: W32. *Tinba (Tinybanker)*. [online]. [cit.15.8.2016]. Disponível em: https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_w32-tinba-tinybanker.pdf

[12] HOŘEJŠÍ, Jaromír. *Faleňý exekucní příkaz ohrozuje uživatele českých banco*. [online]. [cit.15.8.2016]. Disponível a partir de: <https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/>

[13] Ibid. – imagem com código captcha.

[14] HOŘEJŠÍ, Jaromír. *Faleňý exekucní příkaz ohrozuje uživatele českých banco*. [online]. [cit.15.8.2016]. Disponível a partir de: <https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/>

[15] *Sledování zásilky České pošty aneb nová havěť*. [online]. [cit.14.8.2016]. Disponível em: <http://www.viry.cz/sledovani-zasilky-ceske-posty-aneb-nova-havet/>

[16] Os ficheiros SCR são ficheiros executáveis.

São atribuídos principalmente com o programa Ficheiro Desconhecido Apple II (encontrado no CD Rom de Golden Orchard Apple II). Também são atribuídos os seguintes: Windows Screen Saver, Image Pro Plus Ver. 1.x - 4.5.1.x Macro (Media Cybernetics Inc.), TrialDirector Script File (inData Corporation), Screen Dump, Screen Font, StatisticaScrollsheet, Procomm Plus Screen Snapshot File, Movie Master Screenplay, Mastercam Dialog Script File (CNC Software Inc.), Sun Raster Graphic, LocoScript Screen Font File (LocoScript Software), Faxview Fax, DOS DEBUG Input File, Script a FileViewPro.

Co znamená přípona souboru SCR. [online]. [cit.14.8.2016]. Disponível em: <http://www.solvusoft.com/cs/file-extensions/file-extension-scr/>

[17] A seguir referido como SeznamOTP

[18] Mais informações sobre este malware e o curso de todo o ataque podem ser encontradas, por exemplo, em *Podvodníci mění taktiku. Našli novou cestu, jak vybilí lidem účty*. [em linha]. [cit.14.8.2016]. Disponível a partir de: <https://www.novinky.cz/internet-a-pc/bezpecnost/364094-podvodnici-meni-taktiku-nasli-novou-cestu-jak-vybilit-lidem-ucty.html>

[19] É uma combinação de palavras "agricultura" e "phreaking".

[20] Para mais detalhes ver *Co je pharming?* [online]. [cit.14.8.2016]. Disponível a partir de: <http://www.kaspersky.com/cz/internet-security-center/definitions/pharming>

[21] "Um agressor escolhe uma organização que trabalha com informações valiosas, analisa o sítio web para obter informações sobre a estrutura de pessoal, empregados e procedimentos (para informações mais detalhadas sobre empregados, esse agressor pode utilizar as suas páginas privadas e fóruns de discussão) e, no passo seguinte, o agressor cria um relatório cujo conteúdo, forma e aparência imita a comunicação interna na organização. Em seguida, o agressor pede a um empregado que forneça informações sensíveis para acesso à rede informática".

Evoluční teorie v podání spearphishingu. [online]. [cit.15.2.2010]. Disponível a partir de: <http://connect.zive.cz/content/evolučni-teorie-v-podání-spear-phishingu>

[22] Ibidem

[23] *Dica do mês Julho 2016 - Evite ser fisgado por Phishing*. [online]. [cit.14.8.2016]. Disponível em: <http://www.intermanager.org/cybersail/tip-of-the-month-july-2016-avoid-getting-hooked-by-phishing/>

[24] É uma combinação de palavras "voz" e "phishing".

[25] É uma combinação de palavras "SMS" e "phishing".

[26] Por exemplo, **Xshqi** - *Minhoca Andróide no dia dos namorados chineses*. [online]. [cit.14.8.2016]. Disponível a partir de:
<https://securelist.com/blog/virus-watch/65459/android-worm-on-chinese-valentines-day/>

Selfmite - *SMS SMS de verme Android Selfmite regressa, mais agressivo do que nunca*. [online]. [cit.14.8.2016]. Disponível a partir de:
<http://www.pcworld.com/article/2824672/android-sms-worm-selfmite-returns-more-aggressive-than-ever.html>

4.7. Compromisso de e-mail comercial (BEC)

Business Email Compromise[1] é um tipo de ataque fraudulento em que um atacante faz-se passar por um executivo (normalmente o CEO), e tenta conseguir que um empregado, cliente ou fornecedor transfira dinheiro ou informação sensível para o atacante.

O esquema BEC poderia estar ligado a outras formas de fraude como um romance, lotaria, emprego, e esquemas de aluguer.

Pela definição do FBI, o BEC é *um esquema sofisticado que visa empresas que trabalham com fornecedores estrangeiros e/ou empresas que efectuem regularmente pagamentos por transferência bancária. O esquema é levado a cabo comprometendo contas de e-mail comerciais legítimas através de engenharia social ou técnicas de intrusão informática para realizar transferências não autorizadas de fundos.*[2]

Ao contrário de um ataque de phishing tradicional, BEC é dirigido a um determinado indivíduo ou organização. No caso de BEC, o atacante prepara-se para o ataque muito cuidadosamente e tenta obter o máximo de informação sobre a vítima antes de o ataque ocorrer. Normalmente utilizam websites, relatórios anuais, informações sobre os funcionários da organização a partir de redes sociais, de contas de correio electrónico comprometidas, etc.

Este elevado nível de segmentação ajuda estes esquemas de correio electrónico a escapar aos filtros de spam e a escapar às campanhas de listas brancas de correio electrónico. Também pode tornar muito, muito mais difícil para os empregados reconhecerem que o correio electrónico não é legítimo.[3]

As vítimas do esquema do BEC vão desde pequenas empresas a grandes corporações. O esquema do BEC está ligado a outras formas de fraude, incluindo mas não limitado a: romance, lotaria, emprego, e esquemas de aluguer.

O FBI advertiu que os esquemas de BEC provavelmente *"continuariam a crescer, evoluir, e visar empresas de todas as dimensões"*. O FBI também mencionou que viu um aumento de 1.300% nos ataques de compromisso de correio electrónico empresarial desde Janeiro de 2015.[4]

Os atacantes do BEC dependem fortemente de táticas de engenharia social para enganar empregados e executivos insuspeitos. Algumas das amostras de mensagens de correio electrónico têm assuntos que contêm palavras como **pedido, pagamento, transferência, e urgente**, entre outros.

O esquema BEC toma geralmente uma das seguintes formas:

1. Fraude do CEO

Os atacantes fazem-se passar pelo CEO da empresa ou outro executivo da empresa e enviam um e-mail falso aos funcionários com a capacidade de enviar transferências electrónicas e instruí-los a enviar fundos aos atacantes.

2. Factura falsa[5]

Uma empresa, que frequentemente tem uma relação de longa data com um fornecedor, é solicitada a transferir fundos para pagamento de facturas para uma conta alternativa e fraudulenta. O agressor aproxima-se normalmente da vítima via e-mail ou telefone. Um ataque por correio electrónico tem tipicamente um código fonte (cabeçalho) de correio electrónico falso e objecto do pedido, pelo que parece muito semelhante a um pedido legítimo.

3. Compromisso de conta

Este ataque é semelhante ao da Factura Falsa. O atacante utiliza a conta de e-mail de um empregado (pirateada ou falsificada), depois envia um e-mail aos clientes para os anunciar que houve um problema com o seu pagamento e que precisam de o reenviar para uma conta diferente.

4. Executivo de Negócios e Impersonificação de Advogados

As vítimas são contactadas por atacantes, que se identificam como advogados ou representantes de firmas de advogados. O agressor solicita uma grande transferência de fundos para ajudar a resolver uma disputa legal ou pagar uma conta em atraso. O agressor tenta convencer as vítimas de que a transferência é confidencial e sensível ao tempo, pelo que é menos provável que o funcionário tente confirmar se devem transferir os fundos.

5. Roubo de dados

Um tipo de BEC cujo objectivo não é uma transferência directa de dinheiro. As vítimas típicas desse ataque incluem departamentos/empregados de finanças ou RH. O atacante solicita-lhes que enviem uma grande sensibilidade para a sua conta. A engenharia social é utilizada, e o ataque de roubo de dados pode ser um ponto de partida para os ataques de BEC acima mencionados, centrados na transferência financeira.

Desde 2017, tem havido um aumento dramático de ataques fraudulentos com o carácter de BEC na República Checa. Mais uma vez, a maioria dos ataques de BEC utilizam um modus operandi semelhante:

1. Escolher uma vítima e obter informações sobre a vítima (as organizações de média e pequena dimensão são o alvo mais comum)

2. Preparação de um e-mail falsificado (para criar um e-mail falsificado, são utilizados muito frequentemente serviços gratuitos disponíveis ao público, por exemplo: www.5ymail.com. Este serviço permite ao atacante criar e enviar qualquer correio electrónico falsificado que corresponda a um correio electrónico existente. No entanto, este serviço não permite receber respostas e, portanto, é necessário redireccionar a comunicação de correio electrónico para outro correio electrónico existente, registado, por exemplo, com um serviço de correio electrónico gratuito. A verdadeira identidade pode ser encontrada a partir do código fonte da mensagem).

3. Enviar um e-mail falso a um empregado da vítima (os ataques mais frequentes de BEC incluem Fraude do CEO e Factura Falsa. Os montantes necessários desta forma variam normalmente entre várias centenas de euros a 4000 euros).

4. Pedido de transferência imediata ou "urgente" de dinheiro para uma conta do agressor ou das mulas de dinheiro [validação do pagamento, bem como da pessoa que dá a ordem para fazer o pagamento, é o momento chave em que a conclusão do acto criminoso pode ser impedida. Se a organização tiver estabelecido protocolos de segurança adequados, tal transferência geralmente não tem lugar. Do ponto de vista da identificação do

agressor, a conta do agressor, ou a conta de mulas de dinheiro, é o instrumento que permite determinar na prática se se trata da continuação de um acto criminoso (ou seja, do ponto de vista do direito penal substantivo um acto criminoso) ou se se trata de um caso de concomitância de actos criminosos. Ao mesmo tempo, é de facto a pegada digital mais significativa que permite a identificação do agressor].

5. Transferência de dinheiro para uma conta do atacante ou mulas de dinheiro

[1] Os esquemas BEC são também conhecidos como esquemas de "fraude de CEO" ou "Man-in-the-Email".

[2] *Compromisso de e-mail comercial: O esquema de 3,1 biliões de dólares.* [online]. [citação 12.6.2018]. Disponível em: <https://www.ic3.gov/media/2016/160614.aspx>

[3] *O que é um Compromisso de Email Empresarial (BEC) Attack? E como posso impedi-lo?* [online]. [citação 12.6.2018]. Disponível em: <https://blog.barkly.com/what-is-a-business-email-compromise-bec-attack-and-how-can-i-stop-it>

[4] *Compromisso de e-mail comercial: O esquema de 3,1 biliões de dólares.* [online]. [citação 12.6.2018]. Disponível em: <https://www.ic3.gov/media/2016/160614.aspx>

[5] Este ataque também é chamado: "The Bogus Invoice Scheme", "The Supplier Swindle", e "Invoice Modification Scheme".

4.8. Sítios Web fraudulentos (empresas)

Na Internet, pode encontrar uma série de actividades, ou websites[1] apresentando prémios surpreendentes ou oferecendo vários bens a preços muito razoáveis. Os atacantes utilizam engenharia social e confiam principalmente na confiança e no descuido das pessoas. A própria actividade do agressor pode então tipicamente assumir duas formas.

No primeiro caso, um atacante tenta atrair dados sensíveis (por exemplo, nome, apelido, endereço de entrega, e-mail, número de telefone e palavra-passe) normalmente para efeitos de registo, entrega de mercadorias, prémios, etc. Todos estes dados são introduzidos por um utilizador e de forma voluntária. Um atacante acede assim a dados que pode, como no caso do phishing, utilizar para uma vasta gama de actividades. Por exemplo, com base na senha introduzida e outras informações sobre um utilizador, um atacante pode tentar obter acesso a outros serviços que um utilizador utiliza.[2]

No outro caso, muito mais comum, trata-se de actividades que consistem em atrair de forma fraudulenta fundos de um utilizador. Carros, motocicletas, tractores, outras máquinas agrícolas e, sobretudo, electrónica de qualquer tipo são normalmente oferecidos na Internet a um preço muito vantajoso.

No que respeita a ofertas fraudulentas na Internet, o Centro Europeu do Consumidor[3] emitiu uma recomendação para os utilizadores, que deverá permitir-lhes identificar práticas fraudulentas:

- **Introduzir a informação da empresa (por exemplo, nome da empresa, endereço do website, e-mail) num motor de busca na Internet.**
- **Pense em como o comerciante se apresenta.** O website onde vai comprar algo parece profissional? Endereços de e-mail em servidores gratuitos e anónimos como yahoo.com, hotmail.com, gmail.com, live.com, seznam.cz, etc. não irão certamente criar uma impressão credível. Do mesmo modo, se o sítio web estiver localizado num servidor de alojamento gratuito, é sinal de falta de profissionalismo.
- **Pagar apenas antecipadamente se for um comerciante verdadeiramente digno de confiança.** Certamente não dará dinheiro na rua a um estranho com a promessa de que ele lhe entregará a coisa no futuro. No entanto, muitos utilizadores fazem-no na Internet. Só faça um pagamento adiantado se tiver a certeza de estar a lidar com um fornecedor de confiança. Em particular, os detalhes do cartão de pagamento precisam de ser protegidos.
- **Um pedido de pagamento por parte da Western Union é particularmente suspeito.** Para transferências bancárias, nunca envie dinheiro para contas privadas, a menos que seja a conta da empresa vendedora.
- **Os sinais habituais de fraude incluem linguagem pobre, a exigência de pagar antecipadamente em dinheiro ou por transferência bancária, outros pedidos de pagamento sob um pretexto fictício (alfândega, seguros, embalagem de um maior número de peças do produto) e assim por diante. Lembre-se que se uma oferta parecer demasiado boa para ser verdadeira, provavelmente não é real!**
- **Verificar o registo comercial do país para ver se a empresa está registada.** (Acontece também que alguém se apropria indevidamente do nome de uma empresa existente e inicia um website com um nome semelhante.
- **Verifique o domínio do sítio web.** Acontece que um endereço web é o mesmo que o endereço de uma empresa real e registada. Contudo, existe uma diferença - o domínio, ou seja, o sufixo do endereço da Internet, é diferente (por exemplo, não ".co.uk" para a Grã-Bretanha, mas ".co.cc" para as Ilhas Cocos).
- **Encontre a sede da empresa num servidor de Internet que oferece fotografia de rua de cidades,** de acordo com o endereço dado nos anúncios e no website da empresa.
- **Valorize a sua informação pessoal.** Não partilhe informação sobre si em sítios não confiáveis ou desconhecidos. Apenas forneça informação que seja realmente necessária.
- **Não responder ao spam.** Não responda a e-mails não solicitados, em qualquer caso não revele os dados da sua conta bancária, número do cartão de pagamento ou, por exemplo, os dados de login para o Internet banking por e-mail. Apague as mensagens de correio electrónico não solicitadas, nunca abra anexos desconhecidos.[4]

Todas as características acima referidas devem ser consideradas como meras indicações que podem levar à detecção de fraude. Um atacante pode modificar as suas acções com base no sucesso do seu próprio ataque. Para **além destas dicas, é aconselhável utilizar os avisos publicados noutros sites, tais como www.podvodnefirmy.cz, etc.**

Possibilidades de sanções penais na República Checa

Na República Checa, é possível punir a conduta acima descrita na **Secção 209** (Fraude) do Código Penal. A fraude é completada por um enriquecimento. A criação de uma réplica de um sítio web e a aquisição de nomes de login e de palavras-passe poderia então ser qualificada como preparação ou tentativa de uma infracção penal de acordo com a Secção 209 do Código Penal. Se um agressor tentasse (Secção 21 do Código Penal) o acesso não autorizado à conta de outro utilizador utilizando os dados de acesso obtidos, tal conduta poderia também ser qualificada ao abrigo da **Secção 230** (Acesso não autorizado ao sistema informático e ao portador de informação) do Código Penal.

Possibilidades de sanções penais na Polónia

Na Polónia, isto é regulado pela Arte. 286 (fraude), que diz isso:

§ 1. quem, a fim de obter um lucro material, conduzir outra pessoa a uma disposição desvantajosa dos seus próprios bens ou dos bens de outra pessoa através de engano ou exploração de um erro ou incapacidade de apreender uma acção prevista, será sujeito à pena de privação de liberdade por um período compreendido entre 6 meses e 8 anos.

Possibilidades de sanções penais em Portugal

Mais uma vez, como explicado em relação ao phishing em geral, tais actos seriam puníveis como forja informática (art. 3 da Lei sobre o Cibercrime), bem como fraude informática (art. 221 do Código Penal).

[1] Os mais comuns são os websites, portais de publicidade, mas também podem ser contas nos meios de comunicação social, etc.

[2] Muito frequentemente, a mesma ou semelhante senha é introduzida pelos utilizadores dentro de diferentes serviços online. Como resultado, um atacante pode utilizar, por exemplo, a técnica de ataque de dicionário para invadir dados de acesso a outros serviços. Através desta acção, o atacante pode também cometer outras acções ilegais (por exemplo, ver capítulo 4.15 Identity theft, 4.8 Hacking etc.).

Para mais detalhes, ver por exemplo *Slovníkový útok*. [online]. [cit.30.8.2016]. Disponível em: <https://managementmania.com/cs/slovnikovy-utok>

[3] Para mais detalhes, ver <http://www.evropskyspotrebitel.cz/>

[4] Para mais detalhes: ver *ESC radí, jak poznat podvody na internetu*. [online]. [cit.30.8.2016]. Disponível em: <http://www.evropskyspotrebitel.cz/nakupy-online/esc-radi-jak-poznat-podvod-na-internetu-27250>

4.9. Hacking

O termo hacking é actualmente entendido pelo público pejorativamente como qualquer actividade de uma pessoa destinada a obter acesso ilegal ao sistema ou computador pessoal de outra pessoa.^[1] Especialmente nos meios de comunicação social, este termo é geralmente referido como todos os atacantes cujas acções são dirigidas contra as tecnologias de informação ou cujas actividades se baseiam na utilização de tais tecnologias. Neste contexto, contudo, existe uma diferença fundamental entre a percepção do público sobre o conteúdo do conceito de hacking e aqueles que se autodenominam hackers ou são rotulados como tal pela sua própria comunidade.

Os termos "**hacker**"^[2] e "**hacking**" tiveram origem nos EUA, nos anos 50, e **referiam-se a uma pessoa tecnicamente dotada** (e às suas actividades) **que era capaz de encontrar novas soluções, muitas vezes pouco ortodoxas, para um problema.**

Para compreender como os atacantes, a que costumávamos chamar hackers, percebem a sociedade e as suas regras, é útil conhecer a sua opinião. Em 1984, Levy definiu os seguintes princípios de ética de hacking:

1. O acesso a computadores e tudo o mais que lhe possa ensinar algo sobre como o mundo funciona deve ser ilimitado e absoluto. Respeite sempre a regra da experiência pessoal.
2. Todas as informações devem ser gratuitas.
3. Não confie nas autoridades, apoie a descentralização.
4. Os hackers devem ser julgados pelas suas acções e não por critérios mal orientados, tais como idade, raça ou estatuto.
5. É possível criar "beleza" num computador.
6. Os computadores podem mudar a sua vida para melhor.^[3]

Embora estas regras nem sempre sejam respeitadas ou reconhecidas, elas representam o quadro básico para a percepção do mundo virtual pelos atacantes, a quem chamamos hackers.

Outra visão importante da percepção do mundo através dos olhos de um hacker é o documento *The Hacker Manifesto*:

O seguinte foi escrito pouco depois da minha prisão.

A Consciência de um Hacker

Outro foi apanhado hoje, está em todos os jornais. "Adolescente preso em escândalo de crime informático", "Hacker preso depois de adulteração bancária"...

Malditos miúdos. São todos iguais.

Mas será que, na sua psicologia de três peças e na tecnobrain dos anos 50, alguma vez olhou para trás dos olhos do hacker? Alguma vez se perguntou o que é que o fez fazer tiquetaque, que forças o moldaram, o que o pode ter moldado?

Sou um hacker, entra no meu mundo...

O meu é um mundo que começa com a escola... Sou mais esperto que a maioria das outras crianças, esta porcaria que nos ensinam aborrece-me...

Maldito fraco aproveitamento. São todos iguais.

Estou no liceu ou liceu. Ouvi os professores explicar pela décima quinta vez como reduzir uma fracção. Compreendo-o. "Não, Sra. Smith, eu não mostrei o meu trabalho. Fi-lo na minha cabeça..."

Maldito miúdo. Provavelmente, copiou-o. São todos iguais.

Fiz uma descoberta hoje. Encontrei um computador. Espera um segundo, isto é fixe. Ele faz o que eu quero. Se ele comete um erro, é porque o estraguei. Não é porque não gosta de mim...

Ou sente-se ameaçado por mim...

Ou pensa que sou um espertalhão...

Ou não gosta de ensinar e não deveria estar aqui...

Maldito miúdo. Tudo o que ele faz é brincar. São todos iguais.

E depois aconteceu... uma porta aberta para um mundo... correndo pela linha telefónica como a heroína através das veias de um viciado, um pulso electrónico é enviado, um refúgio das incompetências do dia-a-dia é procurado... uma placa é encontrada.

"É aqui... é aqui que eu pertenço..."

Conheço toda a gente aqui... mesmo que nunca os tenha conhecido, nunca tenha falado com eles, talvez nunca mais tenha notícias deles... Eu conheço-vos a todos...

Malditos miúdos. Voltar a amarrar a linha telefónica. São todos iguais.

Pode apostar que somos todos iguais!

fomos alimentados com comida de bebé na escola quando tivemos fome de bife... os pedaços de carne que deixou escapar foram pré-mordidos e sem sabor. Fomos dominados por sádicos ou ignorados pelos apáticos. Os poucos que tinham algo a ensinar encontraram-nos alunos dispostos, mas esses poucos são como gotas de água no deserto.

