PEDRO AUGUSTO ZANIOLO

CRIMES MODERNOS

O IMPACTO DA TECNOLOGIA NO DIREITO

8ª EDIÇÃO
Revista, ampliada
e atualizada

2026

EDITORA
JusPODIVM
www.editorajuspodivm.com.br

13

SEGURANÇA DIGITAL

13.1 INTRODUÇÃO

Diariamente, os meios de comunicação noticiam assaltos, trapaças, fraudes, corrupção, tráfico de entorpecentes, terrorismo, sequestros, ameaças, tornando nosso mundo um lugar cada vez mais perigoso e carente de segurança.

Sem dúvida, a educação, a saúde e a segurança são prioridades nacionais.

No meio digital não é diferente!

Todos os esforços de vigilância adotados para a segurança pública devem ser aplicados também à segurança digital, onde, infelizmente, não existe similaridade.

Dessa forma, não compete somente ao Poder Público, mas a todos os usuários tornar a Internet mais segura e confiável.

Portanto, a responsabilidade de tornar a Internet mais segura e confiável não recai exclusivamente sobre o Poder Público, mas sim em cada usuário.

Inúmeros aplicativos e sítios solicitam aos usuários que insiram dados pessoais no sistema, incluindo informações vitais para a privacidade e segurança.

Em alguns casos, a proteção desses dados é uma prioridade para o gestor, como nos aplicativos bancários, onde a credibilidade é essencial para a sobrevivência.

A disseminação de transações *on-line*, que envolvem dados cadastrais obtidos via Internet, cria a percepção equivocada de que todas são igualmente seguras, o que, infelizmente, não é verdade!

Essa percepção é alimentada pela semelhança nos métodos utilizados, fazendo com que os usuários acreditem na confidencialidade das informações e compartilhem detalhes de suas vidas privadas, interesses econômicos e sociais, assim como comportamentos pessoais e familiares.

Situação semelhante, por vezes mais intensa, ocorre nas redes sociais, mesmo que os aspectos econômico-financeiros sejam menos proeminentes: há uma exposição significativa da vida privada, muitas vezes com a crença errônea de que os dados estão seguros nesses ambientes.

A máxima "todo cuidado é pouco" nunca foi tão atual.

No entanto, não é necessário adotar uma abordagem radical. Assim como a pandemia do Coronavírus nos ensinou durante os meses de isolamento social, podemos conviver harmoniosamente com o mundo virtual, desde que as condutas, principalmente na Internet, sejam mais cautelosas. Como a clássica lição de F. T. Grampp e R. H. Morris ensina: "É fácil ter um sistema de computação seguro. Basta desconectar o sistema de qualquer rede externa, permitindo apenas terminais conectados diretamente a ele, colocar a máquina e seus terminais em uma sala fechada, e ter um guarda na porta"[1].

A segurança é um processo, não um produto[2].

A segurança tradicional de computadores e redes é definida por três propriedades desejáveis (Confidencialidade, Integridade e Disponibilidade), com o objetivo de mitigar ameaças e gerenciar os riscos enfrentados por redes ou sistemas específicos. Cada um desses "pilares" da informação é importante de diferentes maneiras[3]:

a) *Confidencialidade*: garante que informações sensíveis sejam mantidas privadas e acessadas apenas por indivíduos ou entidades autorizadas. Isso protege contra a divulgação não autorizada de dados sensíveis, o que pode resultar em perdas financeiras, danos à reputação ou responsabilidade legal;
b) *Integridade*: assegura que os dados sejam precisos, completos e não alterados. Isso é essencial para manter a confiança na informação e tomar decisões informadas[4]. Sem integridade de dados, as organiza-

---

1 SEGURANÇA. **Projeto OVNI – Oficina Virtual na Internet**. Disponível em: <http://www.gtrh.tche.br/ovni/seguranca/>. Acesso: em: 26 ago. 2020.

2 SCHNEIER, Bruce. **Click here to kill everybody**: security and survival in a hyper-connected world. New York: W. W. Norton & Company, 2018. p. 20.

3 WATTERS, Paul A. **Cybercrime and cybersecurity**. Boca Raton: CRC Press, 2024. p. 2.

4 Refere-se às decisões tomadas com base em informações completas, precisas e relevantes. Isso implica que o indivíduo tem acesso a todos os dados necessários e compreende as implicações e consequências de suas escolhas antes de tomar uma decisão.

ções podem enfrentar riscos significativos, como perdas financeiras, interrupções operacionais e responsabilidades legais; e

c) *Disponibilidade*: garante que a informação seja acessível e utilizável quando necessário. Isso é fundamental para manter a continuidade dos negócios e garantir que sistemas e dados críticos estejam disponíveis durante emergências ou crises. Sem disponibilidade, as organizações podem enfrentar interrupções significativas em suas operações e perder acesso a dados e sistemas críticos.

