Wilfredo Enrique Pires Pacheco

Manual de Responsabilização Penal de Hackers, Crackers e Engenheiros Sociais

1ª Edição

2011

O Autor é especialista e consultor em Direito Aplicado à Informática, servidor público federal e Coordenador da Ouvidoria do Conselho Nacional do Ministério Público em Brasília/DF.

Pós-Graduado em Direito, Estado e Constituição, e bacharel em Direito pelo Centro Universitário de Brasília - UniCEUB, laborou na 6ª Procuradoria de Justiça Criminal do Ministério Público do Distrito Federal e Territórios, e na 16ª Vara Federal da Seção Judiciária do Distrito Federal.

Entusiasta do ramo tecnológico, *geek* assumido e programador nas linguagens Java, C# e C++, com ênfase em Programação Multithreading (OpenMP).

Email para contato: wilfredo.enrique@gmail.com

Índice

Introdução

O presente manual objetiva esclarecer alguns conceitos relativos aos novos fenômenos jurídicos que surgiram com o avanço tecnológico no setor da Informática e Tecnologia de Informações, e, traçados tais conceitos, apontar as conseqüências jurídicas pertinentes a tal fenômeno.

O público algo dessa obra, portanto, se torna por demais abrangente, haja vista que tais conseqüências jurídicas podem demandar a atuação e o conhecimento das mais variadas profissões. Ao desenvolvedor de software, é importante que se conheça os seus direitos e obrigações, e a responsabilização que possa receber no caso de criação de códigos maliciosos ou no caso de causar danos envolvendo o meu digital. Ao administrador de sistemas informáticos, é relevante que saiba quais atos dos usuários do sistema que administra podem ser considerados crimes digitais, ou como elaborar políticas de utilização dos recursos tecnológicos que previnam tais cominações.

O crime digital é modalidade de delito perpetrado por intermédio de meio eletrônico digital, ou que afete o objeto tutelado e protegido pelo Direito Penal, o qual pode consistir em aparelho digital físico (hardware), suporte lógico (software) ou dados armazenados por sistemas de tecnologia de informação.

Ante a ampla possibilidade de ataques digitais, os instrumentos do crime podem ser dos mais variados, tais como computadores de mesa (Desktops), computadores portáteis (notebooks e netbooks), telefones celulares com funções integradas (smartphones), ou dispositivos mais singelos tecnologicamente, tais como circuitos integrados (processadores ou chips), dispositivos de armazenamento de dados (pendrives ou hard disks) ou outros dispositivos similares que processem dados, além dos recursos empregados por meio de engenharia social.

Por meio do Projeto de Lei da Câmara nº 83, de 2003, e do Projeto de Lei do Senado nº 363, de 2011, o legislador derivado houve por bem estabelecer alguns conceitos de

Tecnologia de Informação aos quais faz-se necessário referenciar para fins penais, nos seguintes termos:

> Art. 154-C. Para os efeitos penais, considera-se:
>
> I – **dispositivo de comunicação**: o computador, o telefone celular, o processador de dados, os instrumentos de armazenamento de dados eletrônicos ou digitais ou similares, os instrumentos de captura de dados, ou qualquer outro meio capaz de processar, armazenar, capturar ou transmitir dados utilizando-se de tecnologias magnéticas, óticas ou qualquer outra tecnologia eletrônica ou digital ou similar;
>
> II – **sistema informatizado**: o equipamento ativo da rede de comunicação de dados com ou sem fio, a rede de telefonia fixa ou móvel, a rede de televisão, a base de dados, o programa de computador ou qualquer outro sistema capaz de processar, capturar, armazenar ou transmitir dados eletrônica ou digitalmente ou de forma equivalente;
>
> III – **rede de computadores**: os instrumentos físicos e lógicos através dos quais é possível trocar dados e informações, compartilhar recursos, entre máquinas, representada pelo conjunto de computadores, dispositivos de comunicação e sistemas informatizados, que obedecem de comum acordo a um conjunto de regras, parâmetros, códigos, formatos e outras informações agrupadas em protocolos, em nível topológico local, regional, nacional ou mundial;
>
> IV – **defesa digital**: manipulação de código malicioso por agente técnico ou profissional habilitado, em proveito próprio ou de seu preponente, e sem risco para terceiros, de forma tecnicamente documentada e com preservação da cadeia de custódia no curso dos procedimentos correlatos, a título de teste de vulnerabilidade, de resposta a ataque, de frustração de invasão ou burla, de proteção do sistema, de interceptação defensiva, de tentativa de identificação do agressor, de exercício de forense computacional e de práticas gerais de segurança da informação.

O que é relevante juridicamente ao Direito da Informática é a intenção de afetar, influenciar ou corromper outro sistema de tecnologia de informação.

Essa seara é estudada pelo Direito Penal Eletrônico ou Informático, o qual se analisa as implicações jurídicas e o direito positivo pertinente aos meios eletrônicos no tocante às conseqüências criminais.

Com o notável avanço tecnológico nas áreas da tecnologia da informação, é perceptível o distanciamento da tecnologia em relação ao momento histórico no bojo do qual foi promulgado o Código Penal vigente, restando aos operadores do Direito a difícil missão de conciliar os institutos com as mudanças tecnológicas atuais.

É necessário, portanto, analisar casuisticamente os elementos típicos dos crimes digitais e verificar a quais espécies normativas penais pode determinada conduta ser subsumida de forma adequada, haja vista que a especificidade da conduta delitiva digital, em todas as circunstâncias que deveriam ser penalmente relevantes, pode não estar suficientemente abrangida por um tipo penal retrógrado.

Objetivou-se, no presente trabalho, esclarecer quais são as espécies de crimes digitais praticados e quais as conseqüências jurídico-penais advindas de tais condutas.

É o que passamos a especificar a seguir.

1) Malware

Embora seja um conceito de ampla utilização na comunidade digital, o malware não possui uma definição universalmente aceita, e sequer a sua taxonomia e classificação tipológica encontra consenso.

Malware seria um código de computador (software) que não possui pretensão legítima de utilização dos recursos físicos da máquina, o fazendo de forma furtiva. Podem desviar, impedir ou comprometer a utilização usual do dispositivo em que se aloja, bem como desviar as informações da máquina ou ganhar acesso autorizado aos recursos do sistema, entre outros comportamentos abusivos.

Arrolaremos as principais características de cada tipo de malware de acordo com o seu *modus operandi*, a partir da forma de atuação promíscua dentro da máquina hospedeira.

Há três características básicas aos malwares, quais sejam:

1 - **Auto-propagação**: O malware tenta ativamente a sua propagação pela criação de outras cópias ou instâncias de seu próprio código malicioso. Também pode se propagar de forma passiva, nos casos em que os usuários mesmo copiem acidentalmente o seu código para outra máquina, por exemplo, o que descaracterizaria, porém, uma auto-propagação típica.

2 - **Crescimento exponencial da contaminação**: O malware caracteriza-se também pela grande taxa de propagação e crescimento populacional entre equipamentos hospedeiros. Ao exemplo, o malware do tipo cavalo de tróia (trojan) TDL-4 infectou, nos três primeiros meses de 2011, 4,5 milhões de computadores no mundo todo.

3 - **Arquivo de execução**: Um malware necessita de um arquivo de execução para funcionar e se propagar, que seria um código que, ao ser ativado na máquina hospedeira, realiza uma série de tarefas e operações, as quais, em sua maioria, serão para realizar as atividades maliciosas, ou encobri-las. O arquivo de execução pode ser um bloco de código no boot (Master Boot Record) ou no

disco da máquina hospedeira, como um aplicativo compilado ou um código que requer compilação antes de sua execução.

Há atualmente várias espécies de malware de acordo com a sua característica precípua, o que não impede que haja um código híbrido, que abranja todas estas atividades:

Spyware: coleta informações dos usuários do sistema de forma furtiva, sem o conhecimento destes. Pode controlar o comportamento de navegação do usuário, monitorando em quais sites este comumente entra, quais produtos compra, e, por vezes, chega a registrar inclusive as teclas pressionadas no teclado (*keylogger*), com o intuito de descobrir senhas ou outros dados reservados.

Adware: é um código que automaticamente mostra propagandas e anúncios no computador hospedeiro, tendo como objetivo gerar renda ao agente desenvolvedor do código, que se remunera do número de vezes em que a propaganda é disponibilizada ou acessada pelo usuário da máquina hospedeira.

Worms: é um código que se propaga por rede, dispositivos de armazenamento móvel (*pendrives*) ou pela internet, se auto-replicando e infectando de forma automática. Usualmente não consome muitos recursos do equipamento infectado, e sua qualidade precípua é a auto-replicação. Usualmente infecta outros equipamentos, mas não corrompe e infect os arquivos do sistema, utilizando executáveis próprios.

Entre os *malwares*, há ainda os vírus e os cavalos de tróia, os quais serão abordados em detalhes a seguir, dada a relevância desse tema à correlata responsabilidade penal, e haja vista que são as espécies que mais causam danos aos equipamentos infectados.

2) Vírus de computador

Um vírus não tem um objetivo técnico intrínseco maior do que danificar a máquina hospedeira ou os dados que contém. Sua índole é primariamente a destruição, e não o roubo de informações ou a utilização dos recursos da máquina para outras finalidades delituosas.

Um vírus é um programa que se replica e se propaga de arquivo em arquivo no sistema infectado, bem como de máquina em máquina, sendo programado para apagar ou danificar os dados do equipamento.

O vírus, enquanto não for identificado e eliminado, infecta cada vez mais arquivos existentes no equipamento infectado. Ao contrário dos worms, que apenas criam uma nova cópia de si próprio, o vírus chega a corromper e integrar arquivos legítimos do equipamento, se inserindo no código binário destes.