"Este é o nosso mundo agora... o mundo do electrão e do interruptor, a beleza do baud. Fazemos uso de um serviço já existente sem pagar pelo que poderia ser barato se não fosse gerido por comilões aproveitadores, e vocês chamam-nos criminosos. Nós exploramos... e vocês chamam-nos criminosos. Nós procuramos o conhecimento... e você chama-nos criminosos. Existimos sem cor de pele, sem nacionalidade, sem preconceitos religiosos... e vocês chamam-nos criminosos. Vocês constroem bombas atómicas, fazem guerras, assassinam, enganam e mentem-nos e tentam fazer-nos acreditar que é para o nosso próprio bem, mas nós somos os criminosos.

Sim, eu sou um criminoso. O meu crime é o da curiosidade. O meu crime é o de julgar as pessoas pelo que dizem e pensam, não pela sua aparência. O meu crime é o de ser mais esperto do que tu, algo que nunca me perdoarás. Eu sou um hacker, e este é o meu manifesto. Pode deter este indivíduo, mas não pode deter-nos a todos... afinal de contas, somos todos iguais.

Mentor

Manifesto do Hacker

8 de Janeiro de 1986

Actualmente, os próprios hackers utilizam o termo hacker para pessoas que têm excelentes conhecimentos de sistemas de informação e comunicação, sistemas informáticos, os seus sistemas operativos e outros programas, os seus princípios e mecanismos de rede, e são também excelentes programadores capazes de criar o seu próprio software, nomeadamente em muito pouco tempo. É o esforço para saber como funcionam as tecnologias de informação, aplicações ou meios técnicos, e para disponibilizar esta informação a outros utilizadores, qual é a força motriz e a filosofia de muitas pessoas. A capacidade de um hacker obter acesso a sistemas informáticos através dos seus próprios programas informáticos concebidos e escritos, mesmo fora dos métodos habituais de acesso (o que não significa necessariamente que a obtenção desse acesso deva ser motivada pela tentativa de causar danos, outros danos ou enriquecer de outra forma) é uma, e não a única capacidade.

Divisão de hackers

É a motivação para obter acesso atípico (não necessariamente ilegal), o método para realizar tal intrusão, a sua motivação e possível tratamento dos dados obtidos, quais são os factores-chave para distinguir estas pessoas nos três grupos básicos seguintes:

Chapéus brancos - estes são hackers que se infiltram num sistema usando vulnerabilidades de segurança do sistema precisamente para detectar estas lacunas na segurança e criar tais mecanismos e barreiras que deveriam impedir tais ataques. São frequentemente empregados ou colaboradores externos de empresas de renome que fazem negócios no campo das tecnologias de informação. A sua intrusão num sistema não causa danos ou outros danos aos utilizadores, pelo contrário, em muitos casos alertam o administrador de tal sistema infectado para falhas de segurança. A sua actividade é fundamentalmente não-destrutiva por natureza.

Chapéus pretos - basicamente o oposto dos hackers de chapéu branco. A sua motivação é uma tentativa de causar danos ou outros danos a um utilizador de um sistema infectado, ou de obter bens ou outros benefícios. Para além da violação efectiva de um sistema pirateado, outro elemento criminoso é evidente nas suas acções.

Chapéus cinzentos - esta é uma zona cinzenta de hackers, ou seja, pessoas que não fizeram o perfil para os dois grupos. Ocasionalmente, podem violar alguns direitos de outros ou princípios morais, mas as suas actividades não são principalmente motivadas pelo desejo de causar danos, como é o caso dos chapéus pretos.

Para além do acima referido, ou seja, a divisão mais comumente utilizada, é possível dividir os hackers em outros grupos com base nos seus motivos. Estes são: Script kiddies, hacktivists, hackers patrocinados pelo Estado, spy hackers, cyber terroristas, iniciantes (n00b), blue hat hackers, etc..[\[4\]](#)

Um factor chave na avaliação do hacking como uma potencial ameaça à segurança é determinar a razão das actividades do hacker (ver a divisão dos hackers). Em alguns casos, a pirataria informática pode constituir uma verdadeira ameaça de segurança, uma vez que é uma violação da segurança do sistema informático, ou uma violação da protecção ou exploração de vulnerabilidades do sistema. Pelo contrário, em outros casos, pode ser um complemento adequado para aumentar a segurança de um sistema como um todo ou para encontrar pontos fracos e vulnerabilidades.

Em geral, o hacking pode ser realmente descrito como qualquer intrusão não autorizada num sistema informático a partir do exterior, na maioria das vezes dentro da Internet. No entanto, nem todos os ataques de hackers são necessariamente um crime.

O perigo de actividades de hacking reside, entre outras coisas, no facto de, além de obterem acesso não autorizado a um sistema atacado (independentemente da motivação do hacker), estas pessoas criarem e utilizarem ferramentas de software altamente eficazes, cujo código fonte é frequentemente publicado posteriormente pelos próprios hackers, por exemplo, dentro dos mercados escuros. Isto pode levar a mais abusos em massa destes programas por utilizadores que não têm o controlo para criar eles próprios tais programas, mas devido à existência de ferramentas disponibilizadas desta forma, podem potencialmente causar danos relativamente significativos aos utilizadores de sistemas infectados. Através da Internet, é assim possível obter conjuntos muitas vezes completos de programas de software hacker contendo software básico e informações necessárias para a sua utilização, praticamente sem um conhecimento profundo do funcionamento destes programas.

Formas de hacking

A actividade real dos hackers compreende uma série de acções. As actividades típicas utilizadas pelos hackers incluem:

1. Engenharia social
2. Quebra de senha [\[5\]](#)
3. Escaneamento de portos [\[6\]](#)

4. Utilização de malware para se infiltrar num sistema informático
5. Phishing
6. Roteiro Cruzado de Sítios [\[7\]](#)
7. Escutas sobre comunicação [\[8\]](#)

Grupos de hackers e hackers bem conhecidos

Provavelmente o grupo hacker mais conhecido actualmente é o Anónimo, mas existem ou existiram outros grupos: [\[9\]](#)

- **Anónimo**
- **Brigada de Lagartos**
- **O Parafuso de Nível Sete**
- **Chaos Computer Club**
- **Lulzsec**
- **Exército Electrónico Sírio**
- **Globalhell**
- **Grupo Hacker do Programa de Crack em Rede**
- **Movimento Antisec**
- **Legião da Desgraça (1984-2000)**
- **Mestres da Enganação (1989-1993)**
- **Milw0rm, etc.**



Os **hackers mais conhecidos** incluem Jonathan James, Vladimir Levin, Gary McKinnon, John McAfee, Astra, Stephen Wozniak, James Kosta, Kevin Mitnick, Adrian Lamo, David L. Smith. [\[10\]](#)

Não há dúvida de que **nem toda a actividade hacker é legal**. Em relação à interferência com o sistema informático, os direitos humanos e liberdades fundamentais garantidos serão certamente violados.

Possibilidades de sanções penais na República Checa

Como mencionado acima, há uma série de acções ou ataques que podem ser classificados como hacking (começando com a quebra de senha e terminando com um complicado ataque de phishing que é combinado com a engenharia social e a utilização de malware).

As acções de um hacker, que consistem apenas na utilização das suas capacidades, devido às quais ele supera as medidas de segurança e ganha acesso a um sistema informático ou à sua parte, podem ser punidas de acordo com a **Secção 230(1)** (Acesso não autorizado ao sistema informático e ao portador de informação) do Código Penal.

No caso de formas combinadas de ataques, em que, por exemplo, é utilizado malware para infectar um computador, tal acção de um infractor deve também ser punida ao abrigo da **Secção 230 (2)** (Acesso não autorizado ao sistema informático e portador de informação) do Código Penal. Se o objectivo de um ataque for obter um benefício injustificado para si próprio ou para outro, ou limitar injustificadamente a funcionalidade de um sistema informático ou outro dispositivo técnico de processamento de dados, é também possível aplicar as disposições do **Artigo 230 (3)** do Código Penal.

Possibilidades de sanções penais na Polónia

O crime de hacking é regulado na Arte. 267§1 do Código Penal.

Quem, sem autorização, obtiver acesso a informações que não lhe sejam destinadas, abrindo uma carta fechada, ligando-se à rede de telecomunicações ou quebrando ou contornando a segurança electrónica, magnética, informática ou outra segurança especial da mesma, será sujeito a uma multa, à pena de restrição de liberdade ou à pena de privação de liberdade por um período máximo de 2 anos.

A violação da segurança electrónica é um dos elementos estatutários de um crime nos termos do Artigo 267 (1) do Código Penal. "A segurança de uma conta com uma senha (código) é um obstáculo no acesso à informação por parte de uma pessoa não autorizada. A superação deste obstáculo através da utilização de um código de acesso pelo perpetrador contra a vontade da pessoa autorizada deve ser tratada como uma violação da segurança electrónica. A utilização de tal código (senha) por uma pessoa não autorizada contra a vontade do proprietário da conta quebra o obstáculo electrónico que protege o acesso a uma conta bancária ou a uma conta de utilizador num portal da Internet" (acórdão do Tribunal Distrital em Świdnica de 10 de Abril de 2019, número de referência: IV Ka 112/19). As marcas deste crime incluem, para além de "quebrar ou contornar a segurança electrónica, magnética, informática, que consiste na remoção de estruturas especiais, coberturas que são utilizadas para impedir o acesso à informação armazenada no sistema", a disposição também abrange a quebra de salvaguardas de informação específicas que não sejam electrónicas, magnéticas ou informáticas, o que significa que se trata de tais salvaguardas, cuja remoção exige que o perpetrador tenha conhecimentos especializados ou disponha de ferramentas especializadas. Em qualquer caso, a quebra da segurança deve causar algumas dificuldades - então pode assumir-se que tal segurança é de natureza "especial". Quebrar a segurança pode ser uma interferência directa no sistema de segurança, normalmente destruindo-o, ou

contornando a segurança sem fazer qualquer interferência no mesmo. Para a implementação das características da Arte. 267 §1, é necessário quebrar tal segurança, cuja principal função é proteger a informação contra o acesso não autorizado à mesma. De acordo com o acórdão do Tribunal Distrital em Świdnica de 10 de Abril de 2019, número de referência: IV Ka 112/19, "a essência da infracção ao abrigo do art. 267 §1. 267 §1 do Código Penal é que o perpetrador não conhece o método de segurança (por exemplo, códigos de acesso a informação específica ou o conteúdo das palavras-passe) após a sua aplicação, tomando determinadas acções (incluindo, por exemplo, decifrar o código ou palavra-passe para aceder à informação) ou quebrar essa segurança especial ou segurança especial é evitada. Não se trata de um crime ao abrigo da Arte. 267 §1 do Código Penal "obter informações para as quais não tenham sido tomadas medidas de protecção, a menos que consista na ligação a uma rede de telecomunicações".

Resumindo as considerações anteriores, segue-se que, de acordo com o acórdão do Tribunal Administrativo de Szczecin de 14 de Outubro de 2008, número de referência: II AKa 120/08, "uma pessoa não comete um crime ao abrigo da Arte. 267 §1 do Código Penal, se tiver obtido acesso não autorizado à informação sem quebrar ou contornar um elemento de segurança, mesmo que o faça por engano". De acordo com o acórdão do Tribunal Distrital em Świdnica de 10 de Abril de 2019, número de referência: IV Ka 112/19, decorre do acima exposto que "obter acesso, sem autorização, à informação referida no art. 267 §1 do Código Penal, por exemplo, utilizando uma palavra-passe fornecida ou previamente partilhada pela parte lesada, ou por exemplo, uma palavra-passe recordada por um navegador web, ou deixando o computador com a palavra-passe de uma determinada conta introduzida e após isso entrar no sistema não pode ser considerada uma violação da palavra-passe, pelo que o acima exposto não constitui uma infracção nos termos do art. 267 §1 do Código Penal". A infracção de hacking é processada a pedido da parte lesada.

Possibilidades de sanções penais em Portugal

Em si mesmo, o acesso ilegal a um sistema informático é punido (Art. 6(1) da Lei sobre o Cibercrime). Além disso, a superação das medidas de segurança e/ou o ganho de um ganho injustificado não são exigidos como elementos objectivos, sendo considerados como infracções agravadas (Art.6(3) e (4)).

Como foi dito anteriormente, a criação, distribuição ou divulgação ilegal de qualquer programa informático, instrução executável, código ou dados destinados a executar um acesso ilegal a um sistema informático é penalizada como sendo um acesso ilegal (Art. 6(2) da Lei sobre o Cibercrime).

[1] Para mais detalhes ver, por exemplo, GRIFFITHS, Mark. Criminalidade Informática e Hacking: uma questão séria para a Polícia? *The Police Journal*, 2000, vol. 73, No. 1, pp. 18-24.

YAR, Majid. Hacking informático: Apenas mais um caso de delinquência juvenil? *The Howard Journal*, 2005, vol. 44, No. 4, pp. 387-399.

[2] Este termo pode ser traduzido de muitas maneiras e precisa de ser baseado no contexto. No jargão americano, isto significava originalmente cavalgar sem rumo a cavalo. Um "hack" também se referia a uma solução simples para um problema. Subsequentemente, significava cometer algum erro por parte de estudantes universitários.

[3] NÍVEL, Steven. *Hackers: Heróis da Revolução Informática* Sebastopol, CA: O'Reilly Media, pp. 32-41. ISBN 978-1449388393. Também disponível online: <https://e11c1b148f6c7c56754c9184e0d1c52ac4d888f9-www.googleusercontent.com/host/0ByAMXZl2-PZ0WjBPYmhaWVVRNOE>

[4] Para mais detalhes, ver, por exemplo SHNEIER, Bruce. *Os Sete Tipos de Hackers*. [online]. [cit.16.8.2015]. Disponível a partir de: https://www.schneier.com/blog/archives/2011/02/the_seven_types.html

7 Tipos de Motivações Hacker. [online]. [cit.16.8.2015]. Disponível em: <https://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/>

7 Tipos de Hackers que Deve Conhecer. [online]. [cit.16.8.2015]. Disponível em: <https://www.cybrary.it/0p3n/types-of-hackers/>

[5] É o processo de obtenção de uma senha para um sistema informático. As seguintes são normalmente utilizadas para decifrar palavras-passe:

- Adivinhar uma senha pela força bruta (testar uma senha. Uma senha suficientemente forte é uma prevenção);
- Adivinhar uma palavra-chave com base em certos conhecimentos sobre um utilizador (obtidos, por exemplo, em redes sociais, etc.);
- Utilização de um dicionário de palavras-passe de uso corrente (ataque de dicionário);
- Pedir a palavra-passe ao administrador do sistema fazendo-se passar por um utilizador autorizado (Um atacante faz-se passar por um utilizador esquecido e tenta recuperá-la).
- Captura de palavras-passe de comunicações em rede não encriptadas ou insuficientemente encriptadas entre o sistema informático e um utilizador
- Pesquisa de palavras-passe em ficheiros de dados armazenados por um sistema

[6] Este é um método que detecta portas de rede abertas num sistema informático que está ligado a uma rede informática. Com base nesta descoberta, é possível determinar quais os serviços que estão a correr no sistema informático (por exemplo, servidor web, servidor ftp, etc.). O ataque real é então centrado nos serviços em execução detectados, com base nas suas vulnerabilidades.

[7] Este é um ataque de intrusão de website. Este tipo de ataque utiliza elementos activos (scripts) no website, nos quais é inserido código malicioso e depois oferecido à vítima.

Uma das acções menos comuns, mas ainda mais perigosas, é explorar a vulnerabilidade de uma aplicação web para executar malware dentro do navegador de uma vítima. A vítima é então incapaz de detectar tal comportamento. O código malicioso corre o mesmo que o resto da página, e o atacante tem permissão para assumir as permissões do navegador dentro do sistema.

Para mais detalhes, ver por exemplo OWASP, XSS [online]. [cit.15.7.2016]. Disponível em: [https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))

[8] Ver capítulo 4.12 Sniffing.

[9] Para mais detalhes, ver por exemplo *10 Grupos de Hacking Mais Notórios*. [online]. [cit.15.7.2016]. Disponível em: <https://www.hackread.com/10-most-notorious-hacking-groups/>

Figura retirada de [online]. [cit. 15.7.2016]. Disponível a partir de:

http://img02.deviantart.net/a2fd/i/2012/330/7/5/we_are_anonymous_by_mrj_5412-d5mb6xc.jpg

[10] Para mais detalhes, ver por exemplo *10 hackers mais notórios de todos os tempos*. [em linha]. [cit.15.7.2016]. Disponível a partir de: <https://hacked.com/hackers/>

Nejznámější počítačové hackeři a jejich útoky. [online]. [cit.15.7.2016]. Disponível a partir de: <https://www.stream.cz/top-5/10004402-nejznamsi-pocitacovi-hackeri-a-jejich-utoky>

4.10. Cracking

O termo **cracking** está associado ao termo hacking, por vezes até estes termos são incorrectamente confundidos pelo público ou nos meios de comunicação social. O termo pode ser traduzido para checo como "louskání" ou "pukání". Em termos de conteúdo, o termo cracking significa quebrar ou contornar os elementos de protecção de um sistema informático, programas ou aplicações, com a intenção da sua posterior utilização não autorizada.

Os crackers são frequentemente hackers da categoria de chapéu preto, ou seja, aqueles que fazem descobertas em sistemas numa tentativa de causar danos a um utilizador, obter informações, ou enriquecer-se a si próprios ou a outros. Além disso, o cracking está principalmente associado à violação de direitos de autor e direitos conexos. Neste sentido, o cracking é um acto que consiste em contornar elementos de protecção que impedem a criação de cópias ou a utilização ilegal de programas de computador e produtos musicais ou cinematográficos (filmes ou CDs de música, DVDs, etc.). Estes elementos de segurança são utilizados como meios de protecção dos direitos de autor no sentido da Secção 43 (1) da Lei dos Direitos de Autor, com as alterações que lhe foram introduzidas.

Uma das formas de cracking é o "**cracking de senha**" utilizado para determinar a senha de acesso a um sistema informático, sistema ou programa licenciado. Quando se trata de violação de direitos de autor, um cracker geralmente cria um keygen ou crack^[1], o que permite a utilização subsequente do programa. Programas modificados desta forma são normalmente partilhados em fóruns warez ou redes P2P.

Possibilidades de sanções penais na República Checa

As acções de um infractor, dentro das quais a protecção de um sistema ou programa informático é violada, com a intenção de obter informações e a sua subsequente utilização não autorizada, cumprem os elementos objectivos de uma infracção penal nos termos da **Secção 230 (1) ou (2)** (Acesso não autorizado ao sistema informático e ao portador de informações) do Código Penal. Se o objectivo de um ataque de cracking for obter um benefício injustificado para si próprio ou para outro, é também possível aplicar as disposições do **artigo 230 (3)** do Código Penal.

A responsabilidade penal nos termos da **Secção 231** (Medidas e armazenamento do dispositivo de acesso e palavra-passe para o sistema informático e outros dados deste tipo) do Código Penal também não está excluída. Durante a distribuição de uma obra protegida por direitos de autor, é cumprida a **Secção 270** (Violação dos direitos de autor, direitos relacionados com os direitos de autor e direitos sobre a base de dados) do Código Penal.

Possibilidades de sanções penais na Polónia

Aplicam-se as mesmas leis que para o hacking.

Possibilidades de sanções penais em Portugal

Como mencionado, a criação, distribuição ou divulgação ilegal de qualquer programa informático, instrução executável, código ou dados destinados a executar um acesso ilegal a um sistema informático é penalizada como sendo um acesso ilegal (Art. 6(2) da Lei sobre o Cibercrime), como infracção agravada se o infractor tivesse acesso a um segredo comercial ou a dados confidenciais, o mesmo acontecendo no caso de um benefício relevante injustificado (Art. 6(4) da Lei sobre o Cibercrime).

Mais uma vez, a evasão de quaisquer medidas tecnológicas eficazes relacionadas com a informação de gestão de direitos é criminalizada (Arts. 217 a 219 e 224-224 do Código dos Direitos de Autor e Direitos Conexos).

^[1]**Keygen** - Gerador de chaves. Programa gerador de números de série ou outros dados. **Crack** - um programa utilizado para remover ou reduzir a funcionalidade de elementos de protecção de outro programa.

4.11. Pirataria na Internet (informática)

Cada autor tem o direito de determinar como a sua obra será tratada.

Se eu não concordar com os termos de utilização da obra,

compreendê-los ou conhecê-los,

Tenho o direito de não utilizar o trabalho.

Jan Kolouch

O termo pirataria na Internet é um termo geral que abrange o crime, que viola os direitos de propriedade intelectual (muitas vezes limitado aos direitos de autor). Só com a expansão dos sistemas informáticos e especialmente com o advento da Internet podemos falar de pirataria em massa como uma das formas mais difundidas de cibercriminalidade.

A violação dos direitos de propriedade intelectual, em particular dos direitos de autor e direitos conexos, é actualmente uma das questões mais prementes no ambiente das tecnologias da informação.

4.11.1. Direito de propriedade intelectual

Em relação à pirataria na Internet, é primeiro necessário definir a questão da propriedade intelectual, especialmente os direitos de autor. Esta definição é necessária para compreender a diferença entre as acções legais e ilegais das pessoas que estão activas na Internet.

Um direito de propriedade intelectual é um bem intangível, a chamada "propriedade intangível", que é o **resultado da actividade criativa de uma pessoa**. Este direito é **independente do substrato material** (pode portanto ser utilizado em qualquer altura e em qualquer parte do mundo) desde que seja **único, irrepetível e suficientemente original**.

Os direitos de propriedade intelectual podem ser divididos em duas áreas:

1) **Direitos de autor** (proteger, por exemplo, obras literárias e artísticas originais, composições musicais, emissões televisivas, programas de computador, bases de dados, criações publicitárias, multimédia, etc.)