Essa tríade é essencial para proteger dados sensíveis, manter a confiança na informação e garantir a continuidade dos negócios. Ao implementar medidas de segurança apropriadas que abordem *confidencialidade*, *integridade* e *disponibilidade*, as organizações podem reduzir seu risco de violações de dados, danos à reputação, perdas financeiras e responsabilidade legal.

13.2 TERMINOLOGIA

A pós-modernidade deu origem aos chamados *tecnobárbaros*, responsáveis por criar vírus e códigos maliciosos, invadindo sistemas em uma prática de criminalidade transnacional e universal[5].

Com o avanço tecnológico, surgem diversos termos para melhor compreensão desse universo digital específico.

Alguns dos principais são os seguintes[6]:

a) *Newbie*: iniciante ou calouro, alguém com conhecimentos limitados em informática e ávido por aprender;
b) *Luser*: derivado da união de *loser* (perdedor) e *user* (usuário), refere-se àquele que tem interesse em aprender, buscando apenas o mínimo necessário para operar o computador e concluir tarefas rapidamente;
c) *Lamer*: um tipo de usuário, geralmente iniciante (*newbie*) ou sem muito conhecimento *(luser)*, caracterizado por não compreender exatamente como as coisas funcionam, mas com habilidades suficientes para operar aplicativos no computador. O termo deriva de *lame*, que em português significa manco ou aleijado;
d) *Hacker*: originalmente utilizado para carpinteiros que faziam móveis com machados, popularizou-se nos anos 1960 como sinônimo de

[5] LEGISLAÇÃO para punir crimes da internet. **Revista Jurídica Consulex**, Brasília, n. 41, 31 maio 2000.

[6] ULBRICH, Henrique César; VALLE, James Della. **Universidade H4CK3R**. 6. ed. São Paulo: Digerati Books, 2009. p. 28-30.

programador e especialista em computadores. Atualmente, a tendência é associá-lo a criminosos digitais. Entretanto, a comunidade *hacker* tradicional repudia essa definição, utilizando o termo *crackers* para descrever aqueles que praticam atividades ilegais;

e) *Crackers*: *hackers* mal-intencionados ou sem ética, especializados em quebrar as proteções de *softwares* comerciais para possibilitar a pirataria, além de usar seus conhecimentos para invadir sítios e computadores com propósitos ilícitos;

f) *Phreaker*: um tipo de *cracker* especializado em sistemas telefônicos, que realiza chamadas sem pagar, transfere faturas para outros números telefônicos (válidos ou não) e modifica telefones públicos para obter crédito ilimitado;

g) *Carder*: especialista em fraudes envolvendo cartões de crédito; e

h) *War driver*: um tipo de *cracker* que explora as vulnerabilidades de redes sem fio (*wireless*). Os *war drivers* europeus criaram o chamado *war chalking*, que consiste em desenhar símbolos no chão com giz para indicar a melhor posição de conexão sem fio para outros *war drivers*.

13.3 INVASÃO DE SISTEMAS

Basicamente, existem três categorias principais de ataques[7]:

a) *Criminosos*: os mais evidentes;

b) *Publicitários*; e

c) *Legais*: possivelmente os mais prejudiciais.

13.3.1 Ataques Criminosos

Os *ataques criminosos* abrangem fraudes de diversas naturezas.

Exemplos: fraudes relacionadas a cartões de crédito e redes de caixas eletrônicos; ataques destrutivos; furto de propriedade intelectual, como versões eletrônicas de livros, jornais, vídeos, música, imagens estáticas, *softwares* e bancos de dados privados; furto de marcas e invasões de privacidade, entre outras possibilidades.

[7] SCHNEIER, Bruce. **Segurança.com**: segredos e mentiras sobre a proteção na vida digital. Rio de Janeiro: Campus, 2001. p. 35-52.

13.3.2 Ataques por Publicidade

Esses ataques objetivam a obtenção de publicidade por meio de atos ilícitos.

Exemplos clássicos: o atraso no lançamento de um produto da *Sony* devido a uma falha de segurança do DVD e a perda significativa de clientes da CD *Universe* em 2000, após o furto de 300.000 números de cartões de crédito de seu sítio na *web*.

Às vezes, a má publicidade pode resultar em custos muito maiores do que o próprio prejuízo financeiro.

A deformação, desfiguração ou alteração de conteúdo de uma página ou sítio *web* (*defacement* ou simplesmente *deface*) também se enquadra nesse tipo de ataque.

Alguns autores denominam essa conduta como *pichação eletrônica* ou *digital*, pois, após o ataque, são inseridas imagens "bobas" nos sítios desfigurados.

Como exemplo dessa ação, citem-se as desfigurações realizadas nos sítios da *Microsoft* Brasil, *Disney* e do Banco do Brasil, entre muitas outras.

13.3.3 Ataques que utilizam o Sistema Legal

Os ataques que se valem do sistema legal são os mais desafiadores de se proteger.

