

CYBERSECURITY

RISCOS, VULNERABILIDADES E AMEAÇAS

À SEGURANÇA DA INFORMAÇÃO E À CONTINUIDADE DO NEGÓCIO

OSMANY DANTAS RIBEIRO DE ARRUDA



3

LISTA DE FIGURAS

Figura 3.1 – Eventos de CyberSecurity vs. Incidentes de CyberSecurity.....	6
Figura 3.2 – Busca no Google pelo CVE do WannaCry.....	8
Figura 3.3 – Detalhes do CVE do WannaCry.....	8
Figura 3.4 – Detalhes do CVE-2017-0144.....	9
Figura 3.5 – Panorama das ameaças 2017.....	10
Figura 3.6 – Oito principais ataques às redes.....	11



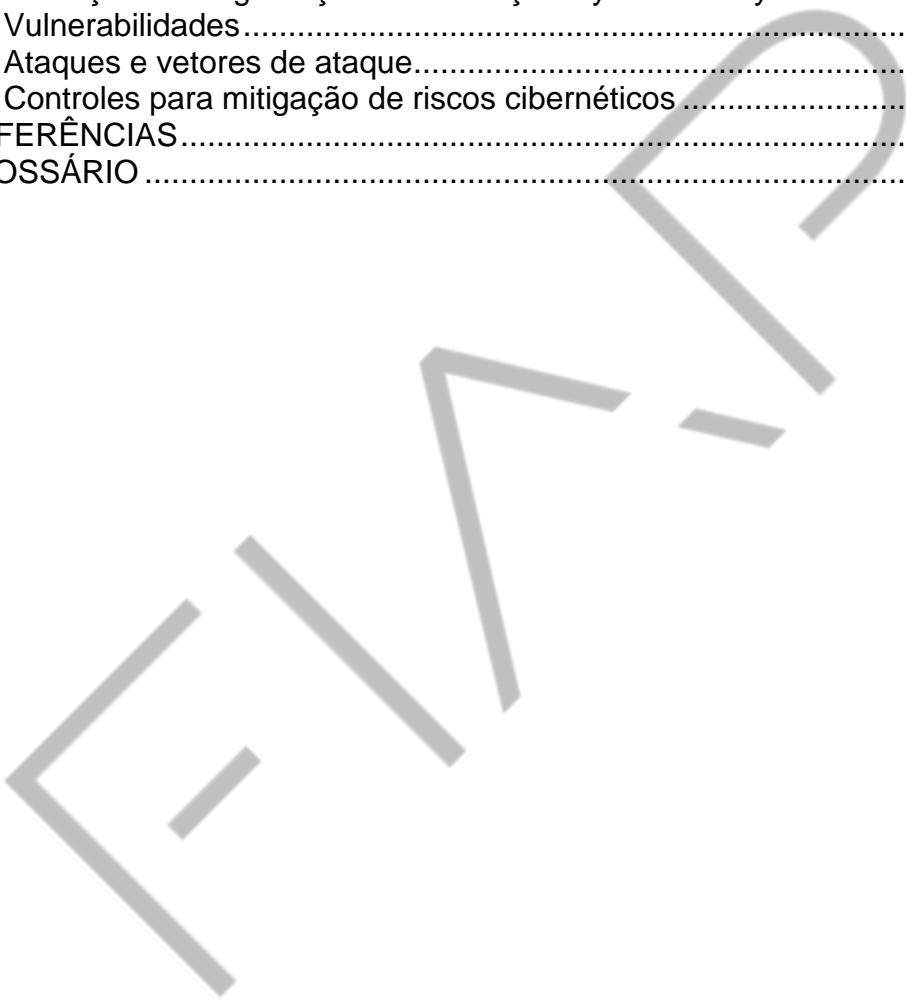
LISTA DE QUADROS

Quadro 3.1 – Cálculo do risco.....9



SUMÁRIO

3 RISCOS, VULNERABILIDADES E AMEAÇAS À SEGURANÇA DA INFORMAÇÃO E À CONTINUIDADE DE NEGÓCIO	5
3.1 Onde tudo se inicia.....	5
3.2 Eventos e incidentes de segurança (da informação/CyberSecurity)	5
3.3 Riscos e a segurança da informação/CyberSecurity	6
3.4 Ameaças e a segurança da informação/CyberSecurity.....	7
3.5 Vulnerabilidades	7
3.6 Ataques e vetores de ataque.....	11
3.7 Controles para mitigação de riscos cibernéticos	14
REFERÊNCIAS	18
GLOSSÁRIO	20