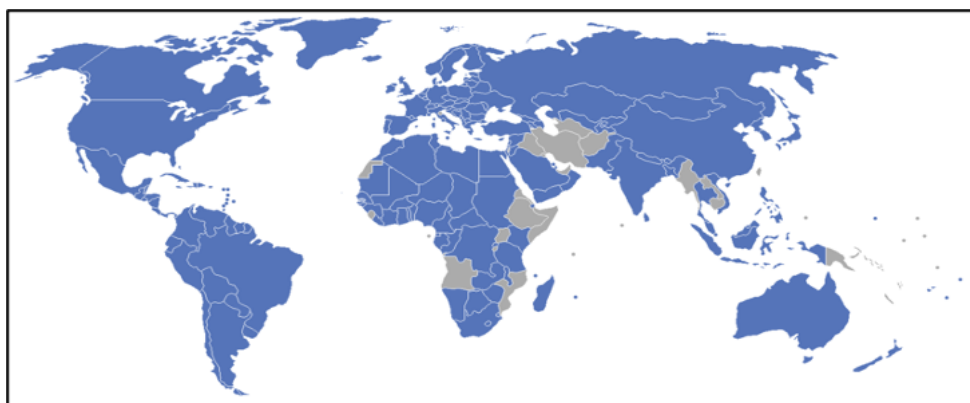
2) **Direitos industriais** (proteger, por exemplo, patentes de invenções, desenhos, modelos industriais, marcas, origem geográfica, etc.)

Em termos do foco desta monografia, tratarei principalmente apenas dos direitos de autor e das interferências com este direito.

4.11.2. Quadro legislativo

A protecção dos direitos de autor começou a ser abordada a nível internacional no século XIX, e os documentos jurídicos mais importantes que lhe dizem respeito incluem:

· **Convenção de Berna para a Protecção das Obras Literárias e Artísticas**^[1] (1886), posteriormente complementada e alterada [1908 (Berlim), 1928 (Roma), 1948 (Bruxelas), 1967 (Estocolmo), 1971 (Paris)]. Desde 1967, tem sido gerida pela **OMPI** (*Organização Mundial da Propriedade Intelectual*).



Lista de estados. Os Estados que adoptaram a Convenção de Berna estão marcados a azul.^[2]

· Acordo sobre Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio, que é um dos anexos do Acordo que instituiu a Organização Mundial do Comércio (OMC) – ver Notificação nº 191/1995 Sb., (**TRIPS - Aspectos dos Direitos de Propriedade Intelectual Relacionados com o Comércio**)

· Convenção Internacional para a Protecção dos Artistas Intérpretes ou Executantes, dos Produtores de Fonogramas e dos Organismos de Radiodifusão de 26th de Outubro de 1961 (Decreto n.º 192/1964 Sb., emendado pelo Corrigendum n.º 157/1965 Sb.) – **Convenção de Roma**

· Tratado da Organização Mundial da Propriedade Intelectual sobre Direitos de Autor Genebra 1996 de 20 de Dezembro de 1996 (ver Not. No. 33/2002 Sb. dos Tratados Int.), (**WCT - WIPO Copyright Treaty**)

· Tratado sobre Prestações e Fonogramas da Organização Mundial da Propriedade Intelectual Genebra 1996 de 20 de Dezembro de 1996 (ver Not. No. 48/2002 Sb. dos Tratados Int.), (**WPPT - WIPO Performances e Fonogramas Tratado**)

- Convenção para a Protecção dos Produtores de Fonogramas contra a Reprodução Não Autorizada dos seus Fonogramas de 29 de Outubro de 1971 (ver Decreto 32/1985 Sb.) - **Convenção de Genebra**
- Convenção Geral sobre os Direitos de Autor revista em Paris em 24 de Julho de 1971 (ver Decreto nº 134/1980 Sb.)
- Directiva 91/250/CEE do Conselho, de 14 de Maio de 1991, relativa à protecção jurídica dos programas de computador,
- Directiva 92/100/CEE do Conselho, de 19 de Novembro de 1992, relativa ao direito de aluguer, ao direito de comodato e a certos direitos conexos aos direitos de autor em matéria de propriedade intelectual, com as alterações que lhe foram introduzidas,
- Directiva 93/83/CEE do Conselho, de 27 de Setembro de 1993, relativa à coordenação de determinadas disposições em matéria de direitos de autor e direitos conexos aplicáveis à radiodifusão por satélite e à retransmissão por cabo,
- Directiva 93/98/CEE do Conselho, de 29 de Outubro de 1993, relativa à harmonização do prazo de protecção dos direitos de autor e de certos direitos conexos, com as alterações que lhe foram introduzidas,
- Directiva 96/9/CE do Parlamento Europeu e do Conselho, de 11 de Março de 1996, relativa à protecção jurídica das bases de dados,
- Directiva 2001/29/CE do Parlamento Europeu e do Conselho, de 22 de Maio de 2001, relativa à harmonização de certos aspectos do direito de autor e dos direitos conexos na sociedade da informação,
- Directiva 2001/84/CE do Parlamento Europeu e do Conselho, de 27 de Setembro de 2001, relativa ao direito de sequência em benefício do autor de uma obra de arte original,
- Directiva 2004/48/CE do Parlamento Europeu e do Conselho, de 29 de Abril de 2004, relativa ao respeito dos direitos de propriedade intelectual.
- Convenção n.º 185 do Conselho da Europa sobre Cibercriminalidade.

4.11.3. Ataques

Vários termos têm sido utilizados no ambiente da Internet para o fenómeno da violação dos direitos de autor e direitos conexos. Os termos **pirataria de software** (para violação de direitos de autor em relação a programas de computador) e **pirataria audiovisual** (para violação de direitos de autor de obras audiovisuais - música e filme) são mais frequentemente utilizados. **No entanto, a base da pirataria de software e audiovisual é sempre uma violação de um dos direitos de autor ou direitos relacionados com os direitos de autor.** Um termo geral que abrange a pirataria de software e audiovisual é pirataria na Internet (por vezes também informática).

Os crimes contra a propriedade intelectual expandiram-se consideravelmente com o advento em massa da Internet. Os casos mais comuns de violação dos direitos de autor no ciberespaço são:

- *divulgação de uma obra por correio electrónico*, que é a forma mais fácil de distribuir pequenos ficheiros (especialmente obras literárias ou gráficas com direitos de autor),
- *publicação de uma obra num sítio web* sem o consentimento do autor. Esta é outra forma muito simples de infringir os direitos de autor. São publicados ficheiros mais pequenos (em termos de tamanho dos dados) e este comportamento ilegal é normalmente detectado muito cedo.
- *divulgação de uma obra carregando para um servidor especializado*, de onde é possível descarregar livremente as obras (por exemplo, Megaupload, Rapidshare),
- *divulgação de um trabalho utilizando redes Peer-to-Peer (P2P)*.^[3] Estas redes são capazes de transmitir/ partilhar enormes quantidades de dados (na ordem de vários GB a dezenas de TB). São os casos mais flagrantes de violação dos direitos de autor.
- *interferência com programas de computador, a fim de superar as medidas técnicas do detentor dos direitos de autor que impedem a realização de cópias de tais programas protegidos* (o chamado crack),
- *divulgação de um trabalho utilizando suportes de dados directamente entre utilizadores* (empréstimo e subsequente cópia de dados de DVD, HDD, etc., venda de suportes de dados e outros),
- *gravação directamente durante uma projecção e subsequente disseminação da gravação* (por exemplo, gravação de um trabalho cinematográfico directamente do ecrã) - camcording,
- *exibições não autorizadas de obras audiovisuais*,
- *uma aquisição efectiva de um trabalho informático*. Um programa de computador é especialmente protegido, e não é possível fazer cópias de tal obra, mesmo para uso pessoal, sem o consentimento dos titulares dos direitos de autor, na acepção da lei de direitos de autor,
- *utilização de um programa de computador em violação da licença*,
- e muito mais.

As formas mais comuns de pirataria audiovisual incluem, em particular, a distribuição não autorizada de obras audiovisuais através de redes informáticas, a gravação de obras cinematográficas directamente nas salas de cinema e a sua posterior "colocação" para descarga no ciberespaço, a distribuição de suportes originais com um filme ou música em violação de um acordo de licença, a produção e difusão de contrafacções de obras cinematográficas ou musicais originais e a exibição pública de obras cinematográficas em violação de um acordo de licença. Além disso, conduta que consiste na divulgação de produtos de software, intervenções em produtos de software, produção ilegal de produtos de software e utilização de produtos de software em violação de um acordo de licença. A violação dos direitos de autor será já uma aquisição não autorizada de um produto de software sem tratamento adicional.

A colocação de uma obra (independentemente de ser audiovisual ou software) no ciberespaço (**upload**) significa a divulgação da obra no sentido da lei de direitos de autor e (a menos que seja permitida pelo autor ou por outra pessoa autorizada) pode ser punível. **A utilização não autorizada de uma obra é também a publicação de uma ligação a um local no ciberespaço onde uma obra pode ser obtida.**

Para comparação com a legislação estrangeira, é adequado mencionar a lei francesa HADOPI,^[4] que deveria proteger contra a pirataria na Internet. De acordo com esta lei, foi criado um gabinete especial encarregado de detectar os downloads ilegais de material protegido por direitos de autor. Os utilizadores que descarregaram música e filmes da Internet gratuitamente (excluindo obras distribuíveis livremente) foram avisados três vezes, e se estes avisos não fossem ouvidos, a autoridade tinha o direito de os desligar da Internet por um período máximo de um ano.^[5] No entanto, mesmo uma lei tão rigorosa não limitava o número de descarregamentos ilegais de obras protegidas por direitos de autor. Ao mesmo tempo, contudo, levantou uma série de questões relativas à admissibilidade de interferência com direitos humanos e liberdades fundamentais sem uma decisão judicial.^[6] A lei HADOPI foi revogada a 10 de Julho de 2013.

O termo "Warez" aparece frequentemente em ligação com a pirataria na Internet. **Warez** é, muito simplesmente colocado, uma **forma de pirataria informática**, onde a tecnologia da informação é apenas um meio de acelerar a distribuição de cópias ilegais de obras protegidas por direitos de autor através da Internet. Os fóruns Warez são actualmente utilizados principalmente para descarregar cracks e keygens, bem como programas, filmes e música modificados completos. O produto final da cena warez chama-se **lançamento**. Para proteger a privacidade, os clientes dos fóruns warez utilizam servidores proxy e bouncers para mascarar o seu endereço IP, impedindo assim uma possível monitorização. A comunicação efectiva e a oferta de lançamento ocorre em salas privadas criadas para este fim na Internet, às quais apenas os membros do grupo têm acesso.

Possibilidades de sanções penais na República Checa

O fornecimento de ficheiros, quer dentro de redes warez ou P2P, pode ser punido ao abrigo da **Secção 270** (Violação de direitos de autor, direitos relacionados com direitos de autor e direitos de bases de dados), ou de acordo com a **Secção 231** (Medidas e armazenamento de dispositivos de acesso e palavras-passe para o sistema informático e outros dados deste tipo) do Código Penal.

Possibilidades de sanções penais na Polónia

As questões de propriedade intelectual na Polónia foram reguladas por dois actos jurídicos básicos: a Lei sobre Direitos de Autor e Direitos Conexos e a Lei sobre a Propriedade Industrial.

O Código Penal tem dois Artigos sobre a violação ou roubo de propriedade intelectual:

Artigo 115°. 1. Quem se apropriar da autoria ou enganar quanto à autoria total ou parcial de uma obra ou performance artística de outra pessoa, será sujeito a uma multa, à pena de restrição de liberdade ou à pena de privação de liberdade por um período até 3 anos.

E artigo 278° (roubo)

§ 1 Quem tomar os bens móveis de outrem para fins de apropriação estará sujeito à pena de privação de liberdade por um período compreendido entre 3 meses e 5 anos. § 2 A mesma pena será imposta a quem, sem o consentimento da pessoa autorizada, obtiver o programa de computador de outrem com o objectivo de obter um lucro material.

Possibilidades de sanções penais em Portugal

Em geral, tais actos são criminalizados como cópia não autorizada, distribuição e venda de obras e/ou como contrafacção de obras protegidas por direitos de autor (Arts. 195 e 196 do Código dos Direitos de Autor e Direitos Conexos).

Por outro lado, seria aplicável a reprodução ilegal de um programa informático protegido (art. 8° da Lei da Criminalidade Informática) e a reprodução ou comunicação ilegal de uma base de dados protegida por direitos de autor (art. 11° do Decreto-Lei nº 122/2000), sendo este o caso.

[1]Disponível em linha. [online]. [cit.15.7.2016]. Disponível de: <http://portal.gov.cz/app/zakony/zakonPar.jsp?page=0&idBiblio=34669&nr=133~2F1980&rpp=100#local-content>; <http://www.zakonyprolidi.cz/cs/1985-19>

[2]Bernská úmluva o ochraně literárních a uměleckých děl. [online]. [cit.15.7.2016]. Disponível em: https://cs.wikipedia.org/wiki/Bernská_úmluva_o_ochraně_literárních_a_uměleckých_děl. O mapa apresentado é apenas ilustrativo e não mostra a actual divisão geopolítica do mundo. Uma lista completa dos Estados que ratificaram o Tratado da OMPI pode ser encontrada em: http://www.wipo.int/treaties/en/ShowResults.jsp?lang=en&treaty_id=15

[3] Ao ligar-se ao P2P, um utilizador, por defeito, começa automaticamente a partilhar o seu conteúdo com outros utilizadores (normalmente desconhecido para ele). Tipicamente, ao descarregar, o carregamento do material descarregado é automaticamente definido.

[4]HADOPI (Alta Autoridade para a Protecção dos Direitos de Autor e Divulgação de Obras na Internet), P: *Loifavorisant la diffusion et la protection de la creation sur l'Internet*.

[5] O Instituto não precisou de uma decisão do tribunal para esta decisão. Com base no parecer do Tribunal Constitucional Fr. de 22 de Novembro de 2009, é necessária a aprovação do tribunal para a desconexão.

[6]Para mais detalhes, ver por exemplo *Francie zakáže internetové pirátství*. [online]. [cit.15.7.2016]. Disponível a partir de: <http://www.blisty.cz/2009/5/13/art46807.html>

Přísný zákon proti hudebním a filmovým pirátům Francii nepomohl. [online]. [cit.15.7.2016]. Disponível a partir de: http://technet.idnes.cz/prisny-zakon-proti-hudebnim-a-filmovym-piratum-francii-nepomohl-phi/-sw_internet.asp?c=A100330_095705_sw_internet_vse

A França deixa cair a controversa "lei Hadopi" depois de ter gasto milhões. [em linha]. [cit.15.7.2016]. Disponível em: <https://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy> etc.

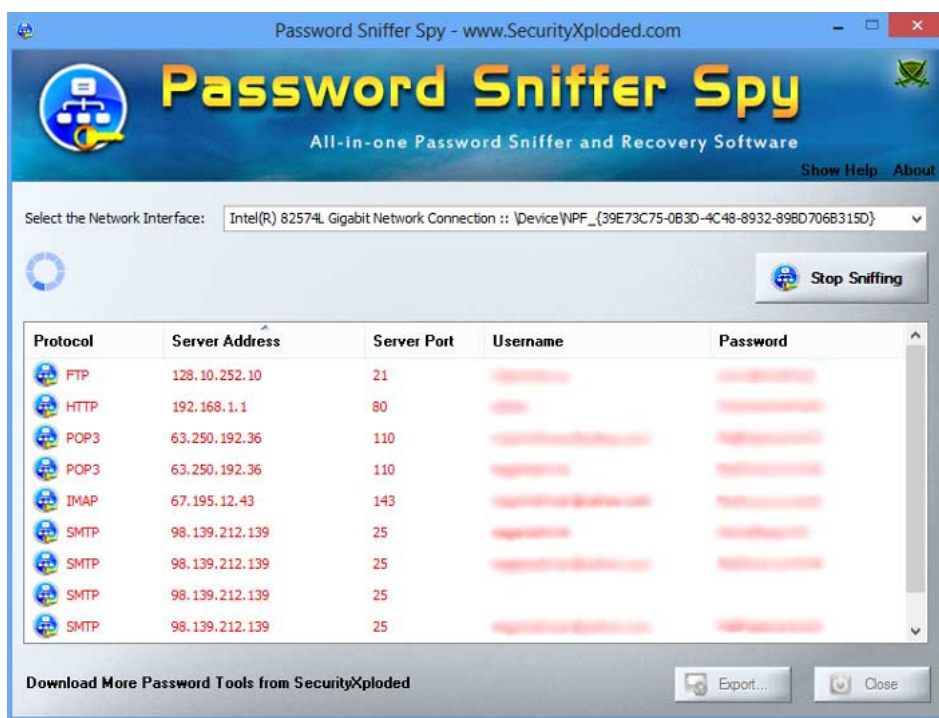
4.12. Sniffing

Sniffing é um método de interceptação ilegal de dados que passa através de uma rede informática durante a comunicação entre um serviço fornecido e um sistema informático através de um **sniffer**.^[1]

Tecnicamente, farejar significa captar e ler pacotes TCP. Do ponto de vista da segurança, o sniffing também pode ser descrito como monitorização da rede ou monitorização do funcionamento da rede, e é uma das ferramentas padrão para o diagnóstico da rede, ou diagnóstico de anomalias no funcionamento da rede. A monitorização da rede é então capaz de exibir, por exemplo, comunicação não normalizada de um sistema informático infectado com malware, etc. A própria actividade dos administradores da rede no caso de monitorização da rede não é ilegal (a menos que cometam outras acções que possam estabelecer uma possível responsabilidade legal - como a instalação de um keylogger ou outro malware num sistema informático sem o conhecimento do utilizador), uma vez que permite manter e gerir uma rede informática.

São utilizadas várias ferramentas para monitorizar o tráfego da rede (por exemplo, Wireshark^[2], NetWorx, monitor de rede PRTG, etc.).

Para que o sniffing seja abrangido por uma das categorias de cibercrime, é necessário que uma pessoa que execute esta actividade aja ilegalmente, normalmente sem o consentimento ou conhecimento de um utilizador. Utilizando dados capturados pelo sniffing, um atacante é capaz de extrair e compor informações sensíveis sobre um utilizador, tais como dados de login (nome de utilizador e palavra-passe), e-mail ou comunicação VOIP, informações sobre serviços usados, etc. O malware sob a forma de Trojans, keyloggers ou spyware também pode ser utilizado para farejar.



Senha Sniffer Spy. Nomes e palavras-passe estão desfocados.^[3]

Possibilidades de sanções penais na República Checa

Esta actividade poderia praticamente ser descrita como **intercepção e registo ilegal do tráfego de telecomunicações**. A conduta acima descrita irá certamente interferir com os direitos humanos e liberdades fundamentais, em particular o **Artigo 13 da Carta**, e é **completamente indiferente se a interceptação ilegal é realizada por um atacante externo ou por um administrador de rede**. De acordo com as normas do direito penal, seria possível subsumir tal conduta ao abrigo do **artigo 182(1)** (Violação do sigilo das mensagens transportadas) do Código Penal, e em caso de abuso de informação obtida desta forma, poderia ser uma infracção penal ao abrigo do **artigo 182(2)** do Código Penal. Se a referida actividade ilegal for executada por um empregado do operador dos serviços postais, dos serviços de telecomunicações ou do sistema informático ou por qualquer outra pessoa que exerça actividades de comunicação, poderá satisfazer os elementos objectivos de acordo com o **Artigo 185 (5)** do Código Penal.

Possibilidades de sanções penais na Polónia

Na Polónia, o farejar é um delito punível de acordo com a lei:

Violação do segredo de comunicação (sniffing) - Artigo 267 § 3 do Código Penal.

Possibilidades de sanções penais em Portugal

Tal acto é colocado no âmbito da Intercepção Ilegal (art. 7 da Lei de Crimes Cibernéticos), mas também o acesso e a partilha de qualquer conteúdo pode ser considerado uma Violação de correspondência ou telecomunicações (art. 194 do Código Penal).

^[1] Sniffing é uma palavra inglesa que significa bisbilhotar ou espiar por aí. Um farejador é então alguém que fareja, bisbilhotar ou espiar em redor.

[2] Mais detalhes sobre a utilização de Wireshark, ver por exemplo *como utilizar Wireshark para capturar, filtrar e inspeccionar Pacotes*. [online]. [cit.15.7.2016]. Disponível a partir de: <http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/>

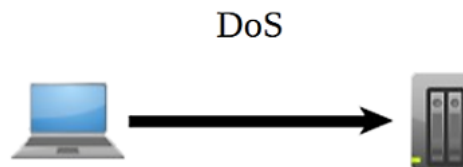
[3] *Senha Sniffer Spy*. [online]. [cit.18.8.2016]. Disponível a partir de: <http://securityxploded.com/password-sniffer-spy.php>

4.13. Ataques DoS, DDoS, DRDoS

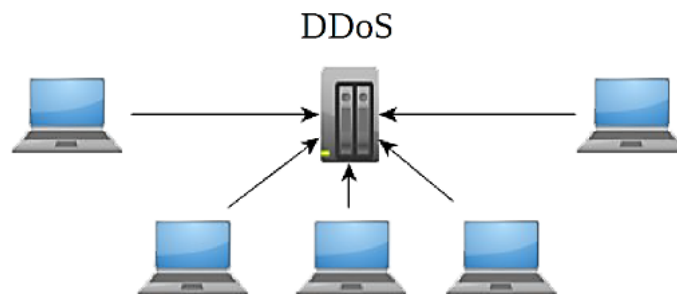
O termo DoS é uma abreviatura de "**negação de serviço**". Esta é uma das formas de ataque a um serviço (Internet), cujo objectivo é desactivar ou reduzir o desempenho do equipamento técnico infectado.^[1] Este ataque é levado a cabo inundando um sistema informático comprometido (ou elemento de rede) com pedidos repetidos de acções a serem tomadas pelo sistema informático. Este ataque também pode ser implementado através de canais de informação de inundação entre o servidor e o computador do utilizador ou através de recursos do sistema sem inundação. Um sistema exhibe principalmente infecção de um ataque DoS através de uma desaceleração invulgar do serviço, indisponibilidade geral ou momentânea do serviço (por exemplo, websites), etc.