Enquanto o worm funciona em um arquivo à parte, o vírus se integra aos arquivos legítimos do sistema.[1]

Há especialista que diferencia o vírus típico dos “virii”, nos seguintes termos:

> There's no agreement on the plural form of "virus." The two leading contenders are "viruses" and "virii;" the latter form is often used by virus writers themselves, but it's rare to see this used in the security community, who prefer "viruses."[2]

A primeira menção a vírus de computador ocorreu na obra de ficção científica The Scarred Man, escrito por Gregory Benford, datado de 1970, e por David Gerrold na obra When Harlie Was One, de 1972.

Em ambas as narrativas, há a descrição de um programa que age para conter o vírus, sendo, também, a primeira menção literária a programas anti-vírus que se tem notícia.

---

1 http://www.kaspersky.com/threats_faq

2 AYCOCK, John. Computer Viruses and Malware. University of Calgary, AB, Canada.Springer Ed. p. 14

A mais antiga pesquisa acadêmica acerca de vírus foi realizada por Fred Cohen em 1983, com a alcunha “vírus” tendo sido cunhada por Len Adleman.

Fred Cohen é comumente chamado de pai dos vírus de computador, mas há registros da existência de vírus criados em data anterior ao seu trabalho.

O vírus Elk Clones, criado por Rich Skrenta, já estava circulando em 1982, e os vírus desenvolvidos por Joe Dellinger foram concevidos entre 1981 e 1983. Todos estes códigos maliciosos foram desenvolvidos para atuarem na plataforma Apple II[3], tendo em vista que o sistema operacional mais utilizado no mundo, o Windows, só tenha sido lançado em 1985.

Alguns citam a falha de 1980 na Arpanet[4] como o primeiro vírus de computador, mas trata-se, apenas, de um código legítimo que funcionou de forma incorreta, não tendo propagado nada além de pacotes de dados.

Gregory Benford, além de ter citado de forma literária os vírus de computador, também concebeu vírus não maliciosos em 1969, no Laboratório Nacional Lawrence Livermore[5], e também na antiga Arpanet.

Um vírus pode se propagar dentro de um mesmo computador, afetando mais e mais arquivos do sistema de dados, ou, ainda, de um computador para outro, por meio de

---

3 “The Apple II series (Trademarked with brackets as "Apple][") is a set of 8-bit home computers, one of the first highly successful mass-produced microcomputer products,[1] designed primarily by Steve Wozniak, manufactured by Apple Computer (now Apple Inc.) and introduced in 1977 with the original Apple II. In terms of ease of use, features and expandability the Apple II was a major technological advancement over its predecessor, the Apple I, a limited-production bare circuit board computer for electronics hobbyists that pioneered many features that made the Apple II a commercial success. Introduced at the West Coast Computer Faire in 1977, the Apple II was among the first successful personal computers; it launched the Apple company into a successful business (and allowed several related companies to start).” in http://en.wikipedia.org/wiki/Apple_ii

4 “The Advanced Research Projects Agency Network (ARPANET), was the world's first operational packet switching network and the core network of a set that came to compose the global Internet. The network was funded by the Defense Advanced Research Projects Agency (DARPA) of the United States Department of Defense for use by its projects at universities and research laboratories in the US. The packet switching of the ARPANET was based on designs by Lawrence Roberts of the Lincoln Laboratory.” in http://www.livinginternet.com/i/ii_roberts.htm

5 “MIT Lincoln Laboratory, located in Lexington, Massachusetts, is a United States Department of Defense research and development center chartered to apply advanced technology to problems of national security. Research and development activities focus on long-term technology development as well as rapid system prototyping and demonstration. These efforts are aligned within key mission areas. The Laboratory works with industry to transition new concepts and technology for system development and deployment.” in http://en.wikipedia.org/wiki/Lincoln_Laboratory

transporte de mídias realizado pelo próprio usuário dos sistemas, através de disquetes, CD-ROM, DVD-ROM, ou dispositivo portátil de interface USB (*pendrive*).

Teoricamente, o vírus de computador não se propaga em redes, somente se propagando no mesmo sistema de dados ou entre sistemas de dados. É característica intrínseca do worm, e não do vírus, a propagação por rede (internet ou intranet).

O vírus de computador possui três partes essenciais:

- **Mecanismo de infecção**: é por meio deste que o vírus se propaga, copiando seu próprio código para fazer uma cópia de si mesmo. É o seu vetor de infecção. Pode se propagar de diversas formas possíveis.
- **Gatilho (trigger)**: a condição que, se preenchida, ativa o resultado (payload) programado no vírus, tal como apagar arquivos de computadores que possuem Windows XP, ou que possua determinado programa instalado.
- **Payload (resultado)**: É o objetivo precípuo do vírus, e onde reside a sua motivação. É o resultado, a forma pela qual se dará o dano. Pode ser a corrupção de arquivos do sistema, inutilizando o uso padrão destes, a exclusão de arquivos, e, inclusive, a exclusão de informação da BIOS do aparelho, impedindo, em alguns casos, até que a máquina seja ligada. Pode ser, ainda, que um danos acidentais que não previstos pelo agente que desenvolveu o vírus surja, tendo em vista que o código malicioso pode encontrar equipamentos e softwares dos mais diversos tipos.[6]

Consideraremos para a presente análise como vírus de computador qualquer código malicioso digital elaborado com o intuito de modificar o fiel desempenho de máquina eletrônica digital ou desviar o seu uso, ou de seus recursos, para fins destrutivos, com o intuito de lesar estrutura de segurança, consumir recursos físicos ou digitais, ou causar danos a estrutura física (hardware), tendo como característica básica a sua habilidade de auto-reprodução e auto-propagação.

Tanto pode inutilizar ou estragar o hardware da máquina, quanto poderá apenas destruir suas informações. Em determinados aparelhos, um mau funcionamento de software

[6] AYCOCK, John. Computer Viruses and Malware. University of Calgary, AB, Canada.Springer Ed. p. 14

pode gerar danos físicos, ao exemplo, um vírus que desliga um cooler de resfriamento que é controlado digitalmente. Caso o vírus afete o software de controle de temperatura da máquina, poderá ocorrer um dano físico consistente no superaquecimento da máquina, lesionando sua estrutura de *hardware*. Caso o vírus apague arquivos, dados, ou os corrompa, estará lesando apenas o suporte lógico virtual, sem nenhum dano material.

Caso o objetivo desse código seja o envio e transmissão de informações, tratar-se-á de um Cavalo de Tróia ou de um *worm*. Portanto, o vírus usualmente objetiva a destruição ou corrupção de arquivos digitais, enquanto estes objetivam o envio não autorizado de dados e submeter a máquina a um controle remoto.

A conduta de implantar, propagar, instalar, ou induzir dolosamente sua execução, caso produza como resultado naturalístico a ocorrência de dano ao suporte lógico, é relevante penalmente, podendo ser imputado à conduta o crime de dano, nos termos do art. 163 do Código Penal, podendo ser incursa em sua modalidade qualificada. Vejamos o dispositivo legal:

> **Dano**
>
> Art. 163 - Destruir, inutilizar ou deteriorar coisa alheia:
>
> Pena - detenção, de um a seis meses, ou multa.
>
> **Dano qualificado**
>
> Parágrafo único - Se o crime é cometido:
>
> I - com violência à pessoa ou grave ameaça;
>
> II - com emprego de substância inflamável ou explosiva, se o fato não constitui crime mais grave;
>
> III - contra o patrimônio da União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista;
>
> IV - por motivo egoístico ou com prejuízo considerável para a vítima:
>
> Pena - detenção, de seis meses a três anos, e multa, além da pena correspondente à violência.

Se atingir, portanto, sistema informático de patrimônio de ente público, pode ser imputado o crime de dano qualificado, bem como se realizado por motivo egoístico ou com

prejuízo considerável à vítima. Dessa forma, a cominação depende da gravidade do resultado advindo dos ataques digitais.

A conduta, por si só, de desenvolver um vírus de computador não é penalmente relevante, desde que este não produza posteriormente o resultado naturalístico. É que o simples desenvolvimento de código malicioso pode ter outros fins que não o de causar dano, tal como finalidade acadêmica, educativa, de contra-inteligência, entre outras. Dessa forma, percebe-se que a ilicitude do delito reside, basicamente, no dolo empregado para a consecução de tais objetivos.

Caso o resultado se dê por conduta de outrem, pode ser o desenvolvedor responsabilizado na modalidade de participação ou co-autoria, por ter fornecido o instrumento do crime.

Para a perfeita tipificação do crime no caso de propagação de vírus de computador, faz-se necessária a análise do resultado causado. Implantado numa máquina doméstica, é possível que o vírus destrua arquivos pessoais, sendo caso de mero crime de dano. Se for implantado num sistema de propriedade federal, será crime de dano qualificado (art. 163, par. 1º, inc. III do CP), ou se adentrar em sistemas, ao exemplo, do Ministério da Defesa, ou da Agencia Brasileira de Inteligência, expondo dados afetos à segurança nacional, será crime de segurança nacional, incurso nas condutas típicas previstas na Lei Federal nº 7.170, de 14 de dezembro de 1983.

Listamos alguns tipos penais da referida lei de crimes contra a segurança nacional que podem ser imputados a determinadas condutas de crimes digitais:

> Art. 13 - Comunicar, entregar ou permitir a comunicação ou a entrega, a governo ou grupo estrangeiro, ou a organização ou grupo de existência ilegal, de dados, documentos ou cópias de documentos, planos, códigos, cifras ou assuntos que, no interesse do Estado brasileiro, são classificados como sigilosos.
>
> Pena: reclusão, de 3 a 15 anos.
>
> Parágrafo único - Incorre na mesma pena quem:
>
> I - com o objetivo de realizar os atos previstos neste artigo, mantém serviço de espionagem ou dele participa;

> II - com o mesmo objetivo, realiza atividade aerofotográfica ou de sensoreamento remoto, em qualquer parte do território nacional;
>
> III - oculta ou presta auxílio a espião, sabendo-o tal, para subtraí-lo à ação da autoridade pública;
>
> IV - obtém ou revela, para fim de espionagem, desenhos, projetos, fotografias, notícias ou informações a respeito de técnicas, de tecnologias, de componentes, de equipamentos, de instalações ou de sistemas de processamento automatizado de dados, em uso ou em desenvolvimento no País, que, reputados essenciais para a sua defesa, segurança ou economia, devem permanecer em segredo.