3 RISCOS, VULNERABILIDADES E AMEAÇAS À SEGURANÇA DA INFORMAÇÃO E À CONTINUIDADE DE NEGÓCIO

3.1 Onde tudo se inicia

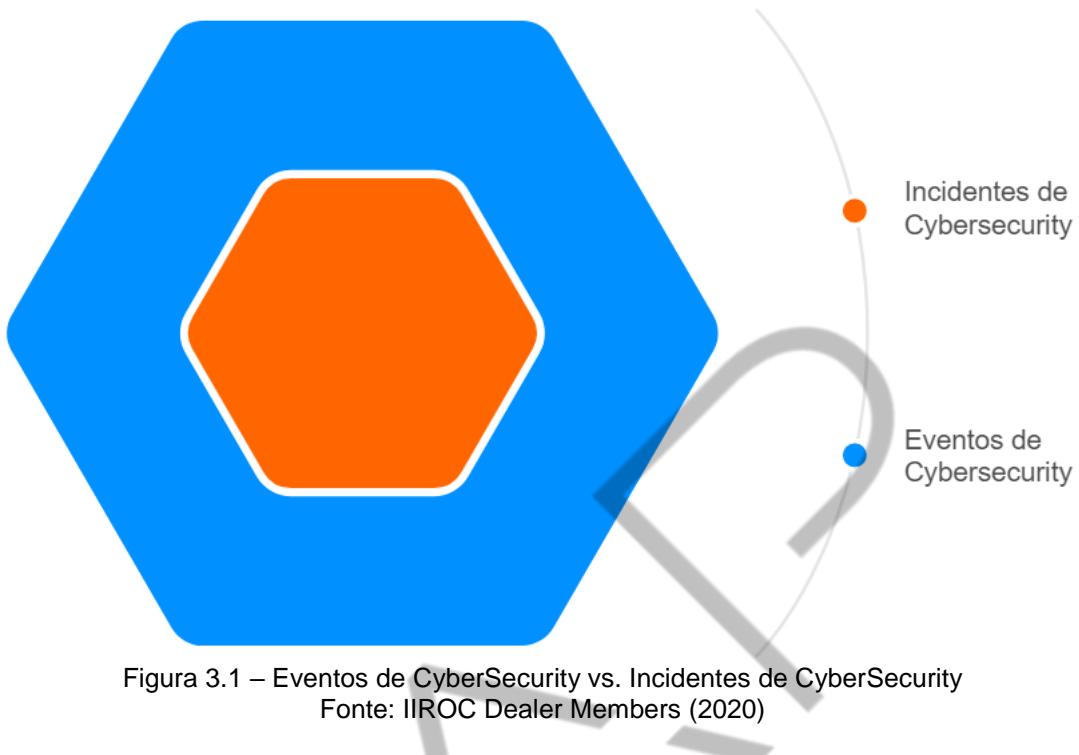
Segundo o professor Gene Spafford (1989), “o único sistema verdadeiramente seguro é aquele que está desligado, preso a um bloco de concreto e trancado em uma sala revestida de chumbo e com guardas armados”. Infelizmente, um sistema em tais condições também não oferece grande contribuição aos negócios da empresa.

Enquanto o time de TI tende a celebrar cada novo serviço colocado em produção, os times de segurança (cibernética e da informação) geralmente enxergam também neste novo serviço uma potencial oportunidade para novos incidentes de segurança. Desta forma, fazendo-se necessário determinar, o mais claro e precisamente possível, quais os principais riscos, vulnerabilidades e ameaças relacionados a todos os serviços, protocolos, sistemas operacionais e quaisquer outros elementos potencialmente capazes de impactar negativamente a segurança do ambiente e a continuidade de negócio.

3.2 Eventos e incidentes de segurança (da informação/CyberSecurity)

Um **evento de segurança** pode ser descrito como uma ocorrência em um sistema, serviço ou estado da rede que aponte para uma possível violação da política de segurança da informação, falha de controles ou uma situação inusitada que pode ser relevante para a segurança. Já, por sua vez, um **incidente de segurança** pode ser entendido como um único ou uma série de eventos de segurança indesejados, ou inesperados, com possibilidades reais de comprometer o fluxo de negócio e ameaçar a segurança da informação (ISO IEC 27001:2005), sendo tais descrições aplicáveis também aos eventos e incidentes de CyberSecurity, respectivamente (IIROC, 2016).