A diferença entre ataques DoS, DDoS e DRDoS reside principalmente na forma como o ataque é conduzido. Para maior clareza, os números que demonstram o método do ataque estão ligados aos tipos individuais de ataque.

No caso da **DoS (Negação de Serviço)**, a fonte do ataque é uma só. Este tipo de ataque é relativamente fácil de defender, uma vez que é possível bloquear o tráfego da origem do ataque.

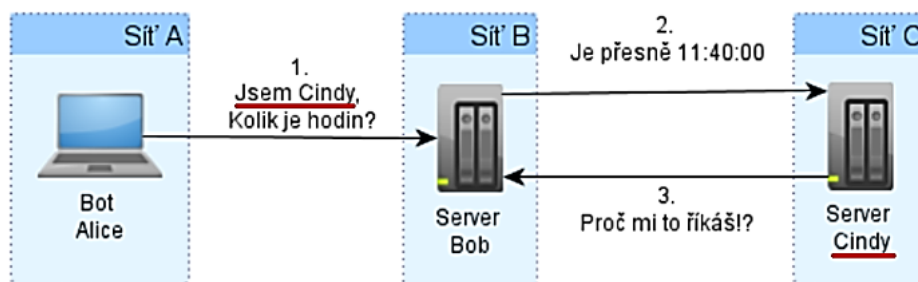


Com a **Negação Distribuída de Serviço (DDoS)**, o sistema informático alvo está congestionado pelo **envio de pacotes de múltiplos sistemas informáticos em vários locais, tornando difícil a defesa e identificação do atacante.**^[2] Botnets ou actividades de utilizadores que apoiam uma certa campanha online são muito frequentemente utilizados para este tipo de ataques (ver abaixo - Anónimos e LOIC).



No caso de **DRDoS (Distributed Reflected Denial of Service)**, é um ataque de DoS distribuído falsificado que utiliza um chamado mecanismo de reflexão. O ataque consiste em enviar falsos pedidos de ligação a um grande número de sistemas informáticos, que depois respondem a estes pedidos, mas não ao iniciador da ligação, mas à vítima. Isto porque os pedidos de ligação falsificados têm o endereço da vítima como endereço de origem, que é depois inundado com respostas a esses pedidos. Muitos sistemas informáticos tornam-se assim um participante involuntário num ataque, de facto, respondendo correctamente a um pedido de ligação.

Os ataques DoS, DDoS, DRDoS utilizam muito frequentemente bugs como o sistema operativo, programas em execução ou protocolos de rede - UDP, TCP, IP, http, etc.



Texto sobre a figura:

Rede A, Bot Alice

1. Eu sou Cindy, Que horas são?

Rede B, Servidor Bob

2. São exactamente 11:40:00

Rede C, Servidor Cindy

3. Porque me estás a dizer isto!?

Existem vários métodos básicos de ataque DoS ou DDoS, os mais conhecidos são os seguintes:

- Inundação com comando ping (*Ping-Flood*)

Devido ao Protocolo de Mensagem de Controlo da Internet e à ferramenta Ping (Packet Internet Groper), é possível utilizar o comando "ping" para determinar a "vida" de um sistema informático com um dado endereço IP e para detectar o tempo de resposta de tal sistema. Como parte do ataque Ping-Flood, uma vítima é inundada com um grande número dos chamados pacotes de pedidos de eco ICMP, aos quais a vítima começa a responder - enviando os chamados pacotes de resposta de eco ICMP. Um agressor espera que isto ultrapasse a largura de banda da vítima (para recepção e envio de dados). O ataque real pode ser ainda mais intensificado através da definição da opção de inundação dos pacotes ICMP emissores de ping. Os pacotes são então enviados sem esperar por uma resposta. Se o sistema informático alvo tiver um mau desempenho, pode ser tornado inacessível.

- Inundação de recursos livres do sistema (*SYN-Flood*)

SYN-Flood é um tipo de ataque em que um agressor tenta sobrecarregar a sua vítima com um grande número de pedidos de ligação. Um atacante envia uma sequência de pacotes com um comando SYN (pacotes SYN) para o sistema informático alvo (vítima), com o sistema alvo a responder a cada pacote SYN enviando um pacote SYN-ACK, mas o atacante já não responde. O sistema informático de destino espera pelo reconhecimento final, o chamado pacote ACK do iniciador da ligação (atacante) e detém os recursos atribuídos para esta ligação, mas tem um número limitado. Isto pode esgotar os recursos do sistema do alvo do ataque.^[3]

- Falsificação do endereço de origem (*IP spoofing*)

IP Spoofing é uma actividade que consiste na falsificação de um endereço de origem de pacotes enviados, quando um atacante que inicia uma ligação a partir da máquina A com o **IP address a.b.c.d** insere, por exemplo, o **endereço IP d.c.b.a** como endereço de origem e envia-os para um alvo B. O alvo B responde então a este endereço de origem, ou seja, a resposta não é endereçada ao endereço IP a.b.c.d, mas ao endereço IP **d.c.b.a**. Usando este método, é possível piorar os ataques (intensificar os ataques), tais como DoS, DDoS. Um atacante usa esta técnica quando não precisa de uma resposta do seu alvo ao seu pedido de ligação, apenas o quer enganar. Quando um atacante especifica o endereço IP do alvo do seu ataque (por exemplo, a.a.a.a) como o endereço IP de origem nos pacotes enviados e envia os pacotes para muitos outros sistemas informáticos (endereços IP), estes respondem então ao sistema informático a.a.a.a. Desta forma, um ataque DRDoS é levado a cabo.

- Ataque de Smurf

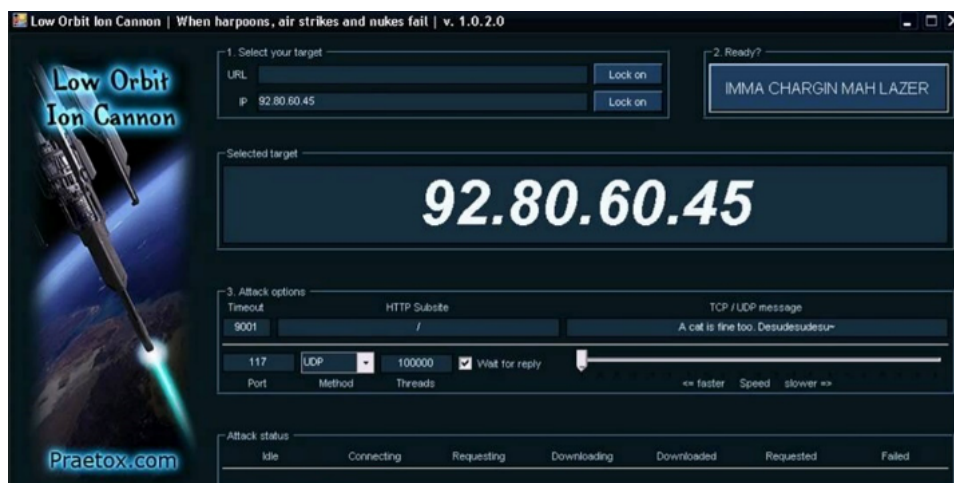
Este ataque é executado através de uma má configuração do sistema, que permite a transmissão de pacotes para todos os computadores ligados à rede de computadores através do endereço de difusão.

O objectivo dos ataques DoS/DDoS **não é** normalmente **infectar um computador** ou sistema informático, ou **ultrapassar a protecção de segurança com uma palavra-passe** que o proteja, mas sim **sobrecarregá-lo ou desactivá-lo temporariamente** utilizando uma série de pedidos repetidos. Normalmente, isto irá restringir ou bloquear o acesso aos serviços.

Para poder processar legalmente um "agressor" que tenha utilizado ataques DoS ou DDoS, é necessário determinar se a **sua conduta foi ilegal** e, em caso afirmativo, quão grave foi a conduta. A questão é que um ataque DDoS na sua natureza pode ser, por exemplo, a actividade completamente acima do quadro dos utilizadores da Internet que tentam ligar-se de uma só vez (num curto período de tempo) a um servidor web de uma empresa que oferece descontos nos bilhetes e, por exemplo, anunciou que a partir das 12.00 haverá uma redução abrangente dos bilhetes em 75%. Ou pode ser o acesso de um grande número de utilizadores a um serviço web de um dos meios de comunicação populares que noticiam eventos importantes ou dignos de notícia - a inauguração de um novo presidente, a morte de uma pessoa proeminente, etc. Se o sistema informático alvo (servidor web) não estiver suficientemente dimensionado ou estiver mal configurado (não é capaz de lidar com a quantidade de acesso necessária), irá "colapsar" de forma semelhante a um ataque DDoS visado. A questão então é se os utilizadores que tentaram entrar no referido website no momento determinado e assim praticamente causaram o encerramento do serviço em questão devem ser punidos.

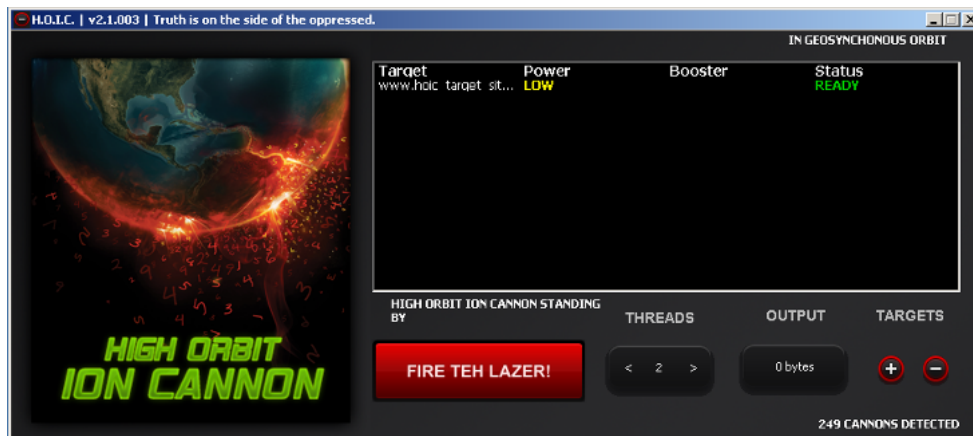
Creio que nos casos acima descritos, embora os utilizadores tenham causado um ataque DDoS maciço ao serviço de um fornecedor, não é realista ou sequer concebível punir estes "pseudo-atacantes" por qualquer instrumento legal, uma vez que a sua conduta não foi ilegal desde o início.

No entanto, um caso diferente seria uma situação em que os atacantes são chamados, por exemplo, através da Internet e num momento específico, devido à sua re-ligação ao serviço prestado, suprimem este serviço.^[4] Tais casos ocorreram, por exemplo, no contexto de protestos contra o ACTA (Acordo Comercial Anticontrafacção) em 2012, quando uma das opções para cometer estes ataques foi utilizar uma ferramenta distribuída a apoiantes anónimos, o LOIC (Low Orbit Ion Cannon).



LOIC (Canhão de íões de órbita baixa)^[5]

O sucessor imaginário do LOIC foi o software HOIC (High Orbit Ion Canon), que foi desenvolvido como um substituto do LOIC.



HOIC (High Orbit Ion Canon)[6]

A conduta dos atacantes neste caso é certamente ilegal, porque estes atacantes estavam conscientes ou pelo menos compreendiam que as suas acções interferiam com os direitos dos outros. Neste caso, seria possível utilizar os instrumentos do direito penal, administrativo e civil.

Devido à adopção da Convenção sobre o Cibercrime, o direito penal deve ser harmonizado e tais normas legais devem ser adoptadas, nos estados membros da UE e não só, que devem ser capazes de punir os ataques DoS ou DDoS pelo direito penal desse país. O que se segue exige protecção contra estes ataques e a implementação de medidas legislativas: Capítulo II - Medidas a tomar a nível nacional, Secção 1 - Infracções contra a confidencialidade, integridade e usabilidade dos dados e sistemas informáticos, Artigo 4 - Interferência com os dados, da Convenção:

1. Cada Parte tomará as medidas legislativas e outras que possam ser necessárias para estabelecer como infracção penal, em conformidade com a sua legislação interna, um dano intencional ilegal, apagamento, deterioração, alteração ou **supressão de dados informáticos**.
2. Uma parte pode reservar-se o direito de estipular que só considerará a conduta descrita no parágrafo 1 como criminosa se esta causar danos graves.

Possibilidades de sanções penais na República Checa

Decorre da redacção das disposições da **Secção 230 (2)** (Acesso não autorizado ao sistema informático e ao portador de informação) do Código Penal:

Quem tiver acesso a um sistema informático ou meio de informação e

- a) utiliza dados armazenados num sistema informático ou num suporte de informação sem autorização,
- b) Apaga ou destrói, danifica, modifica, **suprime** ou corrompe a qualidade dos **dados** armazenados num sistema informático ou num suporte de informação, ou inutiliza-os sem autorização...

Decorre desta disposição que um atacante que cometa um ataque DoS ou DDoS deve, para ser criminalmente responsável, **obter acesso não autorizado a um sistema informático e subsequentemente suprimir os dados nele contidos**. [7]

Neste caso, dois artigos distintos (Capítulo II, Secção 1, **Artigo 2 - Acesso Ilegal** e **Artigo 4 - Interferência com dados**) da Convenção sobre o Crime Cibernético foram fundidos numa única disposição.

O legislador tornou assim praticamente impossível punir os perpetradores de ataques DoS ou DDoS por meio do direito penal, uma vez que um infractor é obrigado a **obter acesso não autorizado ao sistema informático**. Esta interpretação jurídica, que exige a obtenção de acesso não autorizado a um sistema informático, permite assim que um infractor seja punido apenas pela conduta especificada na Convenção sobre a Criminalidade Cibernética no **Artigo 2 - Acesso Ilegal**: "Cada Parte tomará as medidas legislativas e outras que forem necessárias para assegurar que, nos termos do seu direito interno, o **acesso não autorizado à totalidade ou a qualquer parte de um sistema informático** constitui uma infracção penal quando cometida intencionalmente".

Do ponto de vista técnico, os ataques DoS ou DDoS **não** obtêm acesso a um sistema informático ou parte dele, ou pelo menos não é o objectivo principal. [8]

Pelas razões acima expostas, estou convencido da necessidade de incorporar na legislação checa um elemento objectivo separado do crime, que protegeria o sistema informático dos ataques DoS, DDoS, DRDoS, etc., e que respeitaria as disposições da Convenção sobre o Crime Cibernético. Seria possível utilizar, por exemplo, a seguinte redacção:

"Quem impede a utilização de um sistema informático sem autorização..."

Actualmente, seria teoricamente possível acusar os perpetradores de ataques DoS e DDoS por uma infracção penal ao abrigo da **Secção 228** (danos materiais) do Código Penal. [9] Contudo, uma condição para a utilização da instituição dos danos materiais teria de ser o facto de tal coisa (incluindo um sistema informático) ser destruída, danificada ou tornada inutilizável. No entanto, esta condição geralmente só se aplica a este tipo de ataque no que diz respeito a uma certa inutilização temporária.

Neste contexto, contudo, coloca-se também a questão de como e de que forma os danos reais serão quantificados em caso de danos a uma coisa e de quem será responsável. [10]

Outros elementos objectivos que um agressor que cometa um ataque DoS e DDoS poderia cometer em determinadas circunstâncias incluem a Secção 272 (Ameaça geral), Secção 273 (Ameaça geral devido a negligência) do Código Penal.

Relativamente à possível sanção penal de um perpetrador de ataques DoS ou DDoS, é também importante determinar (identificar) o infractor deste crime em particular. Resta saber **quem deve ser criminalmente processado como o infractor** que, por exemplo, causou a indisponibilidade de um determinado serviço (por exemplo, aplicação web).

Possibilidades de sanções penais na Polónia

Neste caso, é aplicável o Artigo 268 do Código Penal, que estabelece que:

§ 1 Quem, sem estar autorizado a fazê-lo, destruir, danificar, apagar ou alterar um registo de informações essenciais ou de outra forma impedir ou impedir consideravelmente uma pessoa autorizada de as conhecer, será sujeito a uma multa, a pena de restrição de liberdade ou privação de liberdade por um período até 2 anos.

Possibilidades de sanções penais em Portugal

Tais actos estão claramente sob o âmbito da sabotagem informática [interferência ilegal] (Art. 5(1) da Lei de Crimes Cibernéticos), possivelmente como ofensa agravada no caso de danos elevados ou interferência com infra-estruturas críticas ou outros serviços essenciais (Art. 5(5)).

[1] Para mais detalhes, por exemplo MARCIÁ-FERNANDÉZ, Gabriel, Jesús E. DÍAZ-VERDEJO e Pedro GARCÍA-TEODORO. Avaliação de um ataque de baixa taxa de DoS contra Servidores de Aplicação. *Computers & Security*, 2008, vol. 27, No. 7-8, pp. 335-354.

CARL, Glenn, Richard BROOKS e Rai SURESH. Detecção de Negação de Serviço com base em Wavelet. *Computers & Security*, 2006, vol. 25, No. 8, pp. 600-615

RAK, Roman e Radek KUMMER. Informační hrozby v letech 2007-2017. *Security magazín*, 2007, vol. 14, No. 1, pp. 3.

[2] Por exemplo, ataques do DoS aos sítios web da presidência, do parlamento, dos ministérios, dos meios de comunicação social e de dois bancos estónios - Estónia (2007). *A Estónia recupera de um ataque maciço de DDoS*. [em linha]. [cit. 4. 3.2010] Disponível a partir de:

http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htmhttp://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack

[3] Neste ponto é necessário mencionar o **aperto de mão** - um processo cuja tarefa é definir os parâmetros de um canal de comunicação entre dois sujeitos antes de iniciar a comunicação propriamente dita. Por exemplo, um aperto de mão é utilizado na Internet para abrir uma ligação TCP (o chamado "**aperto de mão de três vias**", ou seja, uma troca de três datagramas), e só depois é que se segue a transferência de dados propriamente dita. São necessárias três etapas separadas para estabelecer uma ligação TCP:

1. **Uma parte que inicia a ligação (cliente) envia um segmento TCP com o conjunto de bandeiras SYN.**
2. **Um receptor (servidor) responde com um segmento TCP com as bandeiras SYN + ACK definidas.**
3. **O cliente responde com um segmento TCP com o conjunto de bandeiras ACK.**

Outros segmentos TCP já têm apenas o conjunto de bandeiras ACK.

Para mais detalhes, ver por exemplo, o *aperto de mão TCP krok za krokem*. [online]. [cit.18.8.2016]. Disponível a partir de:

<http://www.svetsiti.cz/clanek.asp?cid=TCP-handshake-krok-za-krokem-3122000>

Existem outras formas de ataque DoS, por exemplo "TearDrop", "Nuke", "Peer-to-Peer attack", etc. Para mais detalhes, cf. [online]. [cit.25.9.2010]. Disponível em: http://cs.wikipedia.org/wiki/Denial_of_Service

[4] Também pode ser um caso em que um atacante envia um embuste do tipo "*em 6 de Junho de 2016, de 12 a 13, os bilhetes serão gratuitos na Lufthansa! Clique aqui para mais informações*".

[5] LOIC. [online]. [cit.18.8.2016]. Disponível a partir de: <https://i.ytimg.com/vi/QAbXGy0HbrY/maxresdefault.jpg>

[6] HOIC. [online]. [cit.18.8.2016]. Available from: <https://npercoco.typepad.com/a/6a0133f264aa62970b0167612ea130970b-pi>

[7] Supressão significa a actividade enumerada no artigo 4º da Convenção sobre o Cibercrime.

[8] Se, por exemplo, uma inundação PING for utilizada para um ataque DoS ou DDoS, então é possível imaginar toda a situação como a chamada constante (e subsequente desligamento) para um número de telefone específico. Isto conduzirá a uma situação em que o número de telefone atacado não tem a capacidade de fazer a sua própria chamada (a função de chamada está bloqueada), mas nenhum dos chamadores (atacantes) receberá quaisquer dados armazenados no telefone atacado.

[9] Ver Secção 228 (1) do Código Penal:

"Quem destruir, danificar ou tornar inútil a posse de outrem e assim causar danos não insignificantes aos bens de outrem, será condenado a uma pena de prisão até um ano, à proibição da actividade ou ao confisco de uma posse ou de outro bem de valor".

Danos não insignificantes significam danos no montante de pelo menos 5.000 CZK (ver Secção 138 (1) do Código Penal)

[10] Será que cada atacante será responsabilizado por este dano? Será a responsabilidade por este dano "dividida" entre os atacantes?

4.14. Divulgação de conteúdos defeituosos

Actualmente, podem ser descritos dois tipos básicos de divulgação de conteúdos defeituosos. **Disseminação de tipos de pornografia proibida e disseminação de conteúdos odiosos e extremista.**

No caso da divulgação de **tipos de pornografia proibidos**, trata-se principalmente da divulgação de material pornográfico que represente o contacto com animais e a divulgação (ou posse) de "pornografia infantil" (material que represente ou utilize de outra forma uma criança - uma pessoa com menos de 18 anos, ou uma pessoa que pareça ser uma criança). Há inúmeros métodos de distribuição. Desde simplesmente oferecer este tipo de pornografia para download até à colocação deste material na Internet, distribuindo-o através de redes informáticas de intercâmbio, enviando-o por correio electrónico, etc.

A maioria dos países do mundo comprometeram-se a perseguir o abuso de crianças levando à produção de material pornográfico e à subsequente distribuição de tal material, quer tenham ou não ratificado a Convenção sobre o Cibercrime. Embora esteja a ser desenvolvida uma actividade considerável nesta área (não apenas por Estados, organizações sem fins lucrativos e outras), o problema do abuso sexual de crianças em linha persiste.

O fenómeno da pornografia infantil coexistiu com a sociedade desde os primeiros momentos em que foi possível capturar um acto abusivo em qualquer meio (papel, filme, etc.). Contudo, a verdade é que a Internet permitiu a disseminação em massa de tais materiais entre utilizadores individuais, bem como o seu maior grau de anonimato.