Vimos recentemente a onda de divulgação de informações confidenciais pelo site WikiLeaks. A depender do teor de tais dados, a divulgação pode perfeitamente se adequar aos tipos previstos na referida lei.

Pode advir da conduta resultados mais gravosos ainda, comprometendo bens penais mais caros ao nosso ordenamento jurídico. É o caso do direito à vida, que pode perfeitamente ser posto em ameaça por um vírus de computador. Ao exemplo, caso exponha vulnerabilidades e cause pane em um sistema de ferroviário ou de controle de vôo, pode expor a vida dos cidadãos em perigo. Então, a depender do resultado, pode ser imputado o crime de homicídio, ameaça, crimes referentes a desastres ferroviários, fluviais, aéreos ou de outros meios de transporte (Arts. 260 a 263 do CP).

Pode ser imputada, ainda, a conduta de atentado contra a segurança de serviço de utilidade publica, caso prejudique o fornecimento de água, luz, coleta de esgoto ou lixo (art. 265), bem como o crime de perturbação ou interrupção de serviço telegráfico ou telefônico, se afetar as redes de telecomunicação (art. 266).

Nesses casos, portanto, faz-se necessária a analise do resultado concreto causado pelo vírus de computador.

Caso não haja resultado naturalístico penalmente relevante, trata-se de mero indiferente penal.

Cumpre indagar se, ao implantar vírus de computador, ao agente pode ser imputado o crime de **supressão de documento**. Prescreve o Código Penal:

> Art. 305 - Destruir, suprimir ou ocultar, em benefício próprio ou de outrem, ou em prejuízo alheio, documento público ou particular verdadeiro, de que não podia dispor:
>
> Pena - reclusão, de dois a seis anos, e multa, se o documento é público, e reclusão, de um a cinco anos, e multa, se o documento é particular.

Entendemos que sim. É que, nos termos da Medida Provisória N. 2.200-2, de 24 de agosto de 2001, em seu art. 10, considera-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos de que trata a citada Medida Provisória. Ou seja, para a legislação brasileira, qualquer documento certificado digitalmente passa a ser juridicamente relevante para fins penais.

Caso o agente propague o vírus de computador e venha corromper banco de dados que contenha documentos subscritos por assinatura digital, certificados eletronicamente, cometerá o crime de supressão de documento.

3) Cavalos de Tróia e Spywares

É uma espécie de código malicioso que se apresenta inicialmente como um programa benigno para ser executado no aparelho-alvo, geralmente não possuindo potencial de auto-reprodução e propagação. Normalmente, é emitido para um alvo específico e deixa o aparelho-alvo sujeito a ordens específicas e remotas do agente que o implantou.

Pode corromper arquivos digitais no alvo, mas possui como objetivo maior o roubo de informações, a transmissão não autorizada de dados, e a submissão do aparelho ao controle do agente invasor, de forma a monitorar a atividade da máquina, capturar dados pessoais, ou transformar o aparelho em um instrumento de outros ataques.

A designação advém da lenda do Cavalo de Tróia presente no poema épico de Virgílio, A Eneida, no qual consta que os troianos receberam dos gregos, como presente, uma grande estátua de um cavalo, que continha ocultos 30 soldados gregos, e a posicionaram dentro de sua cidade fortificada. Após receber o presente, à noite, os soldados saíram do interior da estátua, que era oca, e abriram os portões para os soldados gregos entrarem. Esse estratagema foi decisivo para que destruíssem a cidade de Tróia e vencessem a guerra.

A alusão da lenda ao presente engodo digital refere-se à forma em que o código malicioso é inserido no sistema a ser invadido, tendo em vista que se mascara em forma de um código benigno, e é executado pela vítima como se o fosse, mas, abusando da confiança da vítima, é instalado o código malicioso.

Trojans são o primeiro estágio de um ataque cujo propósito primário é permanecer oculto enquanto baixando e instalando um código malicioso mais especializado e complexo, um bot[7]. Ao contrário de vírus e worms, trojans não se propagam por si mesmos. Eles comumente são entregues para uma vítima específica por meio de uma mensagem de email, mascarada por um artifício fraudulento, como uma mensagem amigável, uma suposta foto, ou um programa que faz passar por legítimo.

7

Quando presente esta característica de ser entregue a um destinatário específico, afigura-se mais ainda o dolo de lesionar, o que possui relevância penal para a demonstração da clara intenção do agente de lesionar o bem jurídico.

A instalação de um trojan pode ocorrer, ainda, por um site malicioso na internet, que, aproveitando-se de uma brecha de segurança nos programas de navegação (tais como Internet Explorer, Mozilla Firefox ou Google Chrome), instala o código malicioso na máquina infectada.

Após instalado, o *Trojan* se imiscui silenciosamente na máquina infectada, podendo obter informações privadas, ou puxar da internet, por instrução do agente criador, uma versão mais atualizada de seu código malicioso ou puxar outros trojans, vírus ou worms. O equipamento infectado fica, portanto, à total mercê do agente criminoso, enquanto a vítima usuária do sistema continua utilizando normalmente o equipamento.

Spywares é o termo geral para programas que monitoram a atividade do usuário da máquina infectada, de forma a obter informações pessoais, como logins, senhas, números de contas bancárias, arquivos, número do CPF ou do cartão de crédito.

Alguns spywares monitoram o comportamento pessoal do usuário do equipamento na internet, de forma a obter dados dos sites mais visitados, emails que escreveu ou recebe, ou conversas em programas de mensagem instantânea (MSN, ICQ, IRC, entre outros).

Após obter tais informações, o spyware as transmite a um servidor, controlado pelo agente criminoso, que usa tais dados para fins de propaganda e marketing direcionada. Por vezes, pode colher uma grande quantidade de dados, como emails pessoais, e vender a pessoas interessadas em realizar mala direta.

O spyware pode ser instalado na máquina de várias maneiras. Na maioria dos casos, são instalados junto com programas que você quer utilizar, mas que ocultam um código malicioso em sua instalação, implantando-o furtivamente.[8]

Ao exemplo, quando o usuário baixa um programa pirateado, uma suíte de aplicativo, ou baixa arquivos mediante serviços de compartilhamento *peer-to-peer* para seu computador e o instala, além do programa, pode estar instalando também o spyware. É comum páginas da internet instalarem furtivamente os spywares.

[8] http://us.norton.com/cybercrime/trojansspyware.jsp

O cavalo de tróia (trojan horse), ao seu turno, é um programa cujo propósito aparente é realizar operações legítimas no equipamento implantado, mas ocultamente realiza tarefaas maliciosas. Ao exemplo, seria o caso de quando o usuário instala um programa que automatiza a inserção de senhas e logins em determinada interface de autenticação, mas, ocultamente, este software armazena tais dados e o remete ao agente criminoso.[9]

A repercussão penal desse ilícito é bem aproximada dos vírus de computador, com a peculiaridade de que, nesta espécie, tem-se um maior perigo à intimidade e aos dados pessoais, tendo em vista que o objetivo deste código malicioso não é só a destruição e corrupção dos dados do sistema, mas a transmissão indevida desses.

Com a transmissão destes dados, a repercussão penal pode tomar diversas cominações.

Se o intuito da transmissão dos dados é causar lesão ao patrimônio, por exemplo, de um correntistas, estar-se-á diante de um possível crime de furto mediante fraude, ou estelionato.

> **Furto**
>
> Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:
>
> Pena - reclusão, de um a quatro anos, e multa.
>
> § 1º - A pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno.
>
> § 2º - Se o criminoso é primário, e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicar somente a pena de multa.
>
> § 3º - Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico.
>
> **Furto qualificado**
>
> § 4º - A pena é de reclusão de dois a oito anos, e multa, se o crime é cometido:
>
> I - com destruição ou rompimento de obstáculo à subtração da coisa;

[9] AYCOCK, John. Computer Viruses and Malware. University of Calgary, AB, Canada.Springer Ed. p. 13

> II - com abuso de confiança, ou mediante fraude, escalada ou destreza;
>
> III - com emprego de chave falsa;
>
> IV - mediante concurso de duas ou mais pessoas.
>
> § 5º - A pena é de reclusão de três a oito anos, se a subtração for de veículo automotor que venha a ser transportado para outro Estado ou para o exterior.

Importante criar a estreita ligação entre as técnicas de engenharia social e a implantação de cavalos de Tróia ou vírus de computador.

A engenharia social é técnica de fundamento psico-social, em que o agente dolosamente se utiliza de expediente sociais, tal como ligação telefônica, comunicação via chat, sistema de mensagem eletrônica, ou simples diálogo direto com a vitima, implanta código malicioso na máquina-alvo.

Estas técnicas eram o principal recurso utilizado pelo famoso hacker Kevin Mitnik, que utilizava do expediente psico-social de ludibriar empregados, secretárias, ou outros serventes, para que injetasse o código malicioso, ou conseguindo senhas privadas que muita das vezes são dados pessoais óbvios, de fácil dedução, como datas de aniversario. Ou, ainda, o emprego de expediente mais simples, como a inserção de *pendrive* (dispositivo de armazenamento de dados) no computador da vítima em um momento de distração.

Dessa forma, o modo de inserção do código malicioso, se feito por artífice ou método fraudulento, pode ser penalmente relevante, sendo caso de estelionato.

Se esse mesmo método for utilizado contra a administração publica, pode ocorrer hipótese de exploração de prestígio, prevaricação, entre outras modalidades de crimes próprios.

A prática de, por meio de código malicioso, interceptar emails, comunicação por mensagens instantâneas ou outras formas de interceptar tais dados, a depender do teor das comunicações, pode configurar o delito de violação de comunicação de informática, nos termos do Art. 10 da Lei Federal nº 9.296:

> Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei.

Quanto à conduta de uso indevido de login e senha, é possível que se comine um tipo penal específico para a referida conduta, que seria o do art. 307 do Código Penal. O login e senha, ou o uso de certificado digital de assinatura de terceiro indevidamente, tem como objetivo ganhar acesso a sistema de informática, fazendo-se passar por quem tenha acesso para tanto.