Eles não buscam explorar falhas de um sistema, mas sim persuadir Juízes de que poderia haver uma falha no sistema, colocando em dúvida a segurança perfeita do sistema perante o Poder Judiciário, a fim de provar a inocência de um cliente.

13.4 PROBLEMAS DE SEGURANÇA

13.4.1 Vírus e *Malwares*

13.4.1.1 Vírus

O vírus de computador é um *software* malicioso que se instala em um sistema específico, infectando-o:

> Vírus são programas que se comportam como seus homônimos biológicos: são microscópios, reproduzem-se sozinhos, consomem recursos computacionais que não lhes pertencem e têm alta capacidade de infecção por contágio. [...]

> Um vírus de computador possui objetivos muito claros: infectar o máximo possível de sistemas, reproduzir-se rapidamente e opcionalmente consumir recursos e danificar os sistemas invadidos[8].

Geralmente, possui capacidade destrutiva, replicando-se facilmente para outros dispositivos.

Pode associar-se a *softwares* ilegais baixados da Internet e instalados em um computador. O vírus vai de carona!

Foi dessa forma que, em 1986, surgiu o primeiro vírus de computador: o *Brain* (*cérebro*, em inglês).

Dois irmãos, frustrados com as práticas ilícitas de clientes que copiavam *softwares* de sua loja, admitiram ter desenvolvido o vírus para infectar o setor de inicialização dos disquetes: quando os discos eram copiados, o vírus era disseminado[9].

A partir desse evento, diversos tipos de vírus surgiram.

Podem ser classificados de acordo com sua ação da seguinte forma[10]:

a) *Inofensivos*: não causam perturbação alguma ao sistema;
b) *Humorísticos*: não objetivam causar danos, apenas apresentam mensagens ou imagens gráficas humorísticas na tela;
c) *Alteradores*: modificam dados em arquivos, como planilhas, banco de dados e documentos, por exemplo, substituindo todas as ocorrências do algarismo 6 por 8. Este tipo de vírus é potencialmente o mais destrutivo, pois suas alterações podem ser difíceis de detectar e seus efeitos podem ser desastrosos;
d) *Catastróficos*: ativam-se de forma repentina, causando danos globais e imediatos. Apagam arquivos, corrompem registros, destroem ou inutilizam informações no disco rígido e em outros dispositivos conectados ao sistema; e
e) *Genéricos*: são os mais contagiosos. Parecem invisíveis, escondendo-se nos programas e, geralmente, não interferem no processo normal de execução dos *softwares*. Em determinado momento, respondendo a

---

8 ULBRICH, Henrique César; VALLE, James Della. **Universidade H4CK3R**. 6. ed. São Paulo: Digerati Books, 2009. p. 319.

9 VÍRUS de computador: conheça 8 tipos e como combatê-los. **Kaspersky**. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/computer-viruses-and-malware-facts-and-faqs>. Acesso em: 21 nov. 2024

10 REIS, Maria Helena Junqueira Reis. **Computer crimes**. Belo Horizonte: Del Rey, 1997. p. 34-35.

um sinal esperado, são ativados e começam a agir, modificando ou destruindo arquivos.

Existem diversos tipos de vírus, sendo os mais comuns aqueles disseminados por mensagens de correio eletrônico (*e-mail*), os vírus de *script* (que executam funções específicas conforme a programação realizada no *script*), os vírus de *smartphone* e os vírus de macro[11].

Os *vírus de macro* tinham como alvo os arquivos do *Microsoft Office*: documentos do *Word* (com extensões DOC e DOCX), *Excel* (XLS e XLSX), *Power Point* (PPT e PPTX) e *Access* (MDB e MDBX). Esses vírus se aproveitavam da facilidade de programação das *macros*, pequenos programas utilizados para automatizar funções em um aplicativo, para contaminar arquivos de dados. Geralmente, além de desorganizar textos ou planilhas, realizavam travessuras, como modificar a disposição dos menus ou desabilitar opções nos programas[12].

Ao longo da história, diversos vírus tornaram-se conhecidos devido à extensão de seus danos ou à originalidade com que se apresentaram, conseguindo enganar os programas de detecção (chamados de *polimórficos*). Alguns exemplos notáveis: *Melissa*, *Sexta-feira 13*, *Netsky*, *Stoned*, *Chernobyl*, *Michelangelo*, *Madonna*, *Ping-Pong*, *Klez*, *BugBear*, *Love Letter* (conhecido no Brasil como *I Love You*), *SirCam*, *Creeper*, *Sasser*, *Code Red*, *Storm*, *Slammer*, *Concept*, *Netsky*, *Mozart*, *Nimda*, *Conficker* e *MyDoom*.

Em 1987, surgiu um dos primeiros vírus devastadores para MS-DOS: o *Jerusalem*. Programado para apagar todos os arquivos de programas do disco rígido dos computadores infectados às sextas-feiras, dia 13, ficou conhecido como *Sexta-Feira 13* (*Friday 13th*)[13].