Cabe destacar, conforme livremente representado na figura, que apenas uma pequena parcela dos **eventos** de segurança (da informação/CyberSecurity) acaba efetivamente configurando **incidentes** de segurança (IIROC, 2016).



3.3 Riscos e a segurança da informação/CyberSecurity

O termo **RISCO** é definido de diversas maneiras diferentes, por diferentes autores e entidades, podendo ser simplificadamente entendido como qualquer evento que possa ter impacto (negativo) sobre a capacidade da empresa de alcançar seus objetivos de negócio ou, ainda, como a combinação da probabilidade de ocorrência de um evento e suas consequências (DANTAS, 2011).

Cabe observar que, embora inicialmente talvez os riscos tecnológicos sejam os mais visíveis dentro do contexto da CyberSecurity, eles podem ainda ser classificados em diversas outras categorias, tais como: incontroláveis, mercadológicos, operacionais, legais e humanos, dentre outras. O que significa que deverão ser adequadamente segregados para que possam ser corretamente analisados (DANTAS, 2011), podendo-se concluir que, em última análise, os riscos remetem a perdas para o negócio. Assim sendo, deverão ser criteriosamente avaliados a fim de que se possa dimensionar e direcionar adequadamente os investimentos necessários à sua mitigação e, também, se conhecer o risco residual (nível de risco remanescente após os investimentos efetivados).

3.4 Ameaças e a segurança da informação/CyberSecurity

A ISO/IEC13335-1:2004 define as ameaças como a causa potencial de um incidente indesejado, que pode resultar em dano para um sistema ou para a organização. Já de acordo com Sêmola (2003), ameaças são agentes ou condições que causam incidentes que comprometem as informações e seus ativos, por meio da exploração de vulnerabilidades, comprometendo a CID e, desta forma, impactando os negócios de uma organização.