Dessa forma, o agente se utiliza de uma identidade alheia, usurpando os privilégios que outra pessoa teria para tanto, e, portanto, se utilizando de meio fraudulento para se identificar como o terceiro. É especificamente crime tal conduta, *in verbis*:

> **Falsa identidade**
>
> Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:
>
> Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.
>
> Art. 328 - Usurpar o exercício de função pública:
>
> Pena - detenção, de três meses a dois anos, e multa.
>
> Parágrafo único - Se do fato o agente aufere vantagem:
>
> Pena - reclusão, de dois a cinco anos, e multa.

Caso a utilização do Cavalo de Tróia desencadeie na aquisição de senha de acesso à conta corrente pela Internet (home banking), e o agente invasor consiga acesso aos dados bancários da vítima por meio telefônico, deste resultado pode ensejar a cominação das penalidades previstas para o tipo penal previsto na Lei Complementar nº 105, de 10 de janeiro de 2001.

Esta Lei dispõe sobre o sigilo das operações das instituições financeiras, visando tutelar o bem jurídico consistente no segredo de tais atividades financeiras, conforme seu art. 1º:

> Art. 1º As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados.
>
> § 1º São consideradas instituições financeiras, para os efeitos desta Lei Complementar:
>
> I – os bancos de qualquer espécie;
>
> II – distribuidoras de valores mobiliários;
>
> III – corretoras de câmbio e de valores mobiliários;
>
> IV – sociedades de crédito, financiamento e investimentos;
>
> V – sociedades de crédito imobiliário;
>
> VI – administradoras de cartões de crédito;
>
> VII – sociedades de arrendamento mercantil;
>
> VIII – administradoras de mercado de balcão organizado;
>
> IX – cooperativas de crédito;
>
> X – associações de poupança e empréstimo;
>
> XI – bolsas de valores e de mercadorias e futuros;
>
> XII – entidades de liquidação e compensação;
>
> XIII – outras sociedades que, em razão da natureza de suas operações, assim venham a ser consideradas pelo Conselho Monetário Nacional.

Além desses tipos penais, todos os tipos previstos para a conduta de propagar vírus de computador também são possíveis, a depender do caso, para quem se utilize de programas Cavalos de Tróia.

4) SQL Injection

Uma das formas mais utilizadas de se realizar a descaracterização de um site. Utiliza-se de um método de inserção de código de forma a burlar a forma de interpretação de ordens pelo banco de dados alvo, o qual interpreta a sintaxe SQL.

É a vulnerabilidade que resulta quando o agente criminoso consegue acessar e influenciar as consultas realizadas pela Linguagem de Consulta Estruturada (Structured Query Language) - SQL que uma aplicação passa ao seu banco de dados.

Sendo capaz de influenciar nas instruções que passa ao banco de dados, o agente criminoso pode utilizar a própria linguagem e sintaxe SQL para fins escusos, expondo os próprios recursos do sistema, a sua funcionalidade, bem como o próprio sistema operacional onde o banco de dados se aloja.

A técnica do SQL Injection não é exclusividade das aplicações Web, mas sim de qualquer programa que utilize uma interface de formulário dinâmico para se comunicar e realize consultas a um banco de dados que interpreta a linguagem SQL. Qualquer programa que aceite entradas de código de uma fonte não confiável pode ser vulnerável à esta técnica. E muitos programas atuais utilizam tal linguagem e interface, com mais frequencia ainda em ambientes corporativos, onde a carga de dados por vezes exige uma solução baseada em banco de dados.

Em fevereiro de 2002, Jeremiah Jacks (www.securityfocus.com/news/346) descobriu que o sítio na internet Guess.com era vulnerável à técnica do SQL Injection, resultando no acesso de informações de cartões de crédito de, ao menos, 200.000 clientes.

Em junho de 2003, Jeremiah Jacks (www.securityfocus.com/news/6194) utilizou esta técnica novamente no site PetCo.com, ganhando acesso aos dados de 500.000 cartões de crédito, por meio de uma falha no banco de dados SQL.

Em 17 de junho de 2005, a Mastercard alertou alguns de seus clientes que haveria uma brecha no sistema de segurança de seu sistema de cartões de crédito. Até o momento, é uma das maiores brechas de sua espécie já conhecida. Pela técnica do SQL Injection, um usuário malicioso teve acesso a mais a informações de mais de 40 milhões de cartões de crédito.

Funciona da seguinte forma: em sítios eletrônicos que se utiliza de páginas dinâmicas (a grande maioria dos sites atuais), sempre há um banco de dados, e a sintaxe SQL é a mais utilizada pelos diversos bancos de dados do mundo todo, sendo um grande padrão na área de gerenciamento de dados.

Por se tratar de uma linguagem extremamente poderosa e rica em recursos, o acesso à sintaxe desse sistema para executar comandos maliciosos pode causar grande dano ao sítio. Por meio dela, é possível o roubo de informações, bem como a destruição de dados, ou a descaracterização do site (*deface*).

Caracteriza, portanto, todas as figuras típicas previstas também para a prática de propagação de cavalo de tróia, no caso:

Por vezes, o conteúdo modificado indevidamente por meio da técnica de SQL Injection trás mensagens de ódio, acusações infundadas ou imputações inverossímeis a determinadas pessoas ou autoridades públicas. Nesses casos, pode ser incurso em crimes contra a honra, nos tipos de calúnia, injúria ou difamação.

Seguem abaixo os referidos tipos penais, previstos no Código Penal:

> **Calúnia**
>
> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
>
> Pena - detenção, de seis meses a dois anos, e multa.
>
> § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
>
> § 2º - É punível a calúnia contra os mortos.
>
> (...)
>
> **Difamação**
>
> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
>
> Pena - detenção, de três meses a um ano, e multa.
>
> (...)
>
> **Injúria**
>
> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:

Pena - detenção, de um a seis meses, ou multa.

§ 1º - O juiz pode deixar de aplicar a pena:

I - quando o ofendido, de forma reprovável, provocou diretamente a injúria;

II - no caso de retorsão imediata, que consista em outra injúria.

§ 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes:

Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.

§ 3o Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência:

Pena - reclusão de um a três anos e multa.

O cometimento de invasão mediante *SQL Injection* pode acarretar a exposição total do banco de dados e, dessa forma, expôr dados bancários e números de cartão de crédito.

Esta modalidade de invasão pode ser considerada conduta intermediária dos tipos penais de furto e estelionato, caso o agente aufira irregularmente valores pecuniários da conta corrente, ou outra vantagem pecuniária em prejuízo da vítima, tal como o pagamento indevido de boleto bancário em favor de terceiro.

Nesses casos, em havendo prejuízo pecuniário, ao exemplo, com a utilização de senhas bancárias para transferência de valores, pagamento de contas ou outras formas de desvio, restarão configurados, conforme o caso, os crimes de dano, estelionato ou furto.

Caso a invasão acarrete a destruição ou inutilização do sistema de informática da entidade vítima, então é possível a cominação das penas dos crimes de dano à conduta:

Dano

Art. 163 - Destruir, inutilizar ou deteriorar coisa alheia:

Pena - detenção, de um a seis meses, ou multa.

Dano qualificado

Parágrafo único - Se o crime é cometido:

I - com violência à pessoa ou grave ameaça;

II - com emprego de substância inflamável ou explosiva, se o fato não constitui crime mais grave

III - contra o patrimônio da União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista;

IV - por motivo egoístico ou com prejuízo considerável para a vítima:

Pena - detenção, de seis meses a três anos, e multa, além da pena correspondente à violência.

Se auferir dados de forma ilegítima, obtendo vantagem ilícita em prejuízo alheio, tal como utilizando os dados adquiridos de clientes de sites de compras online para abertura de contas correntes com o intuito de auferir empréstimo bancário, ou para enviar dinheiro pelo sistema de *homebanking* ao exterior, então seria caso da figura típica do estelionato, ou de suas figuras qualificadas:

Estelionato

Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:

Pena - reclusão, de um a cinco anos, e multa.

§ 1º - Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no art. 155, § 2º.

§ 2º - Nas mesmas penas incorre quem:

Disposição de coisa alheia como própria

I - vende, permuta, dá em pagamento, em locação ou em garantia coisa alheia como própria;

Alienação ou oneração fraudulenta de coisa própria

II - vende, permuta, dá em pagamento ou em garantia coisa própria inalienável, gravada de ônus ou litigiosa, ou imóvel que prometeu vender a terceiro, mediante pagamento em prestações, silenciando sobre qualquer dessas circunstâncias;

(...)

Fraude na entrega de coisa

IV - defrauda substância, qualidade ou quantidade de coisa que deve entregar a alguém;

(...)

§ 3º - A pena aumenta-se de um terço, se o crime é cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.

Merece maior repulsa do Direito Penal, ainda, o caso de o ataque por SQL Injection tenha afetado sistema informático de utilidade pública, tal como serviço de distribuição de água, energia, esgoto, trânsito, defesa nacional, sistema bancário central, de telecomunicação, entre outros.

Nesses casos, há a tipificação da conduta os crimes do art. 265 do Código Penal:

Atentado contra a segurança de serviço de utilidade pública

Art. 265 - Atentar contra a segurança ou o funcionamento de serviço de água, luz, força ou calor, ou qualquer outro de utilidade pública:

> Pena - reclusão, de um a cinco anos, e multa.
>
> Parágrafo único - Aumentar-se-á a pena de 1/3 (um terço) até a metade, se o dano ocorrer em virtude de subtração de material essencial ao funcionamento dos serviços.
>
> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
>
> Pena - detenção, de um a três anos, e multa.

Com a Medida Provisória N. 2.200-2, de 24 de agosto de 2001, em seu art. 10, considera-se documentos públicos ou particulares, para todos os fins legais, os documentos eletrônicos certificados digitalmente.

Tais documentos atualmente também possuem equivalência jurídica a sinais ou selos públicos, principalmente na área fiscal.