No ano de 2002, David Smith, criador do vírus *Melissa*, foi condenado a 20 meses de prisão e ao pagamento de uma multa de 5 mil dólares. Ele afirmou que sua criação *foi um erro colossal*[14].

O *MyDoom*, descoberto no início de 2004, infectou mais de um milhão de computadores em todo o mundo em apenas alguns dias, sendo o Brasil

---

11 CARTILHA de segurança para internet. **Comitê Gestor da Internet no Brasil**, jun. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 29 jul. 2020. p. 24.

12 TORRES, Gabriel. Vírus do Word. **Clube do Hardware**, 15 ago. 1997. Disponível em: <http://www.clubedohardware.com.br/artigos/314>. Acesso em: 13 ago. 2020.

13 GUILHERME, Paulo. Os 7 mais famosos vírus de computador da história. **Tecmundo**, 5 jul. 2013. Disponível em: <https://www.tecmundo.com.br/virus/41664-os-7-mais-famosos-virus-de-computador-da-historia.htm>. Acesso em: 13 ago. 2020.

14 CRIADOR de vírus é condenado a 20 meses de prisão. **BBC Brasil**, 2 maio 2002. Disponível em: <https://www.bbc.com/portuguese/ciencia/020502_virusmtc.shtml>. Acesso em: 13 ago. 2020.

um dos países mais afetados. Nesse período, o provedor brasileiro *Terra* relatou bloquear em média 8 mil mensagens por minuto infectadas com o vírus *MyDoom* e suas variantes.

Atualmente, contudo, não se fala mais *somente* nos vírus.

Evoluíram.

Outras variantes surgiram.

Agora são considerados espécies do gênero *malware*.

O termo *malware* ou *código malicioso* é utilizado de maneira ampla para descrever diferentes tipos de *software* que têm como objetivo realizar ações prejudiciais nos computadores, incluindo a coleta de informações pessoais, como senhas dos usuários.

Exemplos: vírus, *spyware*, *ransomware*, cavalos de Troia (*trojans*) e *worms*.

Esses *malwares* podem comprometer sistemas e redes de computadores por intermédio de várias condutas, tais como[15]:

a) Exploração de vulnerabilidades presentes nos programas instalados;
b) Execução automática de mídias removíveis, como *pen drives* e unidades de disco rígido externas, que estejam infectadas;
c) Acesso a páginas *web* com conteúdo malicioso, aproveitando-se de vulnerabilidades nos navegadores;
d) Atuação direta de agentes que, após realizarem a invasão de computadores ou redes, disseminam arquivos contagiados com códigos maliciosos; e
e) Execução de arquivos previamente infectados, obtidos por meio de anexos de mensagens eletrônicas (*e-mail*), mídias removíveis, páginas *web* ou compartilhamento de recursos entre computadores.

Uma vez instalados em computadores ou sistemas, os códigos maliciosos ganham acesso aos dados armazenados e podem executar ações em nome dos usuários, de acordo com as permissões concedidas a cada usuário. As principais motivações por trás do desenvolvimento e propagação de códigos maliciosos são[16]:

a) Busca por vantagens financeiras (principalmente);

---

15 CARTILHA de segurança para internet. **Comitê Gestor da Internet no Brasil**, jun. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 29 jul. 2020. p. 23.

16 CARTILHA de segurança para internet. **Comitê Gestor da Internet no Brasil**, jun. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 29 jul. 2020. p. 23.

b) Coleta de informações confidenciais;
c) Desejo de autopromoção; e
d) Motivações de vandalismo.

As ameaças de códigos maliciosos em evolução incluem código criptográfico[17], criptovírus[18] e *rootkits* baseados em *hardware*. Essas ameaças nem sempre se encaixam em categorias claramente definidas, o que pode causar certa confusão nas discussões sobre o tema, já que não é possível rotular todos os códigos como bons ou maliciosos. Sem a *mens rea* (intenção criminosa do autor ou usuário), o código não pode ser categorizado como bom ou ruim. Os autores desenvolvem códigos para atingir objetivos específicos, assim como os usuários executam esses códigos com determinados propósitos. Portanto, o contexto de uso e a intenção do agente determinam se o código é malicioso[19].

Passa-se, então, à análise dos tipos mais comuns de *malware*.

13.4.1.2 *Spyware*

Spyware é uma categoria de programa de computador especialmente desenvolvida para monitorar as atividades de um sistema, coletar essas informações e enviá-las a terceiros[20].

O uso de *spyware* pode ocorrer de maneira legítima ou fraudulenta, envolvendo ações que violam a privacidade dos usuários.