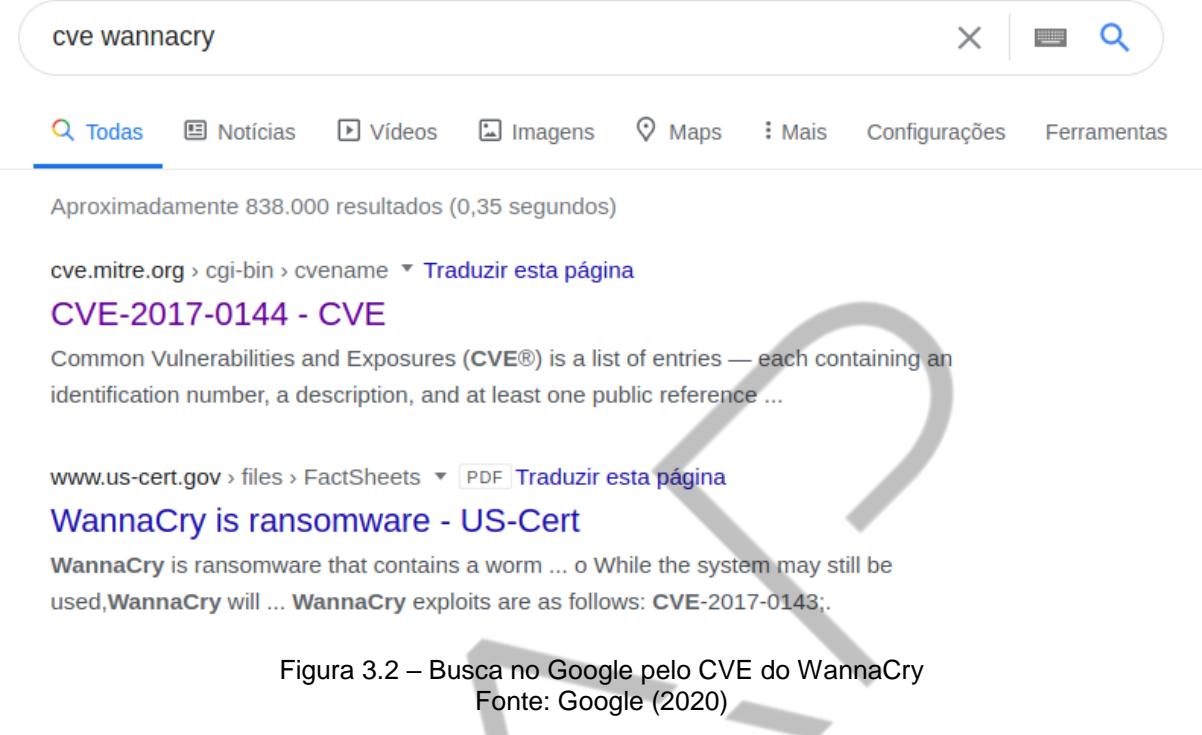
3.5 Vulnerabilidades

Uma vulnerabilidade é uma fraqueza em um sistema, procedimento (de segurança), controle interno ou implementação que poderá ser explorada por uma ameaça. As vulnerabilidades fragilizam os sistemas, deixando-os suscetíveis a incontáveis atividades ilegítimas que poderão causar perdas significativas, por vezes, até irreversíveis, a um indivíduo, grupo ou organização, variando de um simples arquivo danificado em um computador portátil ou dispositivo móvel até grandes bancos de dados em um *Data center* comprometido. Com ferramentas e conhecimentos adequados, um atacante poderá explorar as vulnerabilidades de um sistema, obtendo, assim, acesso às informações nele armazenadas (NIST SP 800-12, 2017).

O site Common Vulnerabilities and Exposures, popularmente chamado apenas como CVE, é uma referência mundial, gratuita e amplamente reconhecida dedicada à identificação e à descrição padronizadas de vulnerabilidades ou exposições e ao compartilhamento de informações sobre vulnerabilidades de softwares específicas.

Admita-se, como exemplo, a necessidade de identificação do CVE do WannaCry a fim de se verificar quais os serviços e sistemas operacionais vulneráveis a esta ameaça e, então, se poder planejar adequadamente a aplicação dos *patches* (correções) dos sistemas operacionais dos *hosts* de uma rede.

O processo pode se iniciar com uma simples busca no Google por: cve wannacry.



Aproximadamente 838.000 resultados (0,35 segundos)

cve.mitre.org › cgi-bin › cvename ▾ Traduzir esta página

CVE-2017-0144 - CVE

Common Vulnerabilities and Exposures (CVE®) is a list of entries — each containing an identification number, a description, and at least one public reference ...

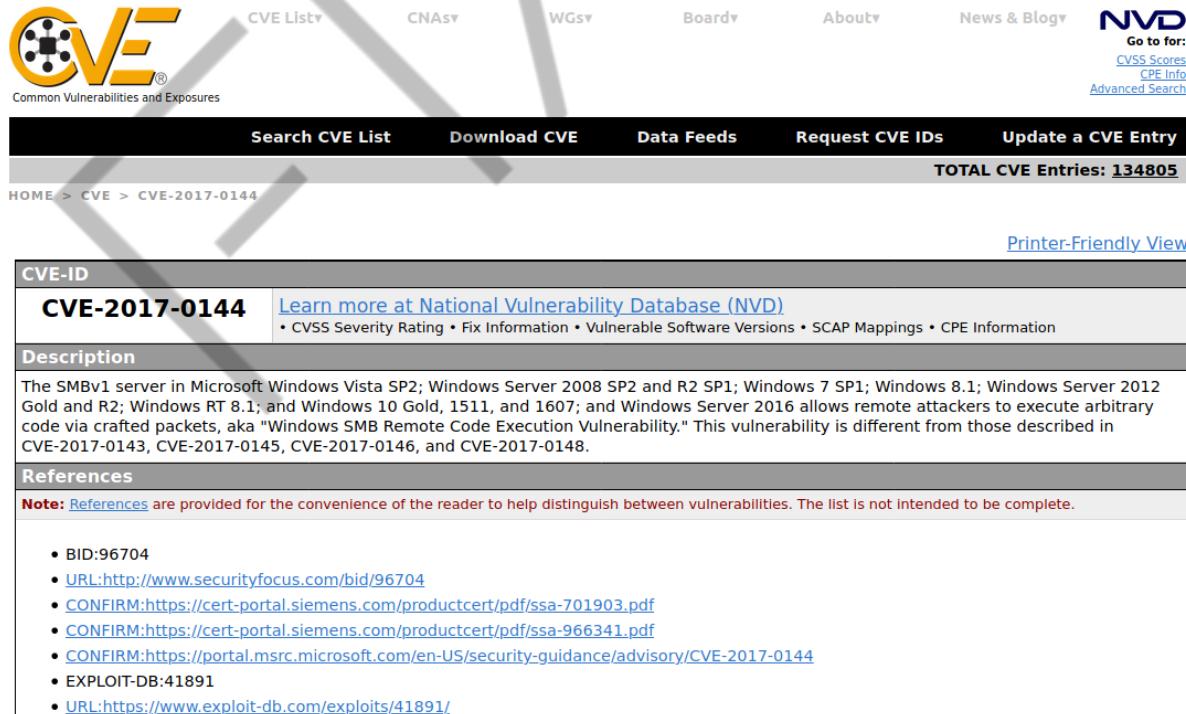
www.us-cert.gov › files › FactSheets ▾ PDF Traduzir esta página

WannaCry is ransomware - US-Cert

WannaCry is ransomware that contains a worm ... o While the system may still be used,WannaCry will ... WannaCry exploits are as follows: CVE-2017-0143;.