É o que se percebe da SPED - Sistema Público de Escrituração Digital, utilizado pela Receita Federal do Brasil para fins fiscais, tal como a emissão de declaração de impostos federais e lançamento fiscal automatizado.

É possível que um ataque por meio de SQL Injection corrompa, adultere ou modifique indevidamente tais dados digitais. Nesses casos, é possível cominar as penas dos tipos penais de falsificação de selo ou sinal público:

> **Falsificação do selo ou sinal público**
>
> Art. 296 - Falsificar, fabricando-os ou alterando-os:
>
> I - selo público destinado a autenticar atos oficiais da União, de Estado ou de Município;
>
> II - selo ou sinal atribuído por lei a entidade de direito público, ou a autoridade, ou sinal público de tabelião:
>
> Pena - reclusão, de dois a seis anos, e multa.
>
> § 1º - Incorre nas mesmas penas:

I - quem faz uso do selo ou sinal falsificado;

II - quem utiliza indevidamente o selo ou sinal verdadeiro em prejuízo de outrem ou em proveito próprio ou alheio.

III - quem altera, falsifica ou faz uso indevido de marcas, logotipos, siglas ou quaisquer outros símbolos utilizados ou identificadores de órgãos ou entidades da Administração Pública. (Incluído pela Lei nº 9.983, de 2000)

Quando seja outro documento que não selo público de autenticação de atos oficiais da União, Estados ou Municípios, mas simplesmente um documento público verdadeiro, pode-se cominar à conduta os tipos abaixos:

Art. 297 - Falsificar, no todo ou em parte, documento público, ou alterar documento público verdadeiro:

Pena - reclusão, de dois a seis anos, e multa.

Ou, ainda, se alterar ou defraudar documento privado assinado digitalmente, também é relevante penalmente, amoldável aos tipos penais abaixo:

Art. 298 - Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro:

Pena - reclusão, de um a cinco anos, e multa.

Falsidade ideológica

Art. 299 - Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante:

Pena - reclusão, de um a cinco anos, e multa, se o documento é público, e reclusão de um a três anos, e multa, se o documento é particular.

Supressão de documento

Art. 305 - Destruir, suprimir ou ocultar, em benefício próprio ou de outrem, ou em prejuízo alheio, documento público ou particular verdadeiro, de que não podia dispor:

Pena - reclusão, de dois a seis anos, e multa, se o documento é público, e reclusão, de um a cinco anos, e multa, se o documento é particular.

É possível, ainda, que, com a invasão por SQL Injection a sistema informático da Administraçao Pública, se obtenha dados reservados ou confidenciais, e se divulguem abertamente tais informações. Essa conduta é penalmente relevante, e se constitui divulgação de segredo, nos termos do art. 152, § 1o-A, do Código Penal:

Divulgação de segredo

Art. 153 – (...)

§ 1o-A. Divulgar, sem justa causa, informações sigilosas ou reservadas, assim definidas em lei, contidas ou não nos sistemas de informações ou banco de dados da Administração Pública:

Pena – detenção, de 1 (um) a 4 (quatro) anos, e multa.

§ 2o Quando resultar prejuízo para a Administração Pública, a ação penal será incondicionada.

Há, ainda, a possibilidade de que, com o acesso não autorizado por meio de ataque SQL Injection, se obtenha os dados de instituições financeiras. Porém, o sigilo de tais dados é resguardado pela Lei Complementar Federal nº 105, de 10 de janeiro de 2001, que pune tais condutas.

É o que prevê os arts. 1º e 10 da mencionada lei:

> Art. 1o As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados.
>
> Art. 10. A quebra de sigilo, fora das hipóteses autorizadas nesta Lei Complementar, constitui crime e sujeita os responsáveis à pena de reclusão, de um a quatro anos, e multa, aplicando-se, no que couber, o Código Penal, sem prejuízo de outras sanções cabíveis.

Percebe-se que o SQL Injection é um dos ataques mais lesivos possíveis a um sistema de informação com interface web, pois pode ensejar a exposição indevida de dados, a modificação ou destruição destes, e, ainda, a descaracterização do sítio eletrônico.

Uma conduta tão lesiva ao patrimônio alheio não pode ser ignorada pelo Direito Penal, o qual fornece subsídios suficientes para a adequada reprimenda estatal.

É necessário, porém, que a vítima e os funcionários de segurança saibam as efetivas consequencias jurídicas de tais atos, bem como que as autoridades policiais, membros do Ministério Público e juízes saibam identificar cada espécie, individualizar e aplicar corretamente os institutos jurídicos aqui expostos.

5) Denial of Service attack

É o abuso do uso de recursos de um site, que normalmente se dá por meio de botnets (network of computers controlled by cybercriminals using a Trojan or other malicious program[10]).

Um ataque de negação de serviço é desenvolvido para prejudicar ou inviabilizar totalmente o normal funcionamento de um sítio da web, um servidor ou outro recurso de rede. Há várias formas de agentes maliciosos realizarem tais ataques.

Um meio comum é sobrecarregar um servidor por meio do envio contínuo, anormal e de grande monta de requisições de dados, de forma a superar a capacidade normal de resposta dos recursos de rede do alvo. Isso irá fazer com que o servidor funcione de forma mais lenta do que o usual, trazendo um prejuízo ao legítimo uso dos aparelhos.

Ademais, pode acarretar na total inutilização do serviço web, parando o servidor, além de gastar de forma demasiada e injusta os recursos físicos necessários para manter tal estrutura, como serviços de manutenção, energia elétrica, serviço de refrigeração dos servidores, entre outros. Há um real gasto pecuniário advindo dessa conduta maliciosa, e isto não pode ser ignorado pelo Direito Penal, afora a clara responsabilidade civil.

Um ataque de negação de serviço difere dos outros pelo fato de que pode ser conduzido por uma série de máquinas controladas remotamente para realizar as requisições indevidas. São as chamadas zombie machines (máquinas-zumbi), as quais são controladas indevidamente e desviadas de seu uso padrão por se encontrarem expostas a vulnerabilidades em seus programas ou sistemas operacionais.

Tais vulnerabilidades podem ter sido implantadas pela propagação de malwares (worms, trojan horses ou spywares), ou pela simples exposição a vulnerabilidades inerentes ao sistema operacional ou aos programas típicos.[11]

O objetivo padrão de um ataque de negação de serviço é impedir o uso legítimo de aparelhos ou de recursos de rede por seus usuários usuais, por meio da sobrecarga de

[10] http://www.kaspersky.com/threats_faq
[11] http://www.kaspersky.com/threats_faq

acessos. Ao exemplo, no último ataque de negação de serviço ocorrido no dia 22 de junho de 2011 ao site da Presidência da Republica, houveram dois bilhões de requisiçoes de acessos, quando o normal seria apenas 10% deste número. Trata-se de uma forma de ataque em que nao há uma grave lesão à integridade de segurança de informação do sistema informáticos, mas apenas um abuso na utilização de seus recurso por parte de seus supostos clientes, que se tornam ilegítimos apenas pelo dolo de lesionar a fiel disposição do serviço.

É de se questionar se a conduta consistente no uso indevido dos recursos informáticos pode ensejar a incursão do agente nos crimes de furto de energia elétrica, na modalidade prevista em seu parágrafo único. Por obvio, o funcionamento de um servidor web só é possível com a utilização de energia elétrica. Ademais, esmiuçando-se o conceito de energia, segundo o dicionário, é de se questionar se a emissão de informacões por um servidor web nao é o bastante para se verificar um abuso no direito de acessar o site atacado e consumir seus recursos tecnológicos, os quais são mantidos por energia elétrica.

Entendemos que isto deve ser verificado caso a caso, a depender da estimativa de dano e do total de recursos consumidos. Esta estimativa deve ser apurada no caso concreto, de forma a se respeitar a razoabilidade e a fragmentariedade do Direito Penal.

Caso o ataque por negação de serviço atinja determinado serviço de comunicação, tal como uma rede social, um serviço de telefonia, ou de chamadas VoIP, ou ainda um serviço de mensagem instantânea, entendemos que é possível o enquadramento da conduta no tipo penal de violação de comunicação telegráfica, radioelétrica ou telefônica.

Em que pese seja discutível o enquadramento do meio de comunicação por internet como comunicação telegráfica ou radioelétrica, é certo que o aparelho de invasão, que pode ser um notebook, um tablet, um telefone celular, ou um circuito integrado conectado em rede WiFi, podem sem dúvidas serem considerados como aparelho radioelétrico, vez que se utilizam da emissão e recepção de ondas eletromagnéticas.

> Art. 151 – (...)
>
> Pena - detenção, de um a seis meses, ou multa.
>
> Sonegação ou destruição de correspondência
>
> § 1º - Na mesma pena incorre:
>
> I - quem se apossa indevidamente de correspondência alheia, embora não fechada e, no todo ou em parte, a sonega ou destrói;
>
> **Violação de comunicação telegráfica, radioelétrica ou telefônica**

> II - **quem indevidamente divulga, transmite a outrem ou utiliza abusivamente comunicação telegráfica ou radioelétrica dirigida a terceiro, ou conversação telefônica entre outras pessoas;**
>
> III - quem impede a comunicação ou a conversação referidas no número anterior;
>
> IV - **quem instala ou utiliza estação ou aparelho radioelétrico, sem observância de disposição legal.**
>
> § 2º - As penas aumentam-se de metade, se há dano para outrem.
>
> § 3º - Se o agente comete o crime, com abuso de função em serviço postal, telegráfico, radioelétrico ou telefônico:
>
> Pena - detenção, de um a três anos.
>
> § 4º - Somente se procede mediante representação, salvo nos casos do § 1º, IV, e do § 3º.

É possível que, do ataque de negação de serviço, haja a grave inutilização ou prejuízo da coisa alheia. É o caso de ataques que comprometam sites de compra, lojas virtuais, sites de serviços online, entre outros e-business. Com o ataque de negação de serviço a estes sites, impede-se que exerça o seu precípuo objetivo de realizar lucro, e, dessa forma, o prejuízo é expresso e quantificável.