Existem vários tipos[21] de *spyware*:

a) *Keylogger*: é capaz de capturar e armazenar as *teclas digitadas* pelo usuário no teclado do computador. Geralmente, ativa-se por meio de determinadas ações dos usuários, como o acesso a determinados sítios de comércio eletrônico ou instituições bancárias;
b) *Screenlogger*: similar ao *keylogger*, o *screenlogger* é capaz de armazenar a posição do cursor e a tela apresentada no monitor durante os cliques

---

17 Tipo de ataque que utiliza criptografia assimétrica para implementar um ***backdoor*** criptográfico.

18 Os ***criptovírus*** utilizam criptografia para codificar dados, tornando-os inacessíveis para o usuário. Deixam uma mensagem solicitando resgate para restabelecimento ao acesso dos arquivos criptografados. Exemplo: ***ransomware*** (vide item 13.4.1.3).

19 GUESS, Robert; SALVEGGIO, Eric. Malicious code. In: BOSWORTH, Seymour; KABAY, M.E.; WHYNE, Eric. **Computer security handbook**. 6. ed. Hoboken: Wiley, 2014. v. 1, p. 16-2.

20 CARTILHA de segurança para internet. **Comitê Gestor da Internet no Brasil**, jun. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 29 jul. 2020. p. 27.

21 CARTILHA de segurança para internet. **Comitê Gestor da Internet no Brasil**, jun. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 29 jul. 2020. p. 27.

do *mouse* ou na região circundante. É frequentemente utilizado por atacantes para capturar as *teclas digitadas pelos usuários em teclados virtuais*, como os disponíveis nos sítios de instituições bancárias; e

c) *Adware*: projetado especificamente para exibir publicidade, o *adware* pode ser utilizado para fins legítimos, como forma de patrocínio ou retorno financeiro aos desenvolvedores de softwares livres, ou prestação de serviços gratuitos. No entanto, há o *lado negro da força*: quando as propagandas apresentadas são direcionadas aos usuários com base em sua navegação, sem o conhecimento de que estão sendo monitorados nesse sentido.

13.4.1.3 *Ransomware*

Ransomware é um tipo de *software* malicioso que infecta computadores e exibe mensagens exigindo o pagamento de uma taxa (resgate) para que o sistema volte a funcionar. Esta classe de *malware* pode ser instalada por meio de *links* enganosos em *e-mails*, mensagens instantâneas ou sítios da *web*, sendo capaz de bloquear a tela do computador ou criptografar arquivos importantes com senha[22].

Em essência, trata-se de um *sequestro digital* de dados.

O *scareware*, que é uma variante mais simples de *ransomware*, se apresenta como um programa *antispyware* falso e inútil, enganando os usuários ao fazê-los acreditar que analisará e protegerá seus computadores.

Um exemplo emblemático desse tipo de ameaça foi o *WannaCry*, um *ransomware* que, em 2017, explorou vulnerabilidades de segurança, e afetou sistemas em todo o mundo. Ele bloqueava o acesso a arquivos importantes, como prontuários de hospitais. Semelhante a um sequestro digital, o *WannaCry* criptografava os documentos e exigia altos valores como "resgate" para restaurar o acesso.

Durante a pandemia de Coronavírus em 2020, a empresa norte-americana *Garmin*, especializada em produtos baseados em tecnologia GPS, foi vítima de *ransomware*, sendo exigido um pagamento de 10 milhões de dólares como *resgate*. Após vários dias fora do ar, conseguiram restabelecer os sistemas de informação utilizados por seus produtos.

---

[22] O QUE é ransomware? **Kaspersky**. Disponível em: <https://www.kaspersky.com.br/resource-center/definitions/what-is-ransomware>. Acesso em: 13 ago. 2020.

No início de novembro de 2020, o *Superior Tribunal de Justiça* (STJ) também foi alvo de *ransomware*, resultando em problemas nos sistemas de informação, suspensão de sessões de julgamento por videoconferência e a indisponibilidade do sítio *web*. Outros órgãos, como o Ministério da Saúde, Governo do Distrito Federal e o Tribunal de Justiça do Estado de Pernambuco, relataram incidentes semelhantes. Não há informações sobre uma possível relação entre esses eventos danosos[23].

Destaca-se o aumento desse tipo de ataque, não apenas no Brasil, mas em escala global. A título de exemplificação, mencionam-se os eventos ocorridos no final de 2021 e em 2022:

a) *2021*: Tribunal de Justiça do Estado do Rio Grande do Sul (TJRS), Supremo Tribunal Federal (STF) e Ministério da Saúde (plataforma do aplicativo *ConecteSUS*); e
b) *2022*: em 30.03, o alvo foi o TRF da 3ª Região, que abrange os Estados de São Paulo e Mato Grosso do Sul. O Tribunal informou que não houve perda de dados. Uma semana depois, uma nova investida atingiu a Justiça Federal em Pernambuco. Outro ataque, ocorrido em 21.04, resultou no vazamento de 420 GB da Secretaria de Estado de Fazenda do Rio de Janeiro. O TJDFT foi vitimado em 31 de julho, levando à retirada do ar do sítio do Tribunal como medida de precaução.