O problema da Internet e do ciberespaço está relacionado com a afirmação anteriormente afirmada de que "*a Internet não esquece*". Se qualquer material for carregado ou transmitido através das TIC, pode sempre haver uma cópia desse material em algum lugar. Um exemplo da República Checa, onde os próprios utilizadores criam material que retrata crianças nuas, pode ser o portal de alojamento de ficheiros www.rajce.net. Este portal não foi certamente criado como um ambiente para a distribuição de qualquer material pornográfico ou de outro modo prejudicial (existem outros sítios para este fim), mas os utilizadores não respeitam as regras básicas do serviço rajce.net, especialmente o Artigo 13, que estipula:

"Os conteúdos que retratam pessoas nuas, especialmente as menores de 18 anos, só podem ser colocados em álbuns privados com uma palavra-chave no Rajce; as outras disposições destas regras, em particular a proibição de colocar conteúdos pornográficos ou conteúdos que violem ilegalmente o direito à protecção da personalidade de terceiros, não serão afectadas em tal caso".

No entanto, é possível encontrar várias fotografias neste site, embora criadas com boas intenções (por exemplo, uma partilha de fotografias entre familiares que vivem longe), que são atractivas para qualquer pessoa, incluindo um potencial agressor. Devido a outras informações publicadas neste portal, ou devido à correlação de dados de outras fontes disponíveis online, é muito mais fácil para um agressor, por exemplo, encontrar uma potencial vítima.

O problema não é o carregamento de fotos de pessoas nuas (com o conhecimento da replicação de dados), mas o facto de estes dados estarem abertos a todos os utilizadores, e não apenas a um grupo restrito (por exemplo, a família já mencionada).



Uma foto de rajce.net (a foto está disponível gratuitamente para todos os utilizadores)

Em conclusão, quero dizer que definitivamente não tenho nada contra tirar fotografias de crianças (ou partilhar algumas fotografias com a família imediata) devido à preservação de belas memórias. O que me incomoda é a forma estúpida e descuidada como estas fotografias são disponibilizadas a qualquer pessoa no ciberespaço.

Um projecto recente sobre o abuso de crianças em linha foi o trabalho da empresa holandesa Terre des Hommes Netherlands (THN). Esta empresa criou uma menina filipina virtual de dez anos de idade, **a Sweetie**. A Sweetie comunicou em chats na Internet durante dez dias e foi abordada por cerca de vinte mil homens. Mil deles ofereceram-lhe dinheiro em troca de sexo online.

O chefe de projecto Hans Guyt disse numa conferência de imprensa em Haia que este tipo de crime exigia uma nova forma de trabalho policial. "Os predadores e as suas vítimas não se aproximam de nós durante a investigação", disse ele.

"Criámos uma identidade virtual sob a forma de uma rapariga filipina de dez anos".

"Não atraímos ninguém até nos oferecerem dinheiro", disse Guyt.

Desta forma, os activistas quiseram chamar a atenção para o crescente problema do abuso de crianças através de webcams. Eles chamam a este fenómeno "*turismo sexual na Internet*".^[1]

Possibilidades de sanções penais na República Checa

No caso de criação, posse ou distribuição de material abrangido pelo termo pornografia infantil, é possível penalizar o utilizador de acordo com a **Secção 192** (Produção e outro tratamento de pornografia infantil), **Secção 193** (Abuso de crianças para produzir pornografia) do Código Penal. A participação num espectáculo pornográfico ou outro espectáculo semelhante, em que uma criança realiza, é também um crime (**Secção 193a** do Código Penal). É também um crime ter acesso a pornografia infantil através das tecnologias da informação ou comunicação (**Secção 192 (2)** do Código Penal).

É também uma infracção penal quando um utilizador tenha produzido, importado, exportado, transportado, oferecido, disponibilizado ao público, intermediado, posto em circulação, vendido ou fornecido de qualquer outra forma um trabalho fotográfico, cinematográfico, informático, electrónico ou outro trabalho pornográfico em que a violência ou desrespeito por uma pessoa, ou que descreva, represente ou represente de qualquer outra forma relações sexuais com um animal (**Secção 191 (1)** do Código Penal).

No caso de uma **divulgação de conteúdo odioso e extremista**, uma infracção penal inclui principalmente o apoio e a promoção de um movimento que vise comprovadamente a supressão dos direitos humanos e das liberdades, manifestações de simpatia por tal movimento, proclamação de ressentimento racial, étnico e nacional, religioso ou de classe ou ressentimento contra outro grupo. Inclui também a difusão da difamação através das tecnologias da informação e, por último mas não menos importante, o envio de mensagens incómodas abrangidas pelo conceito de perseguição ou perseguição cibernética.

Nestes casos, pode haver uma série de crimes, tais como a **Secção 184** (Difamação), **Secção 353** (Ameaça Perigosa), **Secção 354** (Perseguição Perigosa), **Secção 355** (Difamação de Nação, Raça, Étnia ou outro Grupo de Pessoas), **Secção 356** (Instigação do ódio contra um Grupo de Pessoas ou da Supressão dos seus Direitos e Liberdades), **Secção 403** (Estabelecimento, Apoio e Promoção de Movimentos que visam a Supressão dos Direitos Humanos e Liberdades), **Secção 404** (Expressão de Simpatias para Movimentos que visam a Supressão dos Direitos Humanos e Liberdades), **Secção 405** (Negação, Impugnação, Aprovação e Justificação de Genocídio) do Código Penal.

Possibilidades de sanções penais na Polónia

Na Polónia aplica-se o seguinte artigo do Código Penal:

Arte. 200b. Promoção pública de conteúdos pedófilos

Arte. 202. Apresentação e distribuição de pornografia

Possibilidades de sanções penais em Portugal

Tais actos são criminalizados de diferentes formas, dependendo do caso. Em primeiro lugar, podem ser considerados como delitos relacionados com pornografia infantil (art. 176º do Código Penal). Por outro lado, constituem uma violação agravada da privacidade (Artes. 191(1)(b) e 197(b) do Código Penal) ou como Vingança pornográfica relacionada com violência doméstica (art. 152(2)(b) do Código Penal (art. 193() do Código Penal).

Além disso, podem estar presentes elementos objectivos de crimes como a Discriminação e o incitamento ao ódio e à violência (Art. 240 do Código Penal) ou a Difamação (Art. 180 do Código Penal).

^[1] Para mais pormenores, ver:

A 'Queridinha' gerada por computador captura predadores em linha. [em linha]. [cit.19.8.2016]. Disponível em: <http://www.bbc.com/news/uk-24818769>

Nizozemci vytvořili virtuální dívku. Pomohla lapit přes tisíc pedofilů. [online]. [cit.19.8.2016]. Disponível a partir de: http://zpravy.idnes.cz/virtualni-holcicka-pomohla-lapit-tisic-pedofilu-fuu-zahranicni.aspx?c=A131106_210025_zahranicni_zt

O vídeo com o **Sweetie** está disponível online: <https://www.youtube.com/user/sweetie>.

4.15. Ataques cibernéticos em redes sociais

Dentro das redes sociais, é possível cometer a maior parte dos ciberataques anteriormente descritos (por exemplo, malware, phishing, spam, etc.). A razão pela qual os ciberataques em plataformas de redes sociais são descritos separadamente é o facto de ocorrerem principalmente (mas não exclusivamente) no ambiente das redes sociais.

Estes ataques específicos incluem:

1. Cyberbullying
2. Cybergrooming
3. Sexting
4. Cyberstalking

4.15.1. Cyberbullying

A intimidação no mundo real consiste na tentativa de um agressor de prejudicar, humilhar, ridicularizar ou insultar outro, quer física ou mentalmente. O cyberbullying transmite então "bullying clássico" para o mundo virtual e permite a um agressor utilizar ferramentas e recursos que podem ter um impacto muito maior na vítima do que seria o caso no mundo real. O cyberbullying, através da utilização de tecnologias de informação e comunicação e da durabilidade dos dados no ciberespaço, permite ataques repetidos a uma vítima, mesmo que a vítima se tenha afastado geograficamente do mundo real de onde foi originalmente vítima de bullying.

O cyberbullying pode ser ligado ao bullying "clássico" (por exemplo, gravar a agressão física de uma vítima e depois afixar o ataque na web). Para falar de cyberbullying, é necessário utilizar tecnologias de informação e comunicação, ou serviços oferecidos no ciberespaço para o bullying.

Os sinais de cyberbullying incluem:

- **Sentir-se anónimo** (Os atacantes geralmente sentem que não podem ser rastreados devido à Internet).
- **Ataque ilimitado** (Devido às TIC, os atacantes não têm de lidar com o tempo ou espaço para o seu ataque. É possível intimidar a qualquer momento, de qualquer lugar e de qualquer pessoa. Tal ataque também requer muito menos esforço do que no caso de bullying "clássico").
- **Grupo ilimitado de atacantes** (Ao contrário do mundo real, no mundo virtual não importa a idade, sexo, força física, posição do atacante no grupo, etc. Qualquer pessoa pode ser um agressor).
- **Espaço e recursos ilimitados** (A Internet fornece a um agressor espaço e recursos praticamente ilimitados para o bullying. Um atacante pode publicar repetidamente comentários ofensivos, comentários de fotos e vídeos em vários portais, redes sociais, etc. Ele pode melhorar e "refinar" estes materiais).
- **Difícil de detectar** (Ao contrário do bullying clássico, o cyberbullying pode não ter manifestações externas tais como hematomas, dinheiro em falta, etc.)
- **Persistência** [O bullying clássico consiste geralmente em ataques individuais, que se repetem, mas o ataque único para a vítima acaba sempre. Para o cyberbullying, por exemplo, um SMS, e-mail, etc. é suficiente, uma vítima continua a voltar para eles (respectivamente, são constantemente lembrados, enviados, etc.), para que possa viver em trauma durante meses. Os SMS ofensivos, e-mails, fotos, etc. são mais permanentes do que os ataques físicos individuais].

As manifestações mais comuns de cyberbullying:

1. Fofoca, intimidação, insulto, ridicularização ou outro embaraço (redes sociais, e-mail, SMS, chat, ICQ, Skype, jogos, etc.).
2. Aquisição de gravações sonoras, vídeos ou fotografias, a sua edição gráfica ou outra e posterior publicação a fim de prejudicar (ridicularizar) uma pessoa seleccionada.
3. Filmagem de vídeos em que uma vítima é fisicamente atacada ou de outra forma abusada mentalmente e ridicularizada. Estes vídeos são então publicados online (a isto chama-se Happy Slapping).
4. Criar websites, contas sociais (modificando perfis originais ou criando novos perfis), portais de discussão, etc. que insultam, caluniam ou humilham uma pessoa específica.
5. Uso indevido da conta de outrem - roubo de identidade (e-mail, discussão, etc.).
6. Provocar e atacar utilizadores em fóruns de discussão (salas de chat, etc.).
7. Descobrir os segredos de outras pessoas.
8. Chantagem utilizando um telemóvel ou a Internet.
9. Assédio e perseguição através de chamadas, mensagens escritas ou toques.

Consequências de alguns ataques:

- **Amanda Todd** (15 anos de idade) era uma estudante canadiana de 15 anos e vítima de cyberbullying que se enforcou na sua casa em Port Coquitlam, British Columbia. Antes da sua morte, Todd publicou um vídeo no YouTube no qual utilizou uma série de flashcards para contar a sua experiência de ser chantageada para expor os seus seios via webcam, e de ser intimidada e agredida fisicamente. (*Wikipedia*)
- **Rebecca Ann Sedwick** (12 anos de idade) foi intimidada na Internet durante quase um ano. Cometeu suicídio em 2013. O bullying começou depois de Rebecca ter namorado um rapaz durante algum tempo. A sua mãe disse aos repórteres que a sua filha tinha estado a receber mensagens como: 'Você é nojento', 'Porque é que ainda está vivo?' e 'Vá matar-se'. A situação agravou-se tanto que a mãe deixou a filha fora da escola de Crystal Lake e cancelou a sua conta no Facebook. Segundo consta, ela teve de deixar a escola. A mãe ensinou-a em casa durante o resto do ano. Ela entrou noutra escola em Setembro. Tudo parecia estar a melhorar e Rebecca animou-se na nova escola. Mas ela inscreveu-se secretamente para novas candidaturas, incluindo mensagens telefónicas Kik Messenger e Ask.fm, e o bullying recomeçou depois de ela ter começado a perguntar sobre o excesso de peso na Internet. O Xerife Judd disse que a rapariga tinha sido "completamente aterrorizada" nas redes sociais.
- **Ghyslain Raza** (14 anos, Canadá), conhecido como o Star Wars Kid.

youtube.com/watch?v=HPPj6vilBmU&spfreload=10. Ghyslain Raza filmou-se a si próprio a representar uma cena de batalha do Star Wars. Ele tentou imitar a personagem de Darth Maul. Os seus colegas de turma roubaram a gravação e publicaram-na na Internet para entreter os outros. Em poucas semanas, a gravação voou pelo mundo, foi modificada muitas vezes, e foram criados vários websites e blogs, nos quais o rapaz foi ridicularizado. Os fãs de Ghyslain escreveram uma petição aos criadores do Star Wars para o lançarem num dos episódios. Ele até foi parodiado em algumas séries (por exemplo South Park, American Dad, Veronica Mars). Ghyslain teve um colapso mental e teve de ser tratado durante muito tempo.

- **Anna Halman** (14 anos de idade, Polónia). Cinco colegas de turma submeteram Anna a assédio sexual em frente de toda a turma. (Tiraram-lhe as roupas e fingiram violá-la.) Gravaram toda a cena num telemóvel e ameaçaram a rapariga de que iriam publicar a gravação na Internet. Também o fizeram mais tarde, publicando o vídeo no YouTube. Era suposto ser uma vingança para Anna por não querer namorar com um dos rapazes. Anna cometeu suicídio.
- **Jessica Logan** (18 anos, EUA). Após a sua separação, o ex-namorado de Jessica publicou as suas fotografias íntimas, que ela lhe tinha enviado enquanto ainda namoravam. Jessica foi então exposta ao constante ridículo dos seus colegas de turma. Os ataques contra ela intensificaram-se depois de ela ter aparecido anonimamente na televisão para avisar os outros sobre os riscos de sexting. Jessica cometeu suicídio.

Possibilidades de sanções penais na República Checa

O cyberbullying (como o bullying clássico) não é em si mesmo um crime ou uma ofensa. Depende sempre das acções do agressor. Se tal acção fosse uma forma de, por exemplo, dano físico a uma vítima, chantagem ou intimidação, então poderia ser considerada a aplicação, por exemplo, da **Secção 146** (Dano Corporal) ou da **Secção 145** (Dano Corporal Grave), **Secção 175** (Extorsão) do Código Penal. No caso de assédio e perseguição de uma pessoa, seria possível utilizar as disposições da **Secção 354** do Código Penal (Perseguição Perigosa). No entanto, no caso de cyberbullying, que pode manifestar-se, por exemplo, em constante ridicularização, embaraço e danos psicológicos através das tecnologias de informação e comunicação, a aplicação de algumas das disposições acima referidas será problemática, se não impossível.

Possibilidades de sanções penais na Polónia

Na Polónia, isto é regulamentado por:

Arte. 212 kk - Difamação

e

Arte. 190 § 1 Quem ameaçar outra pessoa com a prática de uma infracção penal em seu detrimento ou em detrimento de uma pessoa próxima, se a ameaça induzir na pessoa ameaçada um receio razoável de que a ameaça será executada, será sujeito a uma multa, à pena de restrição da liberdade ou à pena de privação da liberdade por um período até 2 anos.

§ 2 A acusação deve ocorrer com a moção da pessoa lesada.

Possibilidades de sanções penais em Portugal

Como tal, o cyberbullying não é um delito criminal. Contudo, pode ser considerado como uma forma de perseguição (art. 154-A do Código Penal), mas também como assédio sexual, um insulto, uma difamação, uma violação agravada da privacidade ou mesmo como discriminação e incitação ao ódio e à violência (Artes. 170, 181, 180, 192 e 197 (b) e 240, todos do Código Penal).

4.15.2. Cybergrooming

O ciberespaço é um acto que envolve uma manipulação psicológica de uma pessoa (tipicamente utilizando engenharia social), realizado através da Internet ou de tecnologias de informação e comunicação (por exemplo, telemóveis, etc.). O objectivo do ciberespaço é evocar a falsa confiança numa vítima e, assim, fazê-la encontrar-se pessoalmente. O resultado de um tal encontro pode ser qualquer ataque físico, sexual ou outro ataque a uma vítima. As vítimas de ciberconferência podem ser crianças, bem como adultos. De acordo com as estatísticas, as vítimas mais comuns são raparigas com idades compreendidas entre os 13 e os 17 anos.

"A manipulação psicológica dentro do cybergrooming demora geralmente mais tempo - de cerca de 3 meses a vários anos. O tempo é directamente dependente do método de manipulação e da confiança de uma vítima. Há casos em que um predador manipulou uma criança durante 2-3 anos antes de um encontro pessoal e abuso sexual. A maturidade da criança também deve ser tida em conta - um agressor pode comunicar com uma criança quando era menor, mas um ataque terá lugar após a idade da maioridade. (É evidente que as penas por abuso sexual de um menor e de um adulto são muito diferentes)".[1]

O Cybergrooming tem diferentes fases:

1. Despertar a confiança e tentar isolar uma vítima do ambiente (um agressor muda a sua identidade; ele é muito paciente)
2. Suborno com presentes ou vários serviços, construindo uma amizade
3. Induzir a dependência emocional de uma vítima de uma pessoa de um agressor
4. Reunião pessoal
5. Assédio sexual, abuso de crianças ou outras agressões[2]

O grupo de risco das crianças é constituído por:

1. *adolescentes/adolescentes* (eles estão interessados na sexualidade humana, estão dispostos a falar sobre ela),
2. *crianças com baixa auto-estima ou falta de auto-confiança* (podem ser mais facilmente isoladas emocional ou fisicamente),
3. *crianças com problemas emocionais, vítimas em situações difíceis da vida* (muitas vezes à procura de uma compensação para os seus pais e necessitando de uma mão amiga),
4. *crianças confiantes e demasiado ingénuas* (estão mais dispostas a conversar em linha com estranhos, têm mais dificuldade em reconhecer a comunicação arriscada).

Possibilidades de sanções penais na República Checa

Uma pessoa que comete um ciberespaço pode, pelos seus actos, cumprir o elemento objectivo de certas infracções penais especificadas no Código Penal. Em regra, dependendo da natureza da conduta de um agressor, estes significarão infracções penais ao abrigo das disposições do **Artigo 168** (Tráfico de Seres Humanos), **Artigo 171** (Contenção Ilegal), **Artigo 175** (Extorsão), **Artigo 185** (Violação), **Artigo 187** (Abuso Sexual), **Artigo 201** (Ameaça aos Cuidados de uma Criança), **Artigo 209** (Fraude), **Artigo 353** (Ameaça Perigosa), **Artigo 354** (Perseguição Perigosa) do Código Penal.

Outra possível definição de ciberespaço afirma que é **"tal comportamento dos utilizadores da Internet que é suposto evocar uma falsa confiança numa criança vítima e fazê-los encontrar pessoalmente". O resultado de tal encontro pode ser abuso sexual da vítima, violência física contra a vítima, abuso da vítima para prostituição infantil, produção de pornografia infantil, etc."**[3] Neste contexto, é possível utilizar uma disposição especial da **Secção 193b** (Estabelecimento de Contacto Ilegal com uma Criança) do Código Penal.

Possibilidades de sanções penais na Polónia

Em Junho de 2010, entrou em vigor uma alteração ao Código Penal. Um tipo de crime completamente novo aparece no Código Penal, regulamentado no Art.200 a do Código Penal, o chamado grooming, ou aliciamento através da Internet. Trata-se de pessoas que, através do sistema TIC ou da rede de telecomunicações, entram em contacto com um menor com menos de 15 anos, com o objectivo de o deturparem, explorando o seu erro ou incapacidade de compreender a situação ou uma ameaça ilegal de o encontrar. Esta infracção é punível com uma pena de prisão até 3 anos.

Quem submeter a um menor de 15 anos, através do sistema TIC ou da rede de telecomunicações, a mera proposta de relações sexuais, submissão ou outra actividade sexual ou participação na produção ou registo de conteúdos pornográficos e visar a sua implementação, será então sujeito a uma multa, a pena de restrição da liberdade ou de prisão por 2 anos.

Possibilidades de sanções penais em Portugal

A solicitação de crianças para fins sexuais através das tecnologias da informação e comunicação é um crime (Art. 176-A do Código Penal).

4.15.3. Sexting

Uma das formas de conduta perigosa, especialmente no ambiente das redes sociais, é a chamada sexting. O termo sexting teve origem numa combinação das palavras sexo e texturização, o que torna claro o seu significado. É uma distribuição electrónica de mensagens de texto, fotografias ou vídeos com conteúdo sexual. Este material sexualmente explícito pode ser carregado para redes sociais ou outros repositórios de dados directamente pelos próprios autores ou por outro utilizador que tenha obtido acesso a tal material. Isto acontece mais frequentemente através do envio voluntário de ficheiros com conteúdo sexual, que são levados pelos próprios remetentes.

Subsequentemente (após a cessação da comunicação, relação ou por qualquer outro motivo), o infractor utilizará o material sensível obtido para ameaçar ou chantagear. Em alguns casos, um infractor pode, sob a ameaça de publicar tal material, solicitar o envio de fotografias ou vídeos adicionais, forçando assim a vítima a produzir e adquirir outro material que o infractor exija quer para seu próprio uso quer com a intenção de o partilhar na Internet (no caso de crianças, elas partilham-nos entre as comunidades de pornografia infantil). A segunda variante das acções de um infractor é a utilização do material obtido para outras pressões (por exemplo, renovação de uma parceria, actividades sexuais, envio de um montante financeiro, etc.) sob a ameaça de publicar fotografias ou vídeos previamente adquiridos (originalmente enviados voluntariamente por uma vítima).