Portanto, essa conduta não pode ser um mero irrelevante penal, mas sim encontra guarida na legislação penal, podendo, inclusive, ser enquadrada como crime de dano em sua modalidade qualificada:

> **Dano**
>
> Art. 163 - Destruir, inutilizar ou deteriorar coisa alheia:
>
> Pena - detenção, de um a seis meses, ou multa.
>
> Dano qualificado
>
> Parágrafo único - Se o crime é cometido:
>
> I - com violência à pessoa ou grave ameaça;
>
> (...)
>
> III - contra o patrimônio da União, Estado, Município, empresa concessionária de serviços públicos ou sociedade de economia mista;
>
> IV - por motivo egoístico ou com prejuízo considerável para a vítima:
>
> Pena - detenção, de seis meses a três anos, e multa, além da pena correspondente à violência.

Se o ataque tiver como alvo serviços de utilidade pública, também é passível de responsabilização penal:

> **Atentado contra a segurança de serviço de utilidade pública**
>
> Art. 265 - Atentar contra a segurança ou o funcionamento de serviço de água, luz, força ou calor, ou qualquer outro de utilidade pública:
>
> Pena - reclusão, de um a cinco anos, e multa.
>
> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
>
> Pena - detenção, de um a três anos, e multa.

Percebe-se, portanto, que um simples ataque digital pode tomar profundas conseqüências jurídicas, e, portanto, não pode ser ignorado pelas autoridades e negligenciados pelos administradores de sistemas informáticos.

O que se percebe é que não se dá a real importância à tais condutas delituosas, as quais muitas vezes passam incólumes de investigações ou perícias mais completas.

Mas é importante estudar e compreender seus efeitos e conseqüências jurídicas, principalmente pelas autoridades que participam da persecução penal, tais como delegados de polícia, membros do Ministério Público e magistrados.

6) Buffer Overflow

É o abuso do uso de recursos de um site, que normalmente se dá por meio de botnets (rede de computadores submetidos a ordens remotas).

O buffer overflow é uma modalidade de ataque que explora as brechas uma falha do código-fonte do programa de computador, de forma a exorbitar os limites de uma matriz de dados (array) e, ao extrapolar esses limites, inserir um código malicioso.

Normalmente, a array alvo do ataque é um buffer (retentor), um armazenador de dados temporários de leitura e escrita. Ao extrapolar o limite do buffer, há um acesso indevido ao buffer adjacente, ocorrendo uma violação à segurança da memória do programa.

O agente invasor que consegue escrever no buffer, direta ou indiretamente, pode expor todo o sistema de dados através da mudança dos dados na memória, levando o código a produzir efeitos que não eram originariamente previstos.

Dessa forma, o ataque pode se basear na execução de códigos arbitrariamente injetados pelo agente invasor no buffer de memória, e, dessa forma, dar acesso ao invasor com amplos privilégios.

Algumas linguagens de programação são tipicamente problemáticas e sucessíveis a estes erros, tais como as linguagens C e C++, haja vista não possuírem checagem automática dos limites da array (bounds checking).[12]

Cada vez mais tais espécies de ataques são raros, tendo em vista estas linguagens de programação não são tão mais usadas quanto outras que possuem bounds checkin (Java e C#).

Os efeitos penais são os mesmos de um vírus de computador, tendo em vista que expõe o código do programa aos efeitos maliciosos do agente invasor.

[12] AYCOCK, John. Computer Viruses and Malware. University of Calgary, AB, Canada.Springer Ed. p. 113

7) Brute Force Attack

Para compreender o brute force attack (ataque por força bruta), também conhecido como dictionary attack.

Em determinadas partes privativas de um site, ou de um banco de dados de um site, é necessário a utilização de senhas e logins para se ter acesso. É comum que estas partes contenham dados sigilosos e sensíveis ao site, e, portanto, se mostra como uma área propensa a ataques maliciosos, vez que pode armazenar dados de cartões de crédito e informações pessoais dos clientes.

Dessa forma, quebrar a autenticação de sites é um dos objetivos mais cobiçados por agentes maliciosos, justamente por disponibilizarem informações importantes e, nesse contexto, o brute force attack se mostra uma ferramenta interessante para tal propósito.

O ataque por força bruta é uma técnica relativamente simples e de baixa tecnologia, comparado aos outros métodos de ataque. O agente malicioso apenas tenta adivinhar o login e a senha, mediante uma série de combinações previamente determinadas, até conseguir acesso ao sistema informático.

Tecnicamente, as chances de um brute force attack lograr êxito podem ser muito boas, caso o site não esteja propriamente configurado. Um dos aspectos que mais explorados nessa espécie de ataque é a constatação de que a maioria das senhas são palavras comuns (123456, 11111, data de aniversário, entre outras), tendo em vista que o usuário procura definir senhas mais fáceis de serem memorizadas. [13]

Um ataque por força bruta, também chamado de exhaustive key search, é uma estratégia que, em tese, pode ser usada contra qualquer informação encriptada. Um ataque dessa espécie pode ser utilizado quando não é possível a utilização de qualquer outra técnica ou falha no sistema de autenticação que possa facilitar o ataque.

O agente malicioso, podendo se utilizar de um programa com esta finalidade, testa um número grande de senhas até encontrar a correta, utilizando, para isso, uma lista de senhas de grandes proporções (a maioria chega a ter na ordem de 1.000.000 registros), com as opções mais comuns.

[13] http://www.infosecwriters.com/text_resources/pdf/Brute_Force_BSullivan.pdf

Na pior das hipóteses, pode chegar a testar todas as possibilidades de senhas. Ao exemplo, num campo de senha de 4 dígitos numéricos, para se testar todas as senhas possíveis, são necessárias apenas 10.000 tentativas.

O tamanho das senhas de acesso utilizadas na encriptação dos dados determina a facilidade em se adivinhar a senha. Quanto mais longos os campos de senha, mais difícil se torna a utilização dessa técnica.[14]

É, em suma, um ataque que se baseia na tentativa e erro, na adivinhação, e se utiliza de um programa especialmente desenvolvido para esta finalidade, que testa as senhas no sistema a ser atacado de forma bastante rápida.

Esse ataque incide, portanto, na autenticação do site ou dos sistemas informáticos.

[14] http://en.wikipedia.org/wiki/Brute-force_attack

8) Pishing

Um ataque phishing é uma form específica de crime digital, na qual o agente criminoso cria uma réplica praticamente perfeita de um site, normalmente de uma instituição financeira que possibilita acesso à conta corrente por internet (homebanking), e, com esta réplica, tenta enganar o usuário a inserir nela seus dados pessoais, tais como senhas, logins, números de conta, entre outros.

Tais dados são inseridos por meio de um formulário, o qual simula um recurso legítimo da instituição financeira, mas, em verdade, é uma forma de enganar o usuário a roubar seus dados, e, de conhecimento destes, utilizá-los para o desvio de dinheiro das contas correntes.

Os phishers (agentes maliciosos que se utilizam da técnica do phishing) usam várias técnicas para divulgarem seus websites falsos, tal como encaminhar emails a diversas pessoas, fingindo ser um email legítimo da instituição financeira da qual o destinatário seja cliente.

Esses emails normalmente utilizam a marca, logotipo, aparência e estilo idênticos ao site legítimo da instituição financeira, ocultando o real destinatário do email malicioso.

Em geral, essas mensagens eletrônicas utilizam argumentos convincentes para que os clientes insiram seus dados pessoais, tal como que o sistema de informática do banco está passando por uma manutenção, e precisa que os dados sejam reinseridos no sistema, ou que os clientes precisam se recadastrar via internet.

Quando o destinatário entra no link do email malicioso, é automaticamente redirecionado a um site falso, onde são perguntados os dados pessoais do cliente.[15]

Phishing, portanto, é uma forma de adquirir informações importantes e que possuam relevância financeira, como logins, senhas ou informações de cartões de crédito, se passando por um site legítimo da entidade financeira da qual a vítima é cliente, induzindo-o por mensagem eletrônica.

---

15 http://www.kaspersky.com/phishing

O nome advém da prática de fishing (pesca), onde o pescador posiciona a isca no anzol. Da mesma forma, o agente malicioso posiciona a isca, no caso, o site fraudulento, para que a vítima caia no engodo de fornecer seus dados pessoais.

Falsos comunicados de sites, de empresas de processamento de pagamento eletrônico, de bancos ou de administradores de sistemas de informações são disseminados a potenciais clientes.

O phishing normalmente é aplicado por meio da disseminação em massa de emails ou de mensagens instantâneas, e direcionam a vítima formulários onde digitam seus dados pessoais, explorando o pouco conhecimento e a boa fé da vítima.

Utiliza-se, portanto, de ferramentas de engenharia social, tendo em vista que abusa da confiança depositada pela vítima no site ao qual foi direcionado.

Os ataques por phishing são normalmente desencadeados por emails enviados em massa por spammers[16], que enviam uma massa de mensagens eletrônicas, em poucos minutos, a destinatários potenciais dos sistemas informáticos que serão posteriormente alvos de suas condutas delitivas.

Utilizando de falhas no protocolo padrão de envio de emails (SMTP – Simple Mail Transfer Protocol), o phisher pode, inclusive, forjar o endereço destinatário da mensagem. Ao exemplo, pode colocar que o email foi enviado do endereço bancodobrasil@bb.com.br , utilizando de um cabeçalho adulterado.

Com isso, o cliente acredita que realmente está recebendo um email de seu banco, e, ao clicar no link disponibilizado na mensagem eletrônica, é direcionado ao site malicioso, o qual solicita suas informações pessoais, as armazena e envia ao agente malicioso.