Em 2023, os pagamentos de resgate por *ransomware* ultrapassaram pela primeira vez a marca de US$ 1,1 bilhão, revertendo a queda observada em 2022. Isso destaca o ano como altamente lucrativo para grupos de *ransomware*, seguindo um recorde anterior em 2021. O ressurgimento desse tipo de ataque confirma que 2022 foi uma anomalia estatística, com eventos geopolíticos impactando a atividade daquele ano[24].

Os ataques de *ransomware* atingiram níveis recordes em 2024, apesar dos esforços das autoridades. Segundo a *Recorded Future*, houve um aumento de 30% nos ataques de subtração de dados e o número de grupos de *ransomware* ativos também cresceu 30%, com 31 novos grupos surgindo. Entre os incidentes, o ataque ao sistema da *Change Healthcare* expôs dados de 100

---

23 ALVES, Paulo. Ataque hacker ao STJ: seis coisas que você precisa saber sobre o caso. **Tech Tudo**, 7 nov. 2020. Disponível em: <https://www.techtudo.com.br/listas/2020/11/ataque-hacker-ao-stj-seis-coisas-que-voce-precisa-saber-sobre-o-caso.ghtml>. Acesso em: 7 nov. 2020.

24 TOULAS, Bill. Ransomware payments reached record $1.1 billion in 2023. **Bleeping Computer**, 7 fev. 2024. Disponível em: <https://www.bleepingcomputer.com/news/security/ransomware-payments-reached-record-11-billion-in-2023/>. Acesso em: 8 fev. 2024.

milhões de americanos. Operações internacionais, como a *Operação Cronos*, conseguiram desmantelar parte da infraestrutura de grupos de *ransomware*, resultando na apreensão de servidores e prisões de cibercriminosos.

Com o auxílio da inteligência artificial, os ataques se tornaram mais sofisticados e direcionados, afetando setores críticos como saúde, finanças e infraestrutura. Grupos como *LockBit*, *RansomHub* e *Play* foram responsáveis por um grande número de ataques, com o *LockBit* liderando a lista ao impactar 525 empresas. A tática de dupla extorsão, onde os criminosos não apenas criptografam os dados, mas também ameaçam divulgá-los, tornou-se comum[25].

13.4.1.4 *Worm*

Worms (vermes, em inglês) são semelhantes aos vírus, com a diferença de poderem realizar cópias de si mesmos ou de algumas de suas partes (apenas alguns têm essa capacidade)[26].

Ao contrário dos vírus, não necessitam de intervenção humana para se propagar e infectar: eles utilizam as redes de comunicação[27].

Uma característica de alguns *worms* é a capacidade de se autoenviar para os contatos do programa de *e-mail* das máquinas contaminadas. Por exemplo, os conhecidos *Melissa* e *I Love You* eram capazes de se autoenviar para os 50 primeiros contatos de seu Catálogo de Endereços.

13.4.1.5 Cavalo de Troia (*Trojan Horse*)

Cavalos de Troia (*trojans* ou *trojan horses*) são programas que podem se instalar no computador por diversos meios e, uma vez introduzidos, executam ações específicas com o objetivo de controlar o sistema. Geralmente, não possuem a capacidade de se autorreproduzir ou de infectar outros *softwares*[28].

---

25 SURTO de ransomware: mais de 1.000 vítimas impactadas em 2024. **Segurança Eletrônica**. Disponível em: <https://revistasegurancaeletronica.com.br/surto-de-ransomware-mais-de-1-000-vitimas-impactadas-em-2024/>. Acesso em: 24 nov. 2024.

26 ENTENDA o que são vírus, vermes e cavalos de Tróia. **Terra Networks Brasil S.A.**, 29 jan. 2009. Disponível em: <http://tecnologia.terra.com.br/hardware-e-software/entenda-o-que-sao-virus-vermes-e-cavalos-de-troia,f118887dc5aea310VgnCLD200000bbcceb0aRCRD.html>. Acesso em: 13 ago. 2020.

27 VÍRUS de computador: conheça 8 tipos e como combatê-los. Kaspersky. Disponível em: <https://www.kaspersky.com.br/resource-center/threats/computer-viruses-and-malware-facts-and-faqs>. Acesso em: 21 nov. 2024

28 ENTENDA o que são vírus, vermes e cavalos de Tróia. **Terra Networks Brasil S.A.**, 29 jan. 2009. Disponível em: <http://tecnologia.terra.com.br/hardware-e-software/entenda-o-que-sao-virus-vermes-e-cavalos-de-troia,f118887dc5aea310VgnCLD200000bbcceb0aRCRD.html>. Acesso em: 13 ago. 2020.

Curiosamente, o nome faz referência ao famoso episódio dos soldados gregos que se esconderam dentro de um enorme cavalo de madeira, oferecido como presente aos troianos durante a guerra entre os dois povos. Os gregos colocaram alguns soldados dentro do cavalo, simularam a retirada de suas tropas e os cidadãos de Troia levaram o cavalo para dentro da cidade como um símbolo dos deuses. Ao cair da noite, os soldados gregos saíram do cavalo e abriram os portões da cidade, permitindo que todo o exército grego entrasse, resultando na vitória na batalha[29].