Figura 3.2 – Busca no Google pelo CVE do WannaCry
Fonte: Google (2020)

A busca retorna como resposta a identificação do CVE, mais o link para acesso às informações desejadas (Figura “Detalhes do CVE do WannaCry”).



CVE
Common Vulnerabilities and Exposures

[CVE List](#) [CNAS](#) [WG](#) [Board](#) [About](#) [News & Blog](#) [NVD](#)
Go to for:
[CVSS Scores](#) [CPE Info](#) [Advanced Search](#)

[Search CVE List](#) [Download CVE](#) [Data Feeds](#) [Request CVE IDs](#) [Update a CVE Entry](#) **TOTAL CVE Entries: 134805**

HOME > CVE > CVE-2017-0144

[Printer-Friendly View](#)

CVE-ID
CVE-2017-0144 Learn more at National Vulnerability Database (NVD) • CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description
The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.
References
Note: References are provided for the convenience of the reader to help distinguish between vulnerabilities. The list is not intended to be complete.
<ul style="list-style-type: none">• BID:96704• URL:http://www.securityfocus.com/bid/96704• CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-701903.pdf• CONFIRM:https://cert-portal.siemens.com/productcert/pdf/ssa-966341.pdf• CONFIRM:https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2017-0144• EXPLOIT-DB:41891• URL:https://www.exploit-db.com/exploits/41891/

Figura 3.3 – Detalhes do CVE do WannaCry
Fonte: Common Vulnerabilities and Exposures (2020)

É possível observar-se pela Figura “Detalhes do CVE-2017-0144” que o CVE responsável pela identificação e descrição da vulnerabilidade explorada pelo WannaCry é o CVE-2017-0144. Esta vulnerabilidade está relacionada ao serviço de compartilhamento de arquivos implementado pelo protocolo Server Message Block v.1 (SMBv1), executado em sistemas Windows Vista SP2, Windows Server 2008 SP2 e R2 SP1, Windows 7 SP1, Windows 8.1 e demais versões indicadas na referida figura.

CVE-ID	Learn more at National Vulnerability Database (NVD)
CVE-2017-0144	CVSS Severity Rating • Fix Information • Vulnerable Software Versions • SCAP Mappings • CPE Information
Description	
The SMBv1 server in Microsoft Windows Vista SP2; Windows Server 2008 SP2 and R2 SP1; Windows 7 SP1; Windows 8.1; Windows Server 2012 Gold and R2; Windows RT 8.1; and Windows 10 Gold, 1511, and 1607; and Windows Server 2016 allows remote attackers to execute arbitrary code via crafted packets, aka "Windows SMB Remote Code Execution Vulnerability." This vulnerability is different from those described in CVE-2017-0143, CVE-2017-0145, CVE-2017-0146, and CVE-2017-0148.	

Figura 3.4 – Detalhes do CVE-2017-0144
Fonte: Elaborado pelo autor (2020)

Portanto, é notória a grande relevância e aplicabilidade do CVE na mitigação de riscos à segurança da informação relacionados a software. Podendo-se dizer que, de maneira geral, a compreensão das vulnerabilidades é o primeiro passo para mitigação dos riscos, tendo-se ainda como fórmula simplificada para cálculo do risco:



Quadro 3.1 – Cálculo do risco
Fonte: Simplicable (2020)

O quadro aponta ainda alguns exemplos relacionados aos riscos, ameaças e vulnerabilidades mais comumente observados no mercado. De acordo com a fonte tomada como referência, pode-se observar que nem todas as ameaças vêm necessariamente de *hackers* e nem todas as vulnerabilidades são obrigatoriamente tecnológicas.

Em sua pesquisa sobre a Evolução da ameaça de TI no segundo trimestre de 2019 , a Kaspersky concluiu que a distribuição de aplicativos móveis detectados por tipo, como RiskTools (41,24%), Adware (18,71%), Trojan (11,83%) e Trojan-Dropper (10,04%) estão entre as ameaças mais observadas, como mostrado na Figura Distribuição de aplicativos móveis detectados por tipo.