Algumas técnicas são aplicadas para passar uma imagem de seriedade nas mensagens eletrônicas maliciosas, quais sejam[17]:

- Email com aparência oficial
- Cópia quase exata dos legítimos emails corporativos, com ínfimas diferenças

[16] "Spam is the use of electronic messaging systems (including most broadcast media, digital delivery systems) to send unsolicited bulk messages indiscriminately." in http://en.wikipedia.org/wiki/Spam_(electronic)

[17] http://www.technicalinfo.net/papers/Phishing.html

- Mensagem baseada em código HTML, de forma a ocultar a URL adulterada
- Malware padrão anexado ao email
- Email aparentemente pesonalizado ao cliente
- Falsificação do endereço do remetente do email, de forma a ocultar a sua real origem.

A repercussão penal em caso de phishing baseia-se na cominação à conduta do crime de estelionato. Pode ser, ainda, enquadrável como furto mediante fraude, caso haja o uso dos dados para transferência de valores pecuniários.

Caso a vantagem auferida seja outra que não pecuniária (tal como a transferência de milhas aéreas, ou a utilização de dados para lavagem de dinheiro), tratar-se-á de estelionato.

Seguem abaixo os tipos penais:

> **Estelionato**
>
> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
>
> Pena - reclusão, de um a cinco anos, e multa.
>
> § 1º - Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no art. 155, § 2º.

> **Furto**
>
> Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:
>
> Pena - reclusão, de um a quatro anos, e multa.

§ 1º - A pena aumenta-se de um terço, se o crime é praticado durante o repouso noturno.

§ 2º - Se o criminoso é primário, e é de pequeno valor a coisa furtada, o juiz pode substituir a pena de reclusão pela de detenção, diminuí-la de um a dois terços, ou aplicar somente a pena de multa.

§ 3º - Equipara-se à coisa móvel a energia elétrica ou qualquer outra que tenha valor econômico.

Furto qualificado

§ 4º - A pena é de reclusão de dois a oito anos, e multa, se o crime é cometido:

I - com destruição ou rompimento de obstáculo à subtração da coisa;

II - com abuso de confiança, ou mediante fraude, escalada ou destreza;

III - com emprego de chave falsa;

IV - mediante concurso de duas ou mais pessoas.

Há uma atual divergência no entendimento do Superior Tribunal de Justiça a respeito da tipificação da conduta de utilização indevida e não autorizada de dados bancários ou de cartão de crédito pelo agente fraudador, se seria estelionato ou furto mediante fraude.

O Superior Tribunal de Justiça já se posicionou em duas formas distintas, mas em situações fáticas um tanto diferentes:

> CONFLITO DE ATRIBUIÇÕES. MPF E JUIZ FEDERAL. IPL. **MOVIMENTAÇÃO E SAQUES FRAUDULENTOS EM CONTA-CORRENTE DA CEF POR MEIO DA INTERNET. MANIFESTAÇÃO DO MPF PELA DEFINIÇÃO DA CONDUTA COMO FURTO MEDIANTE FRAUDE** E DECLINAÇÃO DA COMPETÊNCIA PARA O LOCAL ONDE MANTIDA A CONTA-CORRENTE. INTERPRETAÇÃO DIVERSA DO JUÍZO FEDERAL, QUE ENTENDE TRATAR-SE DE ESTELIONATO. INEXISTÊNCIA DE CONFLITO DE ATRIBUIÇÕES. ARQUIVAMENTO INDIRETO. APLICAÇÃO ANALÓGICA DO ART. 28 DO CPP. PRECEDENTES DA 3A. SEÇÃO DESTA CORTE. PARECER DO MPF PELO

NÃO CONHECIMENTO DO CONFLITO. CONFLITO DE ATRIBUIÇÃO NÃO CONHECIDO.

1. **A 3a. Seção desta Corte definiu que configura o crime de furto qualificado pela fraude a subtração de valores de conta corrente, mediante transferência ou saque bancários sem o consentimento do correntista;** assim, a competência deve ser definida pelo lugar da agência em que mantida a conta lesada.

(...)

4. Conflito de atribuição não conhecido.

(CAt .222/MG, Rel. Ministro NAPOLEÃO NUNES MAIA FILHO, TERCEIRA SEÇÃO, julgado em 11/05/2011, DJe 16/05/2011)

CONFLITO NEGATIVO DE COMPETÊNCIA. PENAL. INQUÉRITO. **OPERAÇÕES DE CRÉDITO REALIZADAS EM LOJAS VIRTUAIS MEDIANTE A UTILIZAÇÃO DE CARTÕES MAGNÉTICOS E CPF DE TERCEIROS. ESTELIONATO**. CONSUMAÇÃO. COMARCAS DIVERSAS. COMPETÊNCIA FIRMADA PELA PREVENÇÃO.

1. **Indiciado que realizava compras em estabelecimentos virtuais utilizando-se de dados de cartão de crédito e CPF de terceiros. Valendo-se deste ardil, induzia as empresas lesadas a entregar – gize-se – voluntariamente e com o seu consentimento, as mercadorias objeto do crime.**

2. Não sendo possível definir, até o presente momento, o local exato da infração, mormente a indicação de que várias foram as vítimas e empresas lesadas, mostra-se aplicável, portanto, o disposto no art.

(...)

3. Conflito conhecido para determinar competente o suscitado, Juízo de Direito da 1ª Vara Criminal de João Pessoa – PB.

(CC 95.343/SP, Rel. Ministro OG FERNANDES, TERCEIRA SEÇÃO, julgado em 25/03/2009, DJe 24/04/2009)

No primeiro julgado, analisou-se a conduta de movimentação e saques indevidos pela internet. Dessa forma, houve a manipulação indevida de valores pecuniários, e o Superior Tribunal de Justiça entendeu que houve furto mediante fraude.

No segundo julgado, a conduta foi de efetuar compras em sites da internet utilizando-se de dados de cartão de crédito de terceiro, ao qual se cominou as penas do crime de estelionato.

Gize-se que a diferença entre furto mediante fraude e estelionato, na visão do STJ, consiste na conduta da vítima.

O furto mediante fraude não se confunde com o estelionato. A distinção se faz primordialmente com a análise do elemento comum da fraude que, no furto, é utilizada pelo agente com o fim de burlar a vigilância da vítima que, desatenta, tem seu bem subtraído, sem que se aperceba; no estelionato, a fraude é usada como meio de obter o consentimento da vítima que, iludida, entrega voluntariamente o bem ao agente.[18]

Dessa forma, entendemos que, em ambos os casos, tanto no saque e transferência de valores quanto na compra de produtos via internet com dados de terceiros, há o furto mediante fraude.

Em ambos os casos, a vítima que teve o seu patrimônio diminuído, no caso o correntista, não entregou os valores ao agente malicioso. O agente malicioso apenas aproveitou-se do excesso de confiança da vítima ao utilizar o site phisher, fornecendo os seus dados bancários (frise-se, e não os valores em si).

Dessa forma, entendemos que, nesses casos, ocorre o crime de furto mediante fraude, mas é importante que os profissionais da área de tecnologia e operadores do Direito não descartem a hipótese de estelionato, haja vista a divergência jurisprudencial existente quanto ao enquadramento da conduta.

[18] STJ - CC nº 67.343/GO – Relatora Ministra Laurita Vaz

Medidas a adotar em caso de crime digital

Por se tratar de espécie de crime nova, onde não há um entendimento consolidado a respeito da tipicidade, do enquadramento, do método probatório, e das medidas necessárias à conservação das provas obtidas, é necessário que o profissional de tecnologia de informação, a autoridade policial e os demais operadores do Direito empreguem o maior zelo possível quanto à preservação dos indícios.

Inicialmente, o administrador de sistema ou de redes, ou qualquer profissional de tecnologia de informação pode apresentar delação à autoridade policial quando constatar a ocorrência de crime digital.

Deve apresentar a notitia criminis (notícia do crime), que é o conhecimento pela autoridade, espontâneo ou provocado, de um fato aparentemente criminoso. No caso, o será na espécie de delação provocada, que é quando qualquer do povo, nos crimes de ação pública incondicionada, noticiar o fato delituoso à autoridade policial, dando ensejo à instauração de inquérito[19].

É o que faculta o Código de Processo Penal:

> Art. 5º - Nos crimes de ação pública o inquérito policial será iniciado:
>
> (...)
>
> § 3º - Qualquer pessoa do povo que tiver conhecimento da existência de infração penal em que caiba ação pública poderá, verbalmente ou por escrito, comunicá-la à autoridade policial, e esta, verificada a procedência das informações, mandará instaurar inquérito.

O delator, com base nesse dispositivo, poderá elaborar um documento simples contendo seu nome e dados pessoais, especificando as provas que possui que comprovem o cometimento dos crimes digitais, e, caso identifique, indícios de quem cometeu tal conduta.

Após, pode protocolar em delegacia de polícia, endereçado à autoridade policial, no caso, o Delegado de Polícia Civil. Poderá, ainda, dirigir a notícia do crime ao membro do

[19] TÁVORA, Nestor. **Curso de Direito Processual Penal**. Bahia: Ed. JusPODIVM, 2008. p. 90

Ministério Público, qual seja, o Promotor de Justiça, membro do Ministério Público estadual, ou, caso resulte, do crime digital, lesão ao patrimônio da União, ao Procurador da República, lotado na Procuradoria da República no estado.

O Código de Processo Penal determina a série de procedimentos a serem realizados pela autoridade policial (o Delegado de Polícia), ao se ter notícia do cometimento de um crime:

> Art. 6º Logo que tiver conhecimento da prática da infração penal, a autoridade policial deverá:
>
> I - dirigir-se ao local, providenciando para que **não se alterem o estado e conservação das coisas, até a chegada dos peritos criminais**;
>
> II - apreender os **objetos que tiverem relação com o fato**, após liberados pelos peritos criminais;
>
> III - **colher todas as provas que servirem para o esclarecimento do fato e suas circunstâncias;**
>
> IV - ouvir o ofendido;
>
> V - ouvir o indiciado, com observância, no que for aplicável, do disposto no Capítulo III do Título Vll, deste Livro, devendo o respectivo termo ser assinado por duas testemunhas que Ihe tenham ouvido a leitura;
>
> VI - proceder a reconhecimento de pessoas e coisas e a acareações;
>
> VII - determinar, se for caso, que se proceda a exame de corpo de delito e a quaisquer outras perícias;
>
> VIII - ordenar a identificação do indiciado pelo processo datiloscópico, se possível, e fazer juntar aos autos sua folha de antecedentes;
>
> IX - averiguar a vida pregressa do indiciado, sob o ponto de vista individual, familiar e social, sua condição econômica, sua atitude e estado de ânimo antes e depois do crime e durante ele, e quaisquer outros elementos que contribuírem para a apreciação do seu temperamento e caráter.