13.4.1.6 *Backdoor*

Também conhecido como *porta dos fundos*, o *backdoor* é um tipo de programa que, ao ser instalado no computador, torna-o vulnerável a ataques e invasões, deixando uma porta aberta para potenciais ameaças[30].

O *backdoor* pode ser introduzido por ação de outros códigos maliciosos que tenham previamente infectado o computador, ou por agentes que explorem vulnerabilidades existentes nos programas instalados no sistema. Após a inclusão, ele é utilizado para assegurar acesso remoto futuro ao computador vulnerável, sem a necessidade de recorrer à metodologia de invasão e infecção, muitas vezes passando despercebido[31].

Programas de administração remota, como *BackOrifice*, *NetBus*, *Sub-Seven*, VNC e *Radmin*, se mal configurados ou utilizados sem o consentimento do usuário, podem ser categorizados como *backdoors*[32].

13.4.1.7 *Bot* e *Botnet*

Bot é um *software* que possibilita ao invasor controlar remotamente o computador infectado. Similar ao *worm*, ele se propaga sem a necessidade de intervenção humana, explorando vulnerabilidades existentes[33].

---

29 ENTENDA o que são vírus, vermes e cavalos de Tróia. **Terra Networks Brasil S.A.**, 29 jan. 2009. Disponível em: <http://tecnologia.terra.com.br/hardware-e-software/entenda-o-que-sao-virus-vermes-e-cavalos-de-troia,f118887dc5aea310VgnCLD200000bbcceb0aRCRD.html>. Acesso em: 13 ago. 2020.

30 WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos**: ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012. p. 37.

31 CARTILHA de segurança para internet. **Comitê Gestor da Internet no Brasil**, jun. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 29 jul. 2020. p. 28.

32 CARTILHA de segurança para internet. **Comitê Gestor da Internet no Brasil**, jun. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 29 jul. 2020. p. 28.

33 CARTILHA de segurança para internet. **Comitê Gestor da Internet no Brasil**, jun. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 29 jul. 2020. p. 26.

Um computador infectado por um *bot* é comumente chamado de *zumbi* (*zombie computer*), devido à capacidade de controle remoto total, sem o conhecimento do seu proprietário. Também pode ser referido como *spam zombie quando* o bot instalado transforma o computador em um servidor de *e-mails*, sendo utilizado para o envio disseminado de *spam*[34].

Uma *botnet* é uma rede de computadores *zumbis* que potencializa as ações danosas dos *bots*[35].

13.4.1.8 *Rootkit*

O termo *rootkit* origina-se da combinação das palavras *root* (usuário de computador que possui controle total da máquina) e *kit* (conjunto de programas utilizados por usuários do *Linux* para obter controle total sobre um sistema comprometido)[36].

Rootkits são uma das muitas ferramentas disponíveis aos *hackers* maliciosos disfarçarem o fato de que uma máquina foi comprometida *(rooted)*. Um *rootkit* não é usado para invadir um sistema, mas para garantir que o sistema invadido permaneça disponível ao invasor[37].

Eles são compostos por um conjunto de utilitários instalados na máquina da vítima. Esses utilitários começam modificando os programas mais básicos e amplamente utilizados, ocultando atividades suspeitas. Por exemplo, um *rootkit* frequentemente altera comandos simples como *ls* (listar arquivos). Um *ls* modificado por um *rootkit* não exibirá arquivos ou diretórios que o invasor deseja manter ocultos[38].

Os utilitários que compõe o *rootkit* podem ser utilizados para[39]:

a) Remover evidências em arquivos de *logs* (*log-wiping*), como o registro de acesso do invasor;

---

34 CARTILHA de segurança para internet. **Comitê Gestor da Internet no Brasil**, jun. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 29 jul. 2020. p. 26.

35 CARTILHA de segurança para internet. **Comitê Gestor da Internet no Brasil**, jun. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 29 jul. 2020. p. 26.

36 WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos**: ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2012. p. 32.

37 COBB, Chey et al Penetrating computer systems and networks. In: BOSWORTH, Seymour; KABAY, M.E.; WHYNE, Eric. **Computer security handbook**. 6. ed. Hoboken: Wiley, 2014. v. 1, p. 15-26.

38 COBB, Chey et al. Penetrating computer systems and networks. In: BOSWORTH, Seymour; KABAY, M.E.; WHYNE, Eric. **Computer security handbook**. 6. ed. Hoboken: Wiley, 2014. v. 1, p. 15-26.