Os resultados da Investigação sobre Comportamento de Risco das Crianças Checas no Ambiente da Internet[4] 2014 preparada pelo Centro de Prevenção de Comunicação Virtual de Risco da Faculdade de Educação da Universidade de Palacký em Olomouc em cooperação com o Seznam.cz mostram que 9,86% das crianças colocaram as suas fotos ou vídeos "sexy", nos quais estão parcial ou completamente nuas, na Internet. Do número total de 28.232 inquiridos, 12,14% declararam ter enviado tal material a alguém através da Internet/telefone móvel.

No caso de sexting, o envolvimento de uma vítima no crime é indiscutível, pois a vítima é a pessoa que criou a fotografia ou vídeo em questão, mas depois de enviar este material, a vítima perde o controlo total sobre a próxima "vida" de tais dados.

Possibilidades de sanções penais na República Checa

No caso de publicar fotografias de outra pessoa sem o seu consentimento, é possível à pessoa em causa reclamar a protecção dos seus direitos em processos civis.

Se uma pessoa faz uma falsa declaração sobre outra (como foi provavelmente o caso com *Roztahovačky (Slutty girls)*), o que é capaz de pôr significativamente em perigo a sua reputação junto dos seus concidadãos, prejudicando-o especialmente no trabalho, perturbando as suas relações familiares ou causando-lhe outros danos graves, é possível utilizar a **Secção 184** (Difamação) do Código Penal.

Um caso específico é a situação em que materiais audiovisuais representando uma criança são obtidos e mal utilizados. Se um agressor convidar uma criança a criar e depois enviar fotografias, vídeos ou streaming online em frente de uma webcam (que capturem uma criança nua ou que suscitem excitação sexual), esse agressor pode cometer um crime ao abrigo da **Secção 193** (Abuso de uma Criança para Produção de Pornografia) do Código Penal.

A extensão também resulta muito frequentemente em que um infractor força uma vítima a enviar outro material (fotos, vídeos, transmissão em directo, etc.), ameaçando publicar o material que já possui na Internet ou se a vítima não os enviar, o infractor colocá-los-á à disposição da sua família ou amigos. Ao fazê-lo, essa pessoa está a cometer uma infracção penal ao abrigo do **artigo 175 (1)** (Extorsão) do Código Penal.

Uma pessoa que comete sexting pode também cumprir o elemento objectivo de uma infracção penal ao abrigo da **Secção 192** (Produção e Manuseamento de Pornografia Infantil) ou da **Secção 201** (Ameaçar os Cuidados de uma Criança) do Código Penal.

Possibilidades de sanções penais na Polónia

Segundo a lei polaca, são proibidos os seguintes

- produção para divulgação;
- gravação;
- divulgação;
- apresentação;
- posse e armazenamento;
- importação

de material pornográfico com a participação de um menor - pessoas com menos de 18 anos (Artigo 202 do Código Penal). Tais acções são puníveis com pena de prisão de 8 meses a 10 anos. Vale também a pena notar que a divulgação de uma imagem de uma pessoa nua ou de uma pessoa durante uma actividade sexual sem o seu consentimento (Artigo 191º-A do Código Penal) é punível com uma pena de prisão de 3 meses a 5 anos.

Possibilidades de sanções penais em Portugal

Enviar tal conteúdo a outro adulto pode ser perseguido como Assédio Sexual (Art. 170 do Código Penal). No entanto, se alguém enviar esses conteúdos a terceiros, isso seria considerado como uma Difamação, uma violação agravada da privacidade, uma violência doméstica agravada ou mesmo como Discriminação e incitamento ao ódio e à violência (Artes. 180, 152, 192 e 197 (b) e 240, todos do Código Penal).

4.15.4. Cyberstalking

Cyberstalking é um composto das palavras cyberstalking e stalking. Originalmente, a palavra perseguição era utilizada por caçadores de caça selvagem e significava seguir caça até ser morta. A perseguição, tal como é entendida hoje em dia, foi utilizada pela primeira vez nos anos 90 num estudo de Meloy[5], que descreveu a perseguição como sendo a perseguição ameaçadora seguida por um perpetrador conhecido ou desconhecido que perseguiu uma vítima de tal forma que evocava um sentimento de perigo ou medo. Tal perseguição deve ser a longo prazo.

Cyberstalking é um acto que consiste em contactar repetidamente uma vítima, por exemplo, através do envio de mensagens SMS, e-mails, chamadas telefónicas, VoIP, mensagens, etc. As acções do agressor normalmente aumentam e normalmente suscitam preocupações sobre a privacidade, saúde ou vida da vítima. Os *ciberstalkers* caracterizam-se pela sua perseverança e natureza sistemática, e não é raro que um ciberstalker tenha criado uma variedade de identidades falsas que utiliza para contactar uma vítima. Um ciberstalador pode também demonstrar o seu poder e força, por exemplo, publicando informação sobre a vida da vítima que pode obter de várias fontes online.

Possibilidades de sanções penais na República Checa

A perseguição ou ciberperseguição pode cair, sob certas condições, sob as disposições da **Secção 354** (Perseguição Perigosa) do Código Penal. As condições básicas incluem que um agressor deve contactar uma vítima "*persistentemente por meios electrónicos, por escrito ou de outra forma*" durante muito tempo e tal acto é capaz de suscitar uma preocupação razoável pela vida ou saúde da vítima ou pela vida e saúde das pessoas que lhe são próximas. As circunstâncias agravantes de acordo com a **Secção 354(2) (a)** do Código Penal é o facto de o referido acto ser cometido contra uma criança.

Possibilidades de sanções penais na Polónia

De acordo com o Código Penal polaco, a perseguição pode ser cometida de duas formas. Assediando persistentemente a pessoa penal (Artigo 190 a § 1 do Código Penal) ou fazendo-se passar por ela (Artigo 190a § 2 do Código Penal). A qualificação de um comportamento específico como perseguição depende do cumprimento de várias condições pelo perpetrador.

A primeira característica principal da perseguição é a persistência das acções do perpetrador. Isto significa que apenas alguns actos que violam a liberdade mental humana podem ser considerados perseguição. Em termos simplificados, pode dizer-se que a perseguição na sua primeira forma (§1) consiste em assediar outra pessoa pelo menos várias vezes. O comportamento que se qualifica como assédio pode ser diferente, tal como: provocar, incomodar, enviar cartas ou fazer telefonemas. A necessidade de declarar a persistência dos actos do agressor. Os actos isolados não são proibidos por lei, são comuns na nossa vida quotidiana. Em alguns casos, podem qualificar-se como um delito de perturbação maligna. Apenas o comportamento multiplicado e duradouro do perpetrador, que não tem qualquer intenção de suspender os seus actos apesar dos pedidos da parte lesada, pode ser considerado perseguição.

Possibilidades de sanções penais em Portugal

Recentemente, a perseguição, incluindo a perseguição cibernética, tornou-se uma infracção penal como perseguição (art. 154-A do Código Penal).

[1] KOPECKÝ, Kamil. *Nebezpečí zvané kybergrooming I*. In: Metodický portál inspirace a zkušenosti učitelů [online]. 2010. [cit.19.3.2014]. Disponível em: <http://clanky.rvp.cz/clanek/s/Z/9741/NEBEZPECI-ZVANE-KYBERGROOMING-I.html/#6a>

[2] *Kybergrooming*. [online]. [cit.19.8.2016]. Disponível a partir de: <http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx>

[3] KOPECKÝ, Kamil. *Nebezpečí zvané kybergrooming I*. In: Metodický portál inspirace a zkušenosti učitelů [online]. 2010. [cit. 2014-03-19]. Disponível em: <http://clanky.rvp.cz/clanek/s/Z/9741/NEBEZPECI-ZVANE-KYBERGROOMING-I.html/#6a>

[4] *Výzkum rizikového chování českých dětí v prostředí internetu 2014*. [online]. [cit.19.8.2016]. Disponível a partir de: https://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/61-vyzkum-rizikoveho-chovani-eskych-dti-v-prosted-i-internetu-2014-prezentace

[5] MELOY, Reid J. *STALKING (SEGUIMIENTO OBSESSIONAL): UMA REVISÃO DE ALGUNS ESTUDOS PRELIMINARES*. [online]. [cit.3.10.2015]. Disponível em: http://forensis.org/PDF/published/1996_StalkingObsessi.pdf

4.16. Roubo de identidade

O roubo de identidade é um ataque em que uma identidade virtual é roubada^[1], ou é uma tomada de controlo (permanente ou temporária) desta identidade. O motivo da acção de um agressor pode ser um ganho financeiro, mas também outros benefícios, tais como acesso a informações sobre outras pessoas, acesso a dados da empresa, etc., que estão associados ao facto de um agressor agir em nome de outra pessoa.

As acções de um agressor consistem geralmente em várias acções ilegais ao mesmo tempo. O primeiro crime de roubo de identidade é o hacking nos dados de acesso ou a instalação de malware no sistema informático de uma vítima a fim de obter acesso a uma identidade virtual.

Depois de obter acesso a uma identidade de uma pessoa atacada, a informação obtida pode ser mal utilizada para atacar essa pessoa e a identidade pode ser mal utilizada para atacar outra pessoa. Um ataque a outra vítima através de uma identidade roubada é muito mais fácil para um agressor porque esta segunda vítima por defeito não tem qualquer informação sobre a alteração da identidade da pessoa (a primeira vítima), com a qual, por exemplo, comunica e troca regularmente dados sensíveis.

Se voltar à questão das botnets neste contexto, uma das tarefas típicas do malware que é instalado quando um sistema informático é ligado a uma rede de botnets é a extracção automática de dados sobre os utilizadores do sistema informático infectado - ou seja, roubo de identidade. O botmaster pode então utilizar os dados obtidos em qualquer altura, fazendo-se passar por uma certa pessoa ou vendendo esses dados a terceiros.^[2]

Tipicamente, as identidades roubadas estão habituadas:

- realizar ataques de phishing ou malware dentro da lista de utilizadores com os quais uma pessoa com uma identidade roubada comunica,
- envio de spam,
- obter informações que não estão disponíveis publicamente (por exemplo, informações sobre a estrutura de uma empresa, configurações de segurança para outros serviços, etc.),
- obter acesso a outros serviços. Muitos serviços em linha permitem-lhe alterar a sua palavra-passe apenas através da introdução do seu endereço de correio electrónico. Devido ao facto de um atacante controlar uma caixa de correio electrónico de uma pessoa atacada, os dados de acesso podem ser alterados numa série de outros serviços que estão associados a esta caixa de correio electrónico.

Possibilidades de sanções penais na República Checa

Se uma medida de segurança for ultrapassada e for obtido o acesso não autorizado à identidade da vítima, as características do crime de acordo com a **Secção 230 (1)** (Acesso não autorizado a sistemas informáticos e meios de informação) do Código Penal serão cumpridas. Ao utilizar malware para o mesmo fim, um agressor comete um acto nos termos do artigo 230 (2) do Código Penal. Se o objectivo do roubo de identidade for obter um benefício injustificado para si próprio ou para outro, é também possível aplicar as disposições da **Secção 230 (3) do Código Penal**. No caso de um agressor roubar uma identidade com o objectivo de enganar outro, ou seja, enganar alguém para se enriquecer a si próprio, tal conduta poderia também ser avaliada de acordo com o **Artigo 209** (Fraude) do Código Penal.

Possibilidades de sanções penais na Polónia

Nos termos do Art.190 a § 2 do Código Penal, qualquer pessoa que, fazendo-se passar por outra pessoa, utilize a sua imagem ou outros dados pessoais a fim de lhe infligir danos materiais ou pessoais enfrenta uma pena de prisão até três anos.

Possibilidades de sanções penais em Portugal

Fingir ser outra pessoa já não é criminalizado. Contudo, a criação de dados não autênticos para fins juridicamente relevantes seria considerada como uma falsificação relacionada com a informática (art. 3 da Lei sobre o Cibercrime). Além disso, sendo a finalidade de tal falsificação uma intenção fraudulenta ou desonesta de obter, sem direito, um benefício económico para si próprio ou para outra pessoa, sobre as despesas da vítima, também seria considerada como uma fraude informática (art. 221(1) do Código Penal).

[1] Identidade virtual significa qualquer identidade ou avatar utilizado por uma pessoa para interagir no ciberespaço (por exemplo, e-mail, conta de rede social, um jogo, em vários mercados online, dentro de um sistema informático, etc.). Não importa se uma identidade virtual é verdadeira ou falsa, ou seja, se representa uma pessoa real, ou se é uma identidade completamente criada artificialmente, sem uma base real.

[2] Para mais pormenores, ver: PLOHMANN, Daniel, Elmar GERHARDS-PADILLA e Felix LEDER. *Botnets: Detecção, Medição, Desinfecção e Defesa*. ENISA, 2011, p. 22 [online]. [cit.17.5.2015]. Disponível em: <https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence>

4.17. APT (Ameaça Persistente Avançada)

APT significa uma ameaça avançada e persistente. Trata-se de um ciberataque sistemático a longo prazo, centrado num sistema informático alvo, ou nas TIC de uma organização alvo. Várias técnicas e recursos relativamente grandes são utilizados para tal ataque, e normalmente alvos secundários (por exemplo, sistemas informáticos como DoS repetidos ou outros ataques) podem ser atacados a fim de desviar a atenção do alvo principal (infiltração malware de uma empresa), que é depois atacado.

“O APT concentra-se geralmente na extracção de dados classificados ou não públicos estrategicamente valiosos, limitando a capacidade de acção de um alvo, ou tomando uma posição que permita a implementação futura do acima mencionado. A implementação de acções que correspondem à definição de APT está associada a um elevado nível de especialização, a recursos financeiros consideráveis e à capacidade de adaptação às acções da vítima do ataque a longo prazo. O carácter da APT adquire, assim, principalmente actores estatais, ou seja, os seus grupos controlados e patrocinados, ou grupos especializados do crime organizado.”[1]

Um ataque APT consiste tipicamente em:

- uma aquisição de informação sobre um alvo de um ataque (recolha de informação de fontes abertas; utilização de engenharia social, etc.)
- um ataque real:
 - Selecção de meios adequados (malware, criação de identidades de cobertura, etc.)
 - Se um sistema é vulnerável a partir do exterior, é atacado
 - Se um sistema é inacessível do exterior, são utilizadas outras técnicas combinadas com engenharia social (por exemplo, Spear phishing, Identity Theft, etc.)
- assumir o controlo de alguns sistemas informáticos, consolidando posições dentro da rede informática comprometida
- recolher dados e informações e enviá-los ao agressor
- extracção de dados

Durante um ataque APT, os atacantes podem utilizar outros tipos diferentes de ataques contra o alvo seleccionado, dependendo dos dados e informações que tenham adquirido.

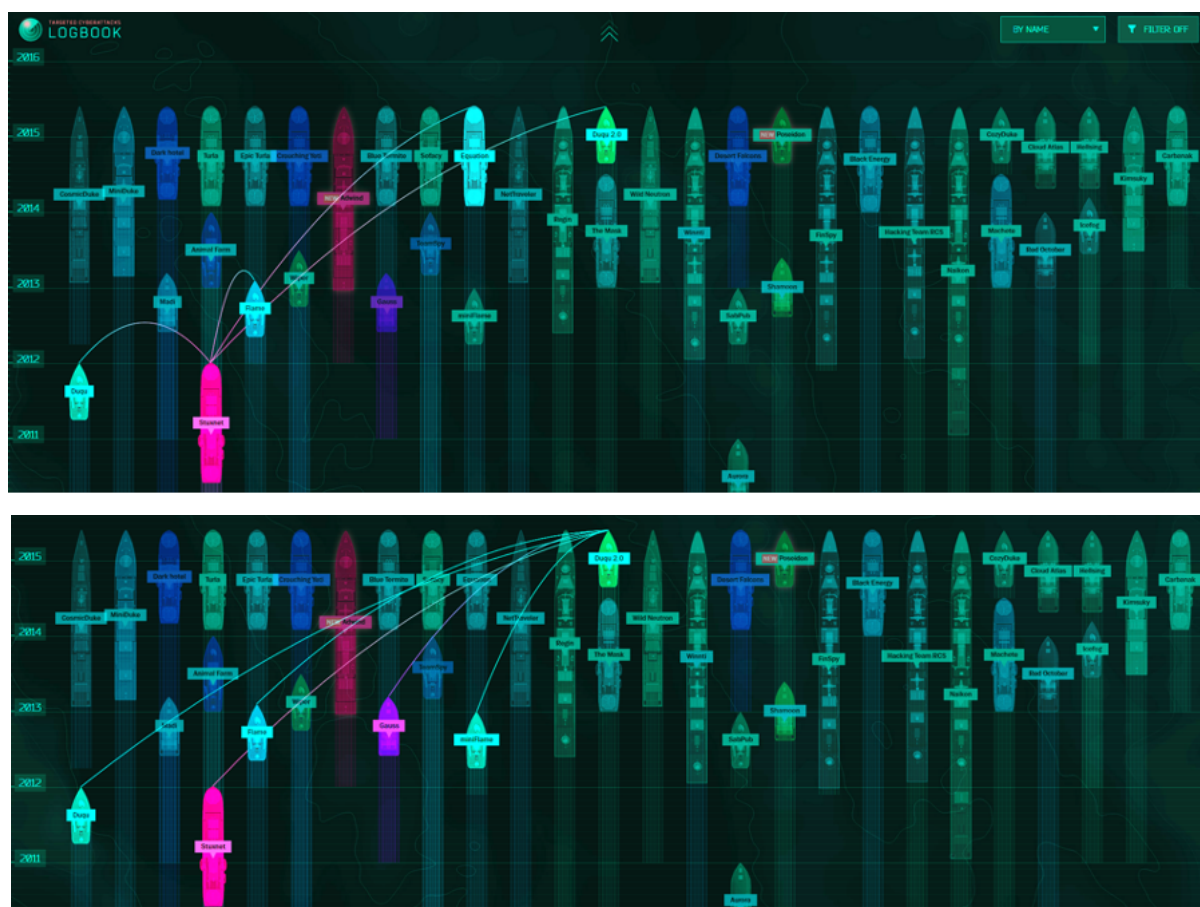
O APT pode ser exibido utilizando o seu ciclo de vida:



Ciclo de vida do ataque APT[2].

Um ataque APT pode durar de vários meses a muitos anos, e um ataque pode incluir períodos relativamente longos quando a actividade dos atacantes é mínima. Não é excepção conduzir um grande número de operações semelhantes contra diferentes objectivos ao mesmo tempo.[3]

O site Kasperky Lab (<https://apt.securelist.com/#firstPage>) descreve visualmente os ataques APT conhecidos, incluindo informação sobre quando uma amostra de malware de ataque apareceu pela primeira vez, quando um ataque APT foi descoberto, onde opera principalmente (informação de geolocalização, sistemas operativos atacados principalmente, número de alvos, etc.), etc. Os dois ecrãs de impressão seguintes mostram a ligação primária de malware Stuxnet (incluindo, entre outros, a Duqu 2.0) e depois a ligação de Duqu 2.0 a outro malware.



Exibição dos ataques APT incluindo a sua interligação[4].

Possibilidades de sanções penais na República Checa

Qualquer sanção penal de um atacante ou atacantes que realizem um ataque APT depende então inteiramente das suas acções, que podem assumir a forma, por exemplo, de distribuição de malware, um dos ataques de phishing, Roubo de Identidade, etc.

Possibilidades de sanções penais na Polónia

Ao analisar um ataque APT em termos de violações da lei em vigor na Polónia, deve considerar-se que se um ataque fosse perpetrado em todas as suas fases, seriam cometidos pelo menos alguns delitos. De acordo com os regulamentos legais aplicáveis, um ataque APT pode ser considerado:

- hacking sob Arte. 267 § 1 do Código Penal
- crime de produzir ou disponibilizar dispositivos ou programas informáticos, palavras-passe e códigos sob Arte. 269 b do Código Penal
- fraude informática ao abrigo da Arte. 287 do Código Penal

Outros crimes que podem ocorrer durante a fase de implementação são:

- sabotagem informática ao abrigo da Arte. 269 do Código Penal,
- trazendo perigo para a vida, saúde ou propriedade sob a arte. 165 do Código Penal,
- destruição, dano, eliminação de dados informáticos da arte. 268 a do Código Penal,
- interrupções no funcionamento do sistema informático ou da rede de TIC, nos termos da Arte. 269a.

Um ataque APT também pode ser equivalente à espionagem sob a arte. 130 § 3 do Código Penal.

Possibilidades de sanções penais em Portugal

O ataque APT não é especificamente criminalizado, nem sequer como ofensas agravadas.

[1] Ameaça avançada e persistente. [online]. [cit.20.8.2016]. Disponível em: <https://www.isouvislosti.cz/advanced-persistent-threat>

[2] Ameaça Persistente Avançada - ciclo de vida. [online]. [cit. 20. 8. 2016]. Disponível a partir de: https://upload.wikimedia.org/wikipedia/commons/7/73/Advanced_persistent_threat_lifecycle.jpg

[3] Para mais pormenores, ver: Ameaça Persistente Avançada. [online]. [cit. 20. 8. 2016]. Disponível em: <https://www.isouvislosti.cz/advanced-persistent-threat>

Ameaça Persistente Avançada (APT). [online]. [cit. 20. 8. 2016]. Disponível a partir de: <http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT>

Ameaças Persistentes Avançadas: Como Funcionam. [online]. [cit.10.7.2016]. Disponível em: <https://www.symantec.com/theme.jsp?themeid=apt-infographic-1>

Como funcionam os APTs? O Ciclo de Vida das Ameaças Persistentes Avançadas (Infográfico). [online]. [cit. 10. 7. 2016]. Disponível em: <https://blogs.sophos.com/2014/04/11/how-do-apt-work-the-lifecycle-of-advanced-persistent-threats-infographic/>

[4] *Livro de registo de ataques cibernéticos direccionados*. [em linha]. [cit.10.7. 2016]. Disponível em: <https://apt.securelist.com/#secondPage>

4.18. Ciberterrorismo

Em relação aos ciberataques, não podemos deixar de mencionar o terrorismo, que é uma das actuais ameaças globais, ou o seu notável crescimento dinâmico e espalhado por todo o mundo.