No caso da ocorrência de um crime digital, os cuidados para preservar o estado e conservação da coisa são, ainda, mais importantes.

Em caso de utilização de malware, phishing, DOS attack, vários dados podem ser perdidos com o simples desligamento do aparelho que o agente malicioso utilizou para o propósito delitivo.

Dessa forma, **recomendamos enfaticamente que não se desligue qualquer aparelho que tenha relação com o crime perpetrado**, tendo em vista que informações importantíssimas podem ser perdidas nesse ínterim.

A maioria dos aparelhos informáticos atuais se utilizam de Memória RAM, a qual pode conter informações essenciais para o deslinde da conduta delituosa, trazendo importantes relevâncias penais. Por se tratar de uma memória volátil, a qual é apagada quando a alimentação elétrica da memória é perdida.

Ademais, há máquinas que exigem senhas no boot, antes de o sistema operacional entrar em funcionamento, e, portanto, caso desliguem a máquina, pode ser necessária uma senha para acesso dos dados encriptados, dificultando ainda mais a atividade instrutória policial, ou sequer sendo possível o posterior acesso, já que a encriptação da referida senha pode ser complexa[20].

O profissional de tecnologia de informação e a autoridade policial devem preservar, portanto, as máquinas ligadas até a chegada do perito.

Não devem, ainda, deixar que o ofendido adultere os dados contidos nos aparelhos por qualquer forma, seja pela modificação do conteúdo pela manipulação da própria máquina, seja pela destruição física do aparelho, a qual pode se dar, inclusive, pela indução magnética (emprego de ímãs próximo ao aparelho), por impactos violentos ou desligamento da fonte de energia.

Os arquivos digitais referentes ao relatório de acesso ao aparelho ou rede invadidos também possui valor probatório relevante. São os chamados *logs de acesso*, aos quais o administrador de sistema deve fornecer à autoridade policial.

Recomenda-se, ainda, a identificação do endereço IP local, em intranet, caso a invasão se dê por usuário da própria rede interna, e identificar a sua vinculação ao usuário.

---

[20] Caso ocorrido na Operação Satiagraha, onde se investigou os discos rígidos encriptados do banqueiro Daniel Dantas. Vide matéria "Nem FBI consegue decifrar arquivos de Daniel Dantas, diz jornal. HDs foram apreendidos pela PF durante a Operação Satiagraha, em 2008. Informações estão protegidas por sofisticado sistema de criptografia." em http://g1.globo.com/politica/noticia/2010/06/nem-fbi-consegue-decifrar-arquivos-de-daniel-dantas-diz-jornal.html .

Pode-se, ainda, identificar o aparelho que foi utilizado como instrumento do crime por meio da identificação, caso o log de acesso forneça essa informação de seu endereço MAC. Cada aparelho possui o seu endereço MAC (Media Access Control) individual, e isso pode auxiliar nas investigações criminais, em que pese esse endereço possa ser adulterado por software.

Quanto à autoridade policial, caso tenha identificado o endereço IP em rede pública, é possível solicitar informações aos provedores de acesso que garantiram acesso ao agente malicioso através do referido endereço.

São essas, em síntese, as medidas que recomendamos em face da constatação de um crime digital.

Conclusão

Questiona-se, com a tramitação do Projeto de Lei nº 84, de 1999, cujo autor é o Deputado Luiz Piauhylino, se é necessário uma legislação específica para os crimes informáticos para a coibição de tais condutas. Vejamos o teor deste projeto no que tange aos crimes digitais:

> **DOS CRIMES DE INFORMÁTICA**
>
> Seção I
>
> **Dano a dado ou programa de computador**
>
> Art. 8º - Apagar, destruir, modificar ou de qualquer forma inutilizar, total ou parcialmente, dado ou programa de computador, de forma indevida ou não autorizada.
>
> Pena: detenção, de um a três anos e multa.
>
> Parágrafo único. Se o crime é cometido:
>
> I - contra o interesse da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;
>
> II- com considerável prejuízo para a vítima;

III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV - com abuso de confiança;

V - por motivo fútil;

VI - com o uso indevido de senha ou processo de identificação de terceiro , ou

VII - com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de dois a quatro anos e multa.

Seção II

Acesso indevido ou não autorizado

Art. 9º Obter acesso, indevido ou não autorizado, a computador ou rede de computadores.

Pena: detenção, de seis meses a um ano e multa.

Parágrafo primeiro. Na mesma pena incorre quem. sem autorização ou indevidamente, obtém, mantém ou fornece a terceiro qualquer meio de identificação ou acesso a computador ou rede de computadores.

Parágrafo segundo. Se o crime é cometido:

I - com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II - com considerável prejuízo para a vítima;

III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV - com abuso de confiança;

V - por motivo fútil;

VI - com o uso indevido de senha ou processo de identificação de terceiro; ou

VII - com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de um a dois anos e multa.

Seção III

Alteração de senha ou mecanismo de acesso a programa de computador ou dados

Art. 10. Apagar, destruir, alterar, ou de qualquer fama inutilizar, senha ou qualquer outro mecanismo de acesso a computador, programa de computador ou dados, de forma indevida ou não autorizada.

Pena: detenção, de um a dois anos e multa.

Seção IV

Obtenção indevida ou não autorizada de dado ou instrução de computador

Art. 11. Obter, manter ou fornecer, sem autorização ou indevidamente, dado ou instrução de computador.

Pena: detenção, de três meses a um ano e multa.

Parágrafo Único. Se o crime é cometido:

I - com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II - com considerável prejuízo para a vítima;

Parágrafo Único. Se o crime é cometido:

I - com acesso a computador ou rede de computadores da União, Estado, Distrito Federal, Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II - com considerável prejuízo para a vítima;

III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV - com abuso de confiança;

V - por motivo fútil;

VI - com o uso indevido de senha ou processo de identificação de terceiro; ou

VII - com a utilização de qualquer outro meio fraudulento.

Pena: detenção, de um a dois anos e multa.

Seção V

Violação de segredo armazenado em computador, meio magnético, de natureza magnética, óptica ou similar

Art. 12. Obter segredos, de indústria ou comércio, ou informações pessoais armazenadas em computador, rede de computadores, meio eletrônico de natureza magnética, óptica ou similar, de forma indevida ou não autorizada.

Pena: detenção, de um a três anos e multa.

Seção VI

Criação, desenvolvimento ou inserção em computador de dados ou programa de computador nocivos

Art. 13. Criar, desenvolver ou inserir, dado ou programa em computador ou rede de computadores, de forma indevida ou não autorizada com a finalidade de apagar, destruir, inutilizar ou modificar dado ou programa de computador ou de qualquer forma dificultar ou impossibilitar, total ou parcialmente, a utilização de computador ou rede de computadores.

Pena: reclusão, de um a quatro anos e multa.

Parágrafo único. Se o crime é cometido:

I - contra a interesse da União, Estado, Distrito Federal. Município, órgão ou entidade da administração direta ou indireta ou de empresa concessionária de serviços públicos;

II - com considerável prejuízo para a vítima;

III - com intuito de lucro ou vantagem de qualquer espécie, própria ou de terceiro;

IV - com abuso de confiança;

V - por motivo fútil;

VI - com o uso indevid6 de senha ou processo de Identificação de terceiro; ou

VII - com a utilização de qualquer outro meto fraudulento.

Pena: reclusão, de dois a seis anos e multa.

Seção VII

Veiculação de pornografia através de rede de computadores

Art. 14. Oferecer serviço ou informação de caráter pornográfico, em rede de computadores, sem exibir, previamente, de forma facilmente visível e destacada, aviso sobre sua natureza, indicando o seu conteúdo e a inadequação para criança ou adolescentes.

Pena: detenção, de um a três anos e multa.

A despeito da adequação ou não de tais tipos penais, é inegável que os dispositivos penais em vigência são suficientes a uma retribuição penal eficaz, se bem utilizada e entendida, pelo Estado aos agentes criminosos.

É louvável a intenção do Projeto de Lei nº 84, de 1999, de trazer à seara da discussão política e popular a repercussão penal de crimes digitais. Nesse sentido, compartilhamos com a visão do prof. Alexandre Atheniense:

> A insegurança jurídica que o cidadão brasileiro convive com as fraudes eletrônicas demanda que a tramitação do PL 84/99 prossiga após a realização nova audiência pública designada para o mês de julho, para votação em Plenário no mês de agosto e posterior sanção presencial.
>
> Até quando os estratosféricos prejuízos de 900 milhões de reais, originado pelas fraudes eletrônicas divulgados pela FEBRABAN e as humilhações destes atentados e pichações virtuais não serão suficientes para que possamos ter uma lei que possa punir estes ilícitos?[21]

[21] ATHENIENSE, Alexandre. A**s consequências jurídicas dos ataques de hackers aos sites do governo brasileiro**. Jus Navigandi, Teresina, ano 16, n. 2921, 1 jul. 2011. Disponível em: <http://jus.com.br/revista/texto/19451>. Acesso em: 7 set. 2011.

Porém, não é necessário que se aguarde a indefinição do Congresso Nacional para apurar e punir tais crimes digitais, com base nos tipos penais vigentes.

É necessário, mais do que a criminalização específica, o esclarecimento técnico aos operadores do Direito, à autoridade policial, aos administradores de sistemas informáticos, aos magistrados e membros do Ministério Público.

E é essa a missão que pretendemos estabelecer com a presente obra.

Nas próximas edições deste manual, pretendemos aprofundar em condutas cuja relevância penal são mais complexas, tais como os ataques por buffer overflow e abusos em serviços de autenticação.