39 CARTILHA de segurança para internet. **Comitê Gestor da Internet no Brasil**, jun. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 29 jul. 2020. p. 29.

b) Instalar outros códigos maliciosos, como *backdoors*[40], para assegurar acesso futuro ao computador vulnerável;
c) Ocultar atividades e informações: arquivos, pastas, processos, chaves de registro, conexões de rede etc.;
d) Mapear potenciais vulnerabilidades em outros computadores, por meio de varreduras na rede; e
e) Capturar informações da rede onde o computador comprometido está localizado, pela interceptação de tráfego (*sniffers*)[41].

Os *rootkits* são extremamente difíceis de serem descobertos, pois os comandos e programas parecem funcionar perfeitamente, como antes. Frequentemente, um *rootkit* é identificado porque algo não *parecia correto* para o administrador do sistema. Como os *rootkits* variam nos programas que alteram, não é possível determinar quais programas foram efetivamente alterados sem uma assinatura criptográfica segura de cada binário do sistema. Dessa forma, um administrador nunca pode ter certeza de ter encontrado o *rootkit* inteiro[42].

13.4.2 Boatos

No item 5.2.4, discutimos os boatos (*hoaxes*), que, em princípio, não representam preocupações significativas de segurança, limitando-se a ocupar espaço nas caixas de entrada de *e-mails*, *smartphones* (*WhatsApp*) ou dando origem ao *spam*.

No entanto, problemas mais sérios e potencialmente prejudiciais podem surgir quando boatos veiculam vírus e cavalos de Troia anexados às mensagens de *e-mail*, ou quando induzem usuários a fornecerem informações pessoais, como número de cartão de crédito e senha da conta bancária.

13.4.3 *Sniffers*

Sniffers são programas projetados para capturar e ler pacotes de informação que trafegam pela rede[43].

---

40 Vide item 13.4.1.6.

41 Vide item 13.4.3.

42 COBB, Chey et al. Penetrating computer systems and networks. In: BOSWORTH, Seymour; KABAY, M.E.; WHYNE, Eric. **Computer security handbook**. 6. ed. Hoboken: Wiley, 2014. v. 1, p. 15-26.

43 PANKO, Raymond; FISHER, Eric. Data communications and information security. In: BOSWORTH, Seymour; KABAY, M.E.; WHYNE, Eric. **Computer security handbook**. 6. ed. Hoboken: Wiley, 2014. v. 1, p. 5-23.

Embora o termo *sniffer* seja amplamente utilizado, é importante observar que se trata de uma marca registrada da *Network General Corporation*[44].

Para ilustrar, considere o controle de acesso de um determinado sistema de informações, onde o usuário fornece seu identificador (*login*) e a respectiva senha (*password*). Enquanto esses dados estão sendo autenticados remotamente, é nesse ponto que o *sniffer* atua, interceptando e armazenando essas informações para uso posterior, muitas vezes de forma fraudulenta.

Invasores utilizam esse artifício para obter acesso não autorizado a uma rede, *escutando* o tráfego por meio de *sniffers*. Deixando a ferramenta em "modo de espera" por alguns dias, é possível capturar senhas de dezenas de usuários e centenas de serviços, como sítios *web*, *e-mails*, servidores, sistemas, entre outros[45].

13.4.4 *Cookies*

Os *cookies* representam uma sofisticada técnica de programação embutida nos navegadores *web*. Embora desempenhem funções úteis e benéficas, seu uso inadequado pode resultar em práticas ilícitas[46].

Esses pequenos arquivos de texto são gerados automaticamente pelos sítios quando os usuários os acessam.

Identificam, portanto, informações dos usuários: histórico de navegação, *login* e senha.

Poderão ser utilizados em visitas subsequentes aos mesmos sítios.

Embora geralmente inofensivos, os *cookies* podem ser bloqueados por usuários que desaprovam a ideia de ter seus identificadores armazenados, bastando para isso alterar as configurações do navegador[47].

Além dos riscos de privacidade para os clientes, é importante ressaltar que as empresas que os utilizam também estão sujeitas a ameaças. Como os *cookies* estão sob o controle dos usuários finais, estes podem alterá-los conforme desejarem. Em cenários como o comércio eletrônico, onde os *cookies* são usados para transportar informações de pedidos, qualquer modificação

---

44 COBB, Chey et al. Penetrating computer systems and networks. In: BOSWORTH, Seymour; KABAY, M.E.; WHYNE, Eric. **Computer security handbook**. 6. ed. Hoboken: Wiley, 2014. v. 1, p. 15-11.

45 ULBRICH, Henrique César; VALLE, James Della. **Universidade H4CK3R**. 6. ed. São Paulo: Digerati Books, 2009. p. 270.

46 SCHNEIER, Bruce. **Segurança.com**: segredos e mentiras sobre a proteção na vida digital. Rio de Janeiro: Campus, 2001. p. 174-175.

47 KABAY, M. E.; TAKACS, Nicholas. Email and internet use policies. In: BOSWORTH, Seymour; KABAY, M.E.; WHYNE, Eric. **Computer security handbook**. 6. ed. Hoboken: Wiley, 2014. v. 1, p. 48-25.