O terrorismo pode ser dividido segundo a forma em formas *letais* e *não letais*, em que o primeiro grupo se caracteriza pelo uso de meios de violência comuns (*convencionais* - ataques cometidos utilizando armas normalmente disponíveis, tais como armas de fogo e não convencionais - uso indevido de armas de destruição maciça). No entanto, as **formas não letais de terrorismo** [1] ou ataques que utilizam instrumentos mais modernos em combinação com meios letais são mais comuns na Internet.

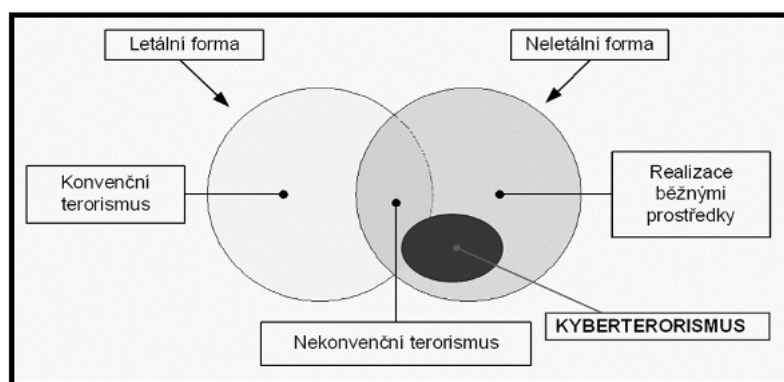
A forma convencional de terrorismo não letal inclui os seguintes subgrupos:

- *Terrorismo desarmado*.

- *Ciberterrorismo*, um dos maiores perigos do século XXI. O princípio é principalmente a má utilização das TIC (incluindo a Internet) como meio e ambiente para a realização de um ataque. Tal como o clássico ataque terrorista convencional, esta é uma actividade planeada geralmente motivada política ou religiosamente e levada a cabo por pequenas estruturas organizadas em vez de militarmente. O objectivo destes grupos é principalmente o de influenciar a opinião pública. Devido à rápida disseminação das tecnologias de informação e comunicação em todo o mundo, o ciberterrorismo representa uma ameaça significativa e é cada vez mais utilizado por grupos terroristas. [2]

- *Terrorismo mediático*, no qual há um abuso planeado dos meios de comunicação e de outras armas psicológicas para influenciar as opiniões de toda a população ou de grupos-alvo da população.

Esta relação é muito bem caracterizada pelo diagrama apresentado na figura seguinte.



Formas de terrorismo, incluindo o ciberterrorismo

Texto sobre a figura:

Forma letal - Terrorismo convencional

Forma não letal - Implementação por meios comuns

Terrorismo não convencional

CIBERTERRORISMO

A natureza global do ambiente informático e de telecomunicações permite a transferência de informação e a coordenação de actividades terroristas em todo o mundo. Afirma-se, por exemplo, que o ataque ao WTC em Nova Iorque foi organizado utilizando a Internet.

Pode haver outros casos de má utilização da Internet para a divulgação de informação maliciosa ou para operações psicológicas relacionadas com o terrorismo nos meios de comunicação social. A Internet desempenha um papel significativo na divulgação de propaganda, ideologia ou intimidação, por exemplo publicando em linha execuções de prisioneiros [3], atraindo e mobilizando novos activistas, simpatizantes ou patrocinadores, defendendo actos terroristas e incitando indivíduos a cometê-los. Os sites de grupos terroristas na Internet contêm frequentemente instruções para fazer armas improvisadas, ou propaganda dirigida à geração mais jovem.

A Internet oferece oportunidades excepcionais a grupos extremistas e terroristas, bem como a indivíduos, especialmente na área da comunicação rápida e relativamente secreta, onde serve para trocar informações e instruções para o planeamento e coordenação de eventos ou transferência de fundos.

Quase todos os grupos e organizações terroristas gerem os seus sites web. São geralmente publicados em várias versões linguísticas, e há também páginas especiais destinadas a crianças e mulheres que contêm contos de fadas ou banda desenhada, que incorporam, por exemplo, as histórias de bombistas suicidas. [4]



TravelWest.info website depois de ter sido atacado por atacantes

Possibilidades de sanções penais na República Checa

Do ponto de vista do direito penal, os actos acima mencionados podem cumprir os elementos objectivos das infracções criminais ao abrigo da **Secção 311(2)** (Ataque Terrorista), **Secção 355** (Difamação de Nação, Raça, Étnia ou outro Grupo de Pessoas), **Secção 356** (Instigação do ódio contra um Grupo de Pessoas ou da Supressão dos seus Direitos e Liberdades), **Secção 364** (Incitação à Ofensa Criminal), **Secção 403** (Estabelecimento, Apoio e Promoção de Movimentos Destinados à Supressão dos Direitos Humanos e Liberdades) e **Secção 404** (Expressão de Simpatias para Movimentos que Procuram Suprimir os Direitos Humanos e Liberdades) do Código Penal.

Possibilidades de sanções penais na Polónia

Na Polónia, os Artigos 265º a 269º e 287º do Código Penal aplicam-se à implementação de um ataque ciberterrorista e, dependendo do efeito do ataque ciberterrorista, alguns outros Artigos do Código Penal podem também ser aplicáveis, tais como

Arte. 163 Causar uma catástrofe

Arte. 164. Causar o perigo de uma catástrofe

Arte. 165. Causar perigo público

Arte. 173. Causar um acidente de viação

Arte. 174. Causar o perigo iminente de um desastre de trânsito

Possibilidades de sanções penais em Portugal

De acordo com a Lei n.º 52/2003, sobre a luta contra o terrorismo, se ligado a intenções terroristas, as penas para infracções tais como fraude informática ou falsificação informática serão agravadas por um terço (n.º 2 do artigo 4.º). Para além disso, a procaução pública de infracções relacionadas com comunicações electrónicas (art. 4 (3) (4), recrutamento (art. 4 (5) (6) ou a promoção de grupos ou acções terroristas são agravadas se praticadas pela Internet (art. 4 (8) (9)).

[1] No entanto, é possível imaginar uma combinação destes ataques. Para mais detalhes, ver, por exemplo

Exclusivo: Vírus de Computador atinge a U.S. Drone Fleet. [online]. [cit.10.7.2016]. Disponível a partir de: <https://www.wired.com/2011/10/virus-hits-drone-fleet/>

[2] JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praga: Grada, 2007, p. 129

[3] O URL apresentado não é censurado e contém filmagens drásticas! Ver, por exemplo

ATENÇÃO: ISIS Downs Prisioneiros Vivos & Rebenta Reféns Com RPG & Mata Outros Com Explosivos - vídeo gráfico. [online]. [cit.20.8.2016]. Disponível a partir de: <https://www.zerocensorship.com/uncensored/isis/drowns-prisoners-alive-blows-hostages-up-with-rpg-kills-others-with-explosives-graphic-video-132382>

O perturbador vídeo ISIS mostra militantes a decapitar quatro prisioneiros e pistoleiros a executar compradores no mercado. [em linha]. [cit.20.8.2016]. Disponível a partir de: <http://www.mirror.co.uk/news/world-news/disturbing-isis-video-shows-militants-7306017>

[4] JIROVSKÝ, Václav. *Kybernetická kriminalita nejen o hackingu, crackingu, virech a trojských koních bez tajemství*. Praga: Grada, 2007, p. 138

Ver também, por exemplo:

Ciberterrorismo: Quão perigosa é a ameaça do Ciber-califado ISIS? [em linha]. [cit.20.8.2016]. Disponível em: <http://www.govtech.com/blogs/lohrmann-on-cybersecurity/Cyber-Terrorism-How-Dangerous-is-the-ISIS-Cyber-Caliphate-Threat.html>

Divisão de Hacking do Estado Islâmico. [online]. [cit.20.8.2016]. Disponível em: https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=698&Itemid=1355

4.19. RESUMO / PRINCIPAIS RESULTADOS DO CAPÍTULO



RESUMO

- Uma parte significativa do cibercrime utiliza ou transmite tipos notórios de actividades ilegais (tais como fraude, violação de direitos de autor, roubo, intimidação, etc.) para o ambiente digital, onde podem ser cometidos "melhor, mais rápida e mais eficazmente" do que no mundo real. Os ciberataques puros podem incluir, por exemplo, hacking, ataques DoS e DDoS, botnets, etc.
- Com o desenvolvimento de serviços baseados no princípio do "as-a-service", surgiram várias plataformas (tipicamente subterrâneas, fóruns escuros) no ambiente do cibercrime, onde são oferecidos serviços que podem ser descritos como **crime como um serviço** (cibercrime- as-a-service). Assim, surge um "*malware* ou *economia subterrânea*" que fornece a quase todos os utilizadores os meios para cometerem crimes cibernéticos.
- O capítulo introduz os ciberataques básicos. É apresentado um modus operandi típico, bem como as possibilidades de sanções penais para estas acções.
- O cibercrime pode ser definido como uma conduta dirigida contra um computador ou, em alguns casos, contra uma rede informática, ou como uma conduta em que um computador é utilizado como um instrumento para cometer um crime. Um critério indispensável para a aplicação da definição de cibercriminalidade é o facto de a rede informática, ou ciberespaço, ser então o ambiente em que esta actividade tem lugar.



PALAVRAS-CHAVE A LEMBRAR

- engenharia social
- botnet
- malware
- ransomware
- spam
- esquema
- phishing
- pharming
- fraude
- hacking
- rachadura
- DoS, DDoS
- APT



PERGUNTAS DE VERIFICAÇÃO DE CONHECIMENTOS

- Que é característico da engenharia social?
- Que é uma botnet e como funciona?
- Quais são as típicas topologias botnet?
- É possível criminalizar um proprietário de uma botnet?
- Que é malware?
- Quais são os exemplos mais comuns de malware?
- Quais são os vectores de infecção por malware mais comuns?
- Que é um resgate e quais são as suas manifestações?
- Que é o phishing e como é este ataque mais frequentemente conduzido?
- Qual é a diferença entre phishing e pharming?
- Que é hacking?
- Que é característico para rachar?

- Qual é a diferença entre hacking e cracking?
- que é um ataque DoS e como é que funciona?
- Qual é a diferença entre DoS e DDoS?
- Que pode ser incluído na distribuição de conteúdo defeituoso?
- Que é APT?

5. Conclusão

Acredito firmemente que o ciberespaço não deve tornar-se um ambiente onde qualquer crime possa ser cometido com impunidade. Por outro lado, as regras e condições devem ser estabelecidas para que não se torne um ambiente em que a censura e a repressão prevaleçam. O equilíbrio destes dois níveis é um pré-requisito fundamental para a aplicação e, em particular, o respeito das regras no ciberespaço, quer sejam legais ou morais.

No que respeita à aplicação de possíveis normas de direito penal a certos tipos de ciberataques, deve notar-se que não é possível processar por lei penal tais condutas, por mais perigosas que sejam, que não estejam consagradas nos códigos penais de um país. O direito penal é um meio *ultima ratio* e como tal deve ser muito preciso para não interferir com os direitos e liberdades dos indivíduos em maior medida do que é estritamente necessário.

Para além do Estado, a protecção do ciberespaço e dos seus utilizadores é tratada por várias organizações privadas. Creio que se quisermos combater eficazmente o cibercrime, deverá haver uma cooperação mais eficaz das organizações privadas (especialmente peritos em TI, equipas CSIRT, etc.) com a administração pública (estatal), ou com as autoridades de aplicação da lei, de modo a que seja possível responder de forma atempada e adequada às formas cada vez mais sofisticadas de cibercrime ou ciberataques.

Como mencionei na introdução: *"A vida sem tecnologias de informação e comunicação é agora inconcebível ou impossível para a nossa sociedade"*.

A minha opinião é que não vale a pena livrar-se das TIC e dos serviços associados a estas tecnologias. O objectivo desta monografia não era forçar os utilizadores a desinstalar o Facebook e não utilizar o Google ou outros serviços. O objectivo era chamar a atenção para os possíveis riscos associados à utilização de tecnologias de informação e comunicação e serviços relacionados. Neste contexto, é necessário recordar a citação *Scientia est potentia* (**conhecimento é poder**). No caso das TIC e serviços relacionados, é necessário saber o que estas tecnologias e serviços representam, o que fazem e para que são utilizados.

A redução dos fenómenos negativos no ciberespaço e o esforço de mudança devem necessariamente começar pelos utilizadores finais porque no ciberespaço são eles que são a típica primeira vítima de um agressor. Ao mesmo tempo, os utilizadores são uma autoridade que pode definir que serviços, dados ou informações serão pesquisados, armazenados e fornecidos no ciberespaço.

Acredito que a educação e formação dos utilizadores deve ser uma parte essencial da penetração das tecnologias de informação e comunicação nas nossas vidas. A alfabetização da informação deve estar inextricavelmente ligada à criação, distribuição e promoção de produtos ou serviços associados às tecnologias da informação e da comunicação. A verdadeira educação nesta área, ou melhor, a aprendizagem sobre possíveis ameaças, riscos e inconvenientes colocados pelas TI, deve fazer parte do ensino de todas as formas de estudo em todos os níveis de ensino.

"Ninguém cometeu um erro maior do que aquele que

não fez nada porque só podia fazer um pouco".

Edmund Burke

6. Lista de referência

1. 10 Grupos de Hacking mais notórios. [online]. [cit.15.7.2016]. Disponível em: <https://www.hackread.com/10-most-notorious-hacking-groups/>
2. 7 Tipos de Motivações Hacker. [online]. [cit.16.8.2015]. Disponível em: <https://blogs.mcafee.com/consumer/family-safety/7-types-of-hacker-motivations/>
3. 7 Tipos de Hackers que Deve Conhecer. [online]. [cit.16.8.2015]. Disponível em: <https://www.cybrary.it/Op3n/types-of-hackers/>
4. Ameaça Persistente Avançada - ciclo de vida. [em linha]. [cit. 20. 8. 2016]. Disponível a partir de: https://upload.wikimedia.org/wikipedia/commons/7/73/Advanced_persistent_threat_lifecycle.jpg
5. Ameaça Persistente Avançada (APT). [online]. [cit. 20. 8. 2016]. Disponível a partir de: <http://searchsecurity.techtarget.com/definition/advanced-persistent-threat-APT>
6. Ameaça Persistente Avançada. [online]. [cit.20.8.2016]. Disponível em: <https://www.isouvislosti.cz/advanced-persistent-threat>
7. Ameaças Persistentes Avançadas: Como Funcionam. [online]. [cit.10.7.2016]. Disponível em: <https://www.symantec.com/theme.jsp?themeid=apt-infographic-1>
8. Adware. [online]. [cit.10.8.2016]. Disponível a partir de: <http://www.mhsaoit.com/computer-networking-previous-assignments/324-lesson-16-h-the-secret-history-of-hacking>
9. O Android Ransomware agora também tem como alvo a sua Smart TV, Too! [online]. [cit.14.8.2016]. Disponível a partir de: <https://thehackernews.com/2016/06/smart-tv-ransomware.html>
10. Distribuição da quota de mercado da versão Android entre os proprietários de smartphones a partir de Maio de 2016. [online]. [cit.14.8.2016]. Disponível a partir de: <http://www.statista.com/statistics/271774/share-of-android-platforms-on-mobile-devices-with-android-os/>
11. BALIGA, Arati, Liviu IFTODE e Xiaoxin CHEN. Contenção Automatizada de Ataques de Rootkits. *Computers & Security*, 2008, vol. 27, No. 7-8, pp. 323-334.
12. BAUDI, Pavel. Programy typu rootkit. Další hrozba pro Windows. *CHIP*, 2005, No. 7, p. 14
13. Cuidado com o Fake Android Prisma Apps Running Phishing, Malware Scam [online]. [cit.14.8.2016]. Disponível a partir de: <https://www.hackread.com/fake-android-prisma-app-phishing-malware/>
14. Botnet - Lista histórica de Botnets. [online]. [cit.15.8.2016]. Disponível a partir de: http://www.liquisearch.com/botnet/historical_list_of_botnets
15. Botnet. [cit.8.7.2016]. Disponível em: <http://research.omicsgroup.org/index.php/Botnet>
16. Botnet. [online]. [cit.15.7.2016]. Disponível a partir de: <https://en.wikipedia.org/wiki/Botnet>
17. Botnets. [online]. [cit.15.7.2016]. Disponível em: <https://www.youtube.com/watch?v=-8FUstzPixU&index=2&list=PLz4vMsOKdWVHb06dLjXS9B9Z-yFbzUWI6>
18. Botnety: nová internetová hrozba. [online]. [cit.15.7.2016]. Disponível a partir de: <http://www.lupa.cz/clanky/botnety-internetova-hrozba/>
19. Bots e Botnets - Uma Ameaça crescente. [online]. [cit.11.8.2016]. Disponível em: <https://us.norton.com/botnet/>
20. Buffalo Spammer jde na 7 let za mříže kvůli rozesílání nevyžádané pošty. [online]. [cit.14.8.2016]. Disponível a partir de: http://technet.idnes.cz/buffalo-spammer-jde-na-7-let-za-mrize-kvuli-rozesilani-nevyzadane-posty-13i-/tec_reportaze.aspx?c=A040528_28629_tec_aktuality
21. CARL, Glenn, Richard BROOKS e Rai SURESH. Detecção de Negação de Serviço com base em Wavelet. *Computers & Security*, 2006, vol. 25, No. 8, pp. 600-615
22. CHOO, Kim-Kwang Raymond. *Aliciamento de crianças em linha: uma revisão bibliográfica sobre a má utilização de sítios de redes sociais para aliciamento de crianças para delitos sexuais* [em linha]. Canberra: Instituto Australiano de Criminologia, c2009, [cit.19.3.2014]. ISBN 978-1-921532-33-7. Available from: <http://www.aic.gov.au/documents/3/C/1/%7b3C162CF7-94B1-4203-8C57-79F827168DD8%7drpp103.pdf>
23. Co je to botnet a jak se šíří? [online]. [cit.15.7.2016]. Disponível a partir de: <https://www.youtube.com/watch?v=ywXqDon5Xtg>
24. Co je to kyberšikana a jak se projevuje? [online]. [cit.19.8.2016]. Disponível a partir de: <http://www.bezpecne-online.cz/pro-rodice-a-ucitele/teenageri-a-komunikace-na-internetu/co-je-to-kybersikana-a-jak-se-projevuje.html>
25. Čosaskrývá v přílohe podvodných e-mailov? [online]. [cit.15.8.2016]. Disponível a partir de: <https://blog.nic.cz/2014/07/23/co-sa-skryva-v-prilohe-podvodnych-e-mailov-2/>
26. Co znamená příponasouboru SCR. [online]. [cit.14.8.2016]. Disponível em: <http://www.solvusoft.com/cs/file-extensions/file-extension-scr/>
27. Combate ao Cibercrime na Era Digital. [online]. [cit.7.5.2016]. Disponível a partir de: <https://www.europol.europa.eu/ec3>
28. A 'Queridinha' gerada por computador captura predadores em linha. [em linha]. [cit.19.8.2016]. Disponível em: <http://www.bbc.com/news/uk-24818769>

29. *Condenado spammer a desafiar a lei* Va. [online]. [cit.14.8.2016]. Disponível a partir de: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htm
30. *Ciberterrorismo: Quão perigosa é a ameaça do Ciber-califado ISIS?* [em linha]. [cit.20.8.2016]. Disponível em: <http://www.govtech.com/blogs/lohmann-on-cybersecurity/Cyber-Terrorism-How-Dangerous-is-the-ISIS-Cyber-Caliphate-Threat.html>
31. *Cibercriminalidade*. [online]. [cit.1.2.2015]. Disponível em: <http://www.britannica.com/EBchecked/topic/130595/cybercrime/235699/Types-of-cybercrime>; etc.
32. *Digital Doom's Digi World*, 2008. ISSN 1802-047X. [online]. [cit.14.8.2016]. Disponível a partir de: <http://www.ddworld.cz/software/windows/jak-se-krade-pomoci-internetu-phishing-v-praxi.html>
33. *Distribované výpočty*. [online]. [cit.2.11.2013]. Disponível em: <http://dc.czechnationalteam.cz/>
34. *O perturbador vídeo ISIS mostra militantes a decapitar quatro prisioneiros e pistoleiros a executar compradores no mercado*. [em linha]. [cit.20.8.2016]. Disponível a partir de: <http://www.mirror.co.uk/news/world-news/disturbing-isis-video-shows-militants-7306017>
35. DOČEKAL, Daniel. Bruce Schneier: *Internet věcí přinese útoky, které si neumíme představit*. [online]. [cit.10.8.2016]. Disponível a partir de: <http://www.lupa.cz/clanky/bruce-schneier-internet-veci-prinese-utoky-ktere-si-neumime-predstavit/>
36. DOČEKAL, Daniel. Google: *Adware napadá miliony zařízení a poškozuje inzerenty, weby i uživatele*. [online]. [cit.10.8.2016]. Disponível a partir de: <http://www.lupa.cz/clanky/google-adware-napada-miliony-zarizeni-a-poskozuje-inzerenty-weby-i-uzivatele/>
37. Protocolo adicional. ETS No. 189 Protocolo Adicional à Convenção sobre Cibercriminalidade, relativo à criminalização de actos de natureza racista e xenófoba cometidos através de sistemas informáticos <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/189>
38. DODGE, Ronald. C., Curtis CARVE e Aaron J. FERGUSON. Phishing for User Security Awareness. *Computers & Security*, 2007, vol. 26, No. 1, pp. 73-80.
39. *Dvanáctiletá dívka se zabila po téměř roční šikaně na internetu*. [online]. [cit.19.8.2016]. Disponível a partir de: <https://www.novinky.cz/zahranicni/amerika/313386-dvanactileta-divka-se-zabila-po-temer-rocni-sikane-na-internetu.html>
40. *A Estónia recupera de um ataque maciço de DDoS*. [online]. [cit. 4. 3.2010] Disponível a partir de: http://www.usatoday.com/tech/news/techpolicy/2007-09-12-spammer-va_N.htmhttp://www.computerworld.com/s/article/9019725/Estonia_recovers_from_massive_DDoS_attack
41. *Exclusivo: Vírus de Computador atinge a U.S. Drone Fleet*. [online]. [cit.10.7.2016]. Disponível a partir de: <https://www.wired.com/2011/10/virus-hits-drone-fleet/>
42. *Luta contra o cibercrime: patrulhas cibernéticas e equipas de investigação na Internet para reforçar a estratégia da UE*. [em linha]. [cit.10.7.2016]. Disponível a partir de: <http://europa.eu/rapid/pressReleasesAction.do?reference=IP/08/1827>
43. *Os clones de aves Flappy Bird ajudam as taxas de malwares móveis a subir*. [online]. [cit.14.8.2016]. Disponível a partir de: <http://www.mcafee.com/us/security-awareness/articles/flappy-bird-clones.aspx>
44. *FLocker Mobile Ransomware Crosses to Smart TV*. [online]. [cit.14.8.2016]. Disponível a partir de: <http://blog.trendmicro.com/trendlabs-security-intelligence/flocker-ransomware-crosses-smart-tv/>
45. *A França deixa cair a controversa "lei Hadopi" depois de ter gasto milhões*. [em linha]. [cit.15.7.2016]. Disponível em: <https://www.theguardian.com/technology/2013/jul/09/france-hadopi-law-anti-piracy> etc.
46. *Frigorífico apanhado a enviar emails de spam em ataque de botnet*. [online]. [cit.17.5.2016]. Disponível em: <http://www.cnet.com/news/fridge-caught-sending-spam-emails-in-botnet-attack/>
47. GONZÁLES-TALAVÁN, Guillermo. Um filtro SMTP Anti-spam simples e configurável: Greilistas. *Computers&Security*, 2006, vol. 25, No. 3, pp. 229-236.
48. BOM BOM MARKETÓ, Marc. *Uma visão dos crimes no futuro*. [em linha]. [cit.13.11.2014]. Disponível a partir de: https://www.ted.com/talks/marc_goodman_a_vision_of_crimes_in_the_future#t-456071
49. *O Google diz que os melhores golpes de phishing têm uma taxa de sucesso de 45 por cento*. [em linha]. [cit. 14.8.2016]. Disponível em: <https://www.engadget.com/2014/11/08/google-says-the-best-phishing-scams-have-a-45-percent-success-r/>
50. GREENBERG, Andy. *Os hackers matam remotamente um jipe na auto-estrada - comigo dentro dela*. [em linha]. [cit.4.5.2016]. Disponível a partir de: <https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/>
51. GRIFFITHS, Mark. Criminalidade Informática e Hacking: uma questão séria para a Polícia? *The Police Journal*, 2000, vol. 73, No. 1, pp. 18-24.
52. GRÍVNA, Tomáš e Radim POLČÁK. *Kyberkriminalita a právo*. Praga: Auditório, 2008
53. *Hackeri se vydávají za Anonymous a hrozí útokem českým firmám*. [online]. [cit.16.8.2015]. Disponível a partir de: <http://www.lupa.cz/clanky/hackeri-vydavaji-se-za-anonymous-hrozi-utokem-na-ceske-firmy-chteji-zaplatit/>
54. *Hackeri zaútočili na uživatele Facebooku*. [online]. [cit.16.8.2015]. Disponível a partir de: <http://tech.ihned.cz/c1-37133210-hackeri-zautocili-na-uzivatele-facebooku-chteli-jejich-hesla>
55. HILL, Caxemira. *Estes dois jogadores de Diablo III roubaram armadura virtual e ouro - e foram processados pela IRL*. [online]. [cit.10.8.2015]. Disponível a partir de: <http://fusion.net/story/137157/two-diablo-iii-players-now-have-criminal-records-for-stealing-virtual-items-from-other-players/>

56. *Lista histórica de botnets*. [em linha]. [cit.15.8.2016]. Disponível em: <http://jpdias.me/botnet-lab/history/historical-list-of-botnets.html>
57. *Mapas históricos de redes informáticas*. [em linha]. [cit.10.7.2016]. Disponível em: <https://personalpages.manchester.ac.uk/staff/m.dodge/cybergeography/atlas/historical.html>
58. HOŘEJŠÍ, Jaromír. *Faleňý exekuční příkaz ohrozuje uživatele českých banco*. [online]. [cit.15.8.2016]. Disponível a partir de: <https://blog.avast.com/cs/2014/07/17/falesny-exekucni-prikaz-ohrozuje-uzivatele-ceskych-bank-2/>
59. *Como funcionam os APTs? O Ciclo de Vida das Ameaças Persistentes Avançadas (Infográfico)*. [online]. [cit. 10. 7. 2016]. Disponível em: <https://blogs.sophos.com/2014/04/11/how-do-apt-work-the-lifecycle-of-advanced-persistent-threats-infographic/>
60. *Como utilizar a Wireshark para capturar, filtrar e inspeccionar Pacotes*. [online]. [cit.15.7.2016]. Disponível a partir de: <http://www.howtogeek.com/104278/how-to-use-wireshark-to-capture-filter-and-inspect-packets/>
61. *Divisão de Hacking do Estado Islâmico*. [online]. [cit.20.8.2016]. Disponível em: https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&bind_to_category=content:37&tagId=698&Itemid=1355
62. *Jessica Logan – O resto da história*. [cit.8.8.2016]. Disponível em: <http://nobullying.com/jessica-logan/>
63. JIRÁSEK, Petr, Luděk NOVÁK e Josef PO`ÁR. *Výkladový slovník kybernetické bezpečnosti*. [online]. 2ª edição actualizada. Praga: AFCEA, 2015, p. 57 e 73. [online]. [cit.10.7.2016]. Disponível em: <https://www.govcert.cz/cs/informacni-servis/akce-a-udalosti/vykladovy-slovník-kyberneticke-bezpecnosti---druhe-vydani/>
64. JIROVSKÝ, Václav e Oldřich KRULÍK. *Základní definice vztahující se k tématu. Security magazín*, 2007, vol. 14, No. 2, p. 47.
65. *Juiz, 69 anos, que descarregou pornografia infantil enfrentando 'humilhação catastrófica'*. [em linha]. [cit.1.9.2009]. Disponível a partir de: <http://news.sciencemag.org/social-sciences/2015/02/facebook-will-soon-be-able-id-you-any-photo>
66. *Caso Kevin Mitnick: 1999*. [online]. [cit.2.11.2011]. Disponível a partir de: <http://www.encyclopedia.com/doc/1G2-3498200381.html>
67. KOLOUCH, Jan, Pavel BAŠTA et al. *CyberSecurity*. Praga: CZ.NIC, 2019. ISBN 978-80-88168-31-7.
68. KOLOUCH, Jan. *Evolution of Phishing and Business Email Compromise Campaigns in the Czech Republic*. In: *Investigação Académica e Aplicada em Ciências Militares e de Gestão Pública*. Budapeste: Universidade Nacional de Serviço Público, 2018, pp. 83-100. ISSN 2498-5392
69. KOLOUCH, Jan. *CyberCrime*. Praga: CZ.NIC, 2016. ISBN 978-80-88168-15-7
70. KOLOUCH, Jan e Andriana KROPÁČOVÁ. *Ransomware*. In: ZHUANG, Xiaodong. *Avanços recentes na Informática: Actas da 19ª Conferência Internacional sobre Informática*. B.m. : B.n. , 2015, pp. 304-307. Recent Advances in Computer Engineering Series, [Nr. 32]. ISBN 978-1-61804-320-7. ISSN 1790-5109.
71. *Kybergrooming*. [online]. [cit.19.8.2016]. Disponível a partir de: <http://www.policie.cz/clanek/vite-co-je-kybersikana.aspx>
72. *Kyberšikana I, II*. [online]. [cit.19.8.2016]. Disponível a partir de: <https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy>
73. *Kyberšikana I, II*. [online]. [cit.19.8.2016]. Disponível a partir de: <https://www.e-bezpeci.cz/index.php/component/content/article/7-o-projektu/925-materialy>
74. NÍVEL, Steven. *Hackers: Heróis da Revolução Informática*. Sebastopol, CA: O'Reilly Media, pp. 32-41. ISBN 978-1449388393.
75. LI, Tao, GUAN, Zhihong, WU, Xianrong. *Modelação e análise da propagação de minhocas activas com base em sistemas P2P. Computers & Security*, 2007, vol. 26, No. 3, pp. 213-218.
76. *Malware, mayhem, e a tomada de McColo*. [em linha]. [cit.14.8.2016]. Disponível a partir de: <http://betanews.com/2008/11/13/malware-mayhem-and-the-mccolo-takedown/>
77. MARCIÁ-FERNANDÉZ, Gabriel, Jesús E. DÍAZ-VERDEJO e Pedro GARCÍA-TEODORO. *Avaliação de um ataque de baixa taxa de DoS contra Servidores de Aplicação. Computers & Security*, 2008, vol. 27, No. 7-8, pp. 335-354.
78. MATĚJKA, Michal. *Počítačová kriminalita*. Praga: Computer Press, 2002
79. MELOY, Reid J. *STALKING (SEGUIMENTO OBSESSIONAL): UMA REVISÃO DE ALGUNS ESTUDOS PRELIMINARES*. [online]. [cit.3.10.2015]. Disponível em: http://forensis.org/PDF/published/1996_StalkingObsessi.pdf
80. MINAŘÍK, Pavel. *Wireshark - Paketová analýza pro všechny*. [online]. [cit.18.8.2016]. Disponível em: <https://www.systemonline.cz/it-security/wireshark-paketova-analyza-pro-vsechny.htm>
81. MITNICK, Kevin D. e William L., SIMON. *Ghost in the Wires: as minhas aventuras como o hacker mais procurado do mundo*. Nova Iorque: Little, Brown & Co, 2012. ISBN 9780316037723.
82. MITNICK, Kevin D. *A arte da intrusão: as histórias reais por detrás das explorações de hackers, intrusos e enganadores*. Indianapolis: Wiley, 2006. ISBN 0-471-78266-1.
83. MUELLER, Robert. [em linha]. [cit.3.4.2013]. Disponível a partir de: <https://archives.fbi.gov/archives/news/speeches/combating-threats-in-the-cyber-world-outsmarting-terrorists-hackers-and-spies>

84. Největší hackerský útok potvrzen. V ohrožení jsou stovky miliónů uživatelů. [online]. [cit.16.8.2015]. Disponível a partir de: <https://www.novinky.cz/internet-a-pc/bezpecnost/405260-nejvetsi-hackersky-utok-potvrzen-v-ohrozeni-jsou-stovky-milionu-uzivatelu.html>
85. O novo Ransomware codifica os seus ficheiros de jogo. [online]. [cit.14.8.2016]. Disponível a partir de: <https://techcrunch.com/2015/03/24/new-ransomware-encrypts-your-game-files/>
86. NIGAM, Ruchna. Uma linha temporal de botnets móveis. [online]. [cit.12.7.2016]. Disponível a partir de: <https://www.botconf.eu/wp-content/uploads/2014/12/2014-2.2-A-Timeline-of-Mobile-Botnets-PAPER.pdf>
87. OWASP, XSS [online]. [cit.15.7.2016]. Disponível em: [https://www.owasp.org/index.php/Cross-site_Scripting_\(XSS\)](https://www.owasp.org/index.php/Cross-site_Scripting_(XSS))
88. Senha Sniffer Spy. [online]. [cit.18.8.2016]. Disponível a partir de: <http://securityxploded.com/password-sniffer-spy.php>
89. Relatório de Trends de Actividade de Pesca. [online]. [cit.14.8.2016]. Disponível em: https://docs.apwg.org/reports/apwg_trends_report_q1_2016.pdf
90. Phishing pelos Números: Must-Know Phishing Statistics 2016. [online]. [cit. 14.8.2016]. Disponível a partir de: <https://blog.barkly.com/phishing-statistics-2016>
91. PLETZER, Valentin. Demaskovaný spyware. CHIP, 2007, No. 10, pp. 116-120.
92. PLOHMANN, Daniel, Elmar GERHARDS-PADILLA e Felix LEDER. Botnets: Detecção, Medição, Desinfecção e Defesa. ENISA, 2011. [online]. [cit.17.5.2015], p. 14. Disponível a partir de: <https://www.enisa.europa.eu/publications/botnets-measurement-detection-disinfection-and-defence>
93. Policejní ransomware. [online]. [cit.14.8.2016]. Available from: https://www.f-secure.com/documents/996508/1018028/multiple_ransomware_warnings.gif/8d4c9ca2-fc77-433d-ac16-7661ace37f88?t=1409279719000
94. Postřehy z bezpečnosti: Jinak Ransomware-krát. [online]. [cit.14.8.2016]. Disponível a partir de: <https://www.root.cz/clanky/postrehy-z-bezpecnosti-ransomware-sestkrat-jinak/>
95. PO 'ÁR, Josef. Informační bezpečnost. Plzeň: Aleš Čeněk, 2005
96. Pozor na zprávu o údajné neuhrazené pohledávce - jedná se o podvod. [online]. [cit.15.8.2016]. Disponível em: <https://www.csirt.cz/page/2073/pozor-na-zpravu-o-udajne-neuhrazene-pohledavce---jedna-se-o-podvod/>
97. Pozor na zprávu o výzvě k úhradě před exekucí - jedná se o podvod. [online]. [cit.15.8.2016]. Disponível a partir de: <https://www.csirt.cz/news/security/?page=87>
98. PROSISE, Chris e Kevin MANDIVA. Resposta a Incidentes & Forense Informática, segunda edição. Emeryville: McGraw-Hill, 2003
99. RAK, Roman e Radek KUMMER. Informační hrozby v letech 2007-2017. Security magazin, 2007, vol. 14, No. 1, p. 4.
100. Ransomware. [online]. [cit.14.8.2016]. Disponível a partir de: <https://www.trendmicro.com/vinfo/us/security/definition/ransomware>
101. Riziková komunikace: Kybergrooming [online]. [cit.19.3.2014]. Disponível a partir de: <http://www.e-nebezpeci.cz/index.php/rizikova-komunikace/kybergrooming>
102. SCHNEIER, Bruce. O crime: A Próxima Grande Coisa da Internet. [online]. [cit.6.11.2007]. Disponível em: <https://www.schneier.com/crypto-gram/archives/2002/1215.html>
103. SCHNEIER, Bruce. A Internet das Coisas Transformará os Hacks de Grande Escala em Catástrofes do Mundo Real. [online]. [cit.10.8.2016]. Disponível em: <https://motherboard.vice.com/read/the-internet-of-things-will-cause-the-first-ever-large-scale-internet-disaster>
104. SCHNEIER, Bruce. Os Sete Tipos de Hackers. [online]. [cit.16.8.2015]. Disponível em: https://www.schneier.com/blog/archives/2011/02/the_seven_types.html
105. SCHRYEN, Guido. The Impact that Placing Email Addresses on the Internet Has on the Receipt of Spam: An Empirical Analysis (O Impacto que a Colocação de Endereços de Email na Internet Tem na Recepção de Spam: Uma Análise Empírica). Computers & Security, 2007, vol. 26, No. 5, pp. 361-372.
106. Selfmite - SMS SMS de verme Android Selfmite regressa, mais agressivo do que nunca. [online]. [cit.14.8.2016]. Disponível a partir de: <http://www.pcworld.com/article/2824672/android-sms-worm-selfmite-returns-more-aggressive-than-ever.html>
107. kód cílí na mobily, šíří se jako lavina. [online]. [cit.17.5.2016]. Disponível a partir de: <https://www.novinky.cz/internet-a-pc/bezpecnost/401956-skodlivy-kod-cili-na-mobily-siri-se-jako-lavina.html>
108. Sledování zásilky České pošty aneb nová havěť. [online]. [cit.14.8.2016]. Disponível em: <http://www.viry.cz/sledovani-zasilky-ceske-posty-aneb-nova-havet/>
109. SMEJKAL, Vladimír, Tomáš SOKOL e Martin VLČEK. Počítačové právo. Praga: C. H. Beck, 1995
110. Smejkal, Vladimír. Kriminalita v prostředí informačních systémů a rekodifikace trestního zákoníku. Trestněprávní revue, 2003, vol. 2, No. 6, p. 161.
111. Smejkal, Vladimír. Kybernetická kriminalita. Plzeň: Aleš Čeněk, 2015
112. Estatísticas e Fatos sobre Spam. [online]. [cit.14.8.2016]. Disponível em: <http://www.spamlaws.com/spam-stats.html>

113. *Estatísticas de Spam*. [online]. [cit.14.8.2016]. Disponível a partir de: <https://www.spamcop.net/spamstats.shtml>
114. STRAUS, Jiří et al. *Kriminalistická metodika*. Plzeň: AlešČeněk, 2006
115. *Stuxnet*. [online]. [cit.23.7.2016]. Disponível em: <https://cs.wikipedia.org/wiki/Stuxnet>
116. *Livro de registo de ataques cibernéticos direccionados*. [em linha]. [cit.10.7. 2016]. Disponível em: <https://apt.securelist.com/#secondPage>
117. TAYLOR, Harriet. *Como a "Internet das Coisas" pode ser fatal*. [em linha]. [cit.17.6.2016]. Disponível em: <http://www.cnn.com/2016/03/04/how-the-internet-of-things-could-be-fatal.html>
118. *Aperto de mão TCP krok za krokem*. [online]. [cit.18.8.2016]. Disponível a partir de: <http://www.svetsiti.cz/clanek.asp?cid=TCP-handshake-krok-za-krokem-3122000>
119. *A Avaliação da Ameaça do Crime Organizado na Internet (IOCTA) 2014*. [em linha]. [cit.10.8.2015]. Disponível em: <https://www.europol.europa.eu/content/internet-organised-crime-threat-assessment-iocta>
120. *O Museu Malware @ Internet Archive*. [em linha]. [cit.17.5.2016]. Disponível a partir de: <https://labsblog.f-secure.com/2016/02/05/the-malware-museum-internet-archive/>
121. *O testemunho de um ex-hacker*. [em linha]. [cit.26.9.2008]. Disponível em: <http://www.pbs.org/wgbh/pages/frontline/shows/hackers/whoare/testimony.html>
122. *O primeiro malware móvel: como Kaspersky Lab descobriu Cabir*. [online]. [cit.29.6.2015]. Disponível a partir de: <http://www.kaspersky.com/about/news/virus/2014/The-very-first-mobile-malware-how-Kaspersky-Lab-discovered-Cabir>
123. Tinba: W32. *Tinba (Tinybanker)*. [online]. [cit.15.8.2016]. Disponível em: https://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp_w32-tinba-tinybanker.pdf
124. *Dica do mês Julho 2016 - Evite ser fisgado por Phishing*. [online]. [cit.14.8.2016]. Disponível em: <http://www.intermanager.org/cybersail/tip-of-the-month-july-2016-avoid-getting-hooked-by-phishing/>
125. *Top Spammer Sentenciado a Quase Quatro Anos*. [online]. [cit.14.8.2016]. Disponível a partir de: <http://www.pcworld.com/article/148780/spam.html>
126. Convenção sobre Cibercriminalidade. <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>
127. *Manual das Nações Unidas sobre a prevenção e controlo da criminalidade informática*. [em linha]. [cit.20.8.2016]. Disponível em: http://216.55.97.163/wp-content/themes/bcb/bdf/int_regulations/un/CompCrims_UN_Guide.pdf
128. *Války síťových robotů - jak fungují sítě botnets*. [online]. [cit.15.7.2016]. Disponível a partir de: http://tmp.testnet-8.net/docs/h9_botnet.pdf
129. *Víte co je KYBERŠIKANÁ?* [online]. [cit.19.8.2016]. Disponível a partir de: <http://www.policie.cz/clanek/vite-co-je-kybersikana.asp>
130. *Výzkum rizikového chování českých dětí v prostředí internetu 2014*. [online]. [cit.19.8.2016]. Disponível a partir de: https://www.e-bezpeci.cz/index.php/ke-stazeni/doc_download/61-vyzkum-rizikoveho-chovani-eskych-dti-v-prostedi-internetu-2014-prezentace
131. *Advertência! Mais de 900 milhões de telefones Android Vulneráveis ao Novo Ataque "QuadRooter"*. [online]. [cit.10.8.2016]. Disponível a partir de: <https://thehackernews.com/2016/08/hack-android-phone.html>
132. *ATENÇÃO: ISIS Downs Prisioneiros Vivos & Rebenta Reféns Com RPG & Mata Outros Com Explosivos - vídeo gráfico*. [online]. [cit.20.8.2016]. Disponível a partir de: <https://www.zerocensorship.com/uncensored/isis/drowns-prisoners-alive-blows-hostages-up-with-rpg-kills-others-with-explosives-graphic-video-132382>
133. WILSON Tracy, V. *Como funciona a Phishing*. [online]. [cit.14.8.2016]. Disponível em: <http://computer.howstuffworks.com/phishing.htm>
134. Xshqi - *Minhoca Andróide no dia dos namorados chineses*. [online]. [cit.14.8.2016]. Disponível a partir de: <https://securelist.com/blog/virus-watch/65459/android-worm-on-chinese-valentines-day/>
135. *Yahoo řeší, jestli má hacker opravdu údaje o 200 milíonech účtů*. [online]. [cit.16.8.2015]. Disponível a partir de: <http://www.lupa.cz/clanky/yahoo-resi-jestli-hacker-opravdu-ma-udaje-o-200-milionech-tamnich-uctu/>
136. YAR, Majid. Hacking informático: Apenas mais um caso de delinquência juvenil? *The Howard Journal*, 2005, vol. 44, No. 4, pp. 387-399.
137. ZETTER, Kim. *É Possível para Passageiros Hackear Aeronaves Comerciais?* [online]. [cit.5.5.2016]. Disponível em: <https://www.wired.com/2015/05/possible-passengers-hack-commercial-aircraft/>
138. *Znovu se objevily podvodné zprávy*. [online]. [cit.15.8.2016]. Disponível em: <https://www.csirt.cz/news/security/?page=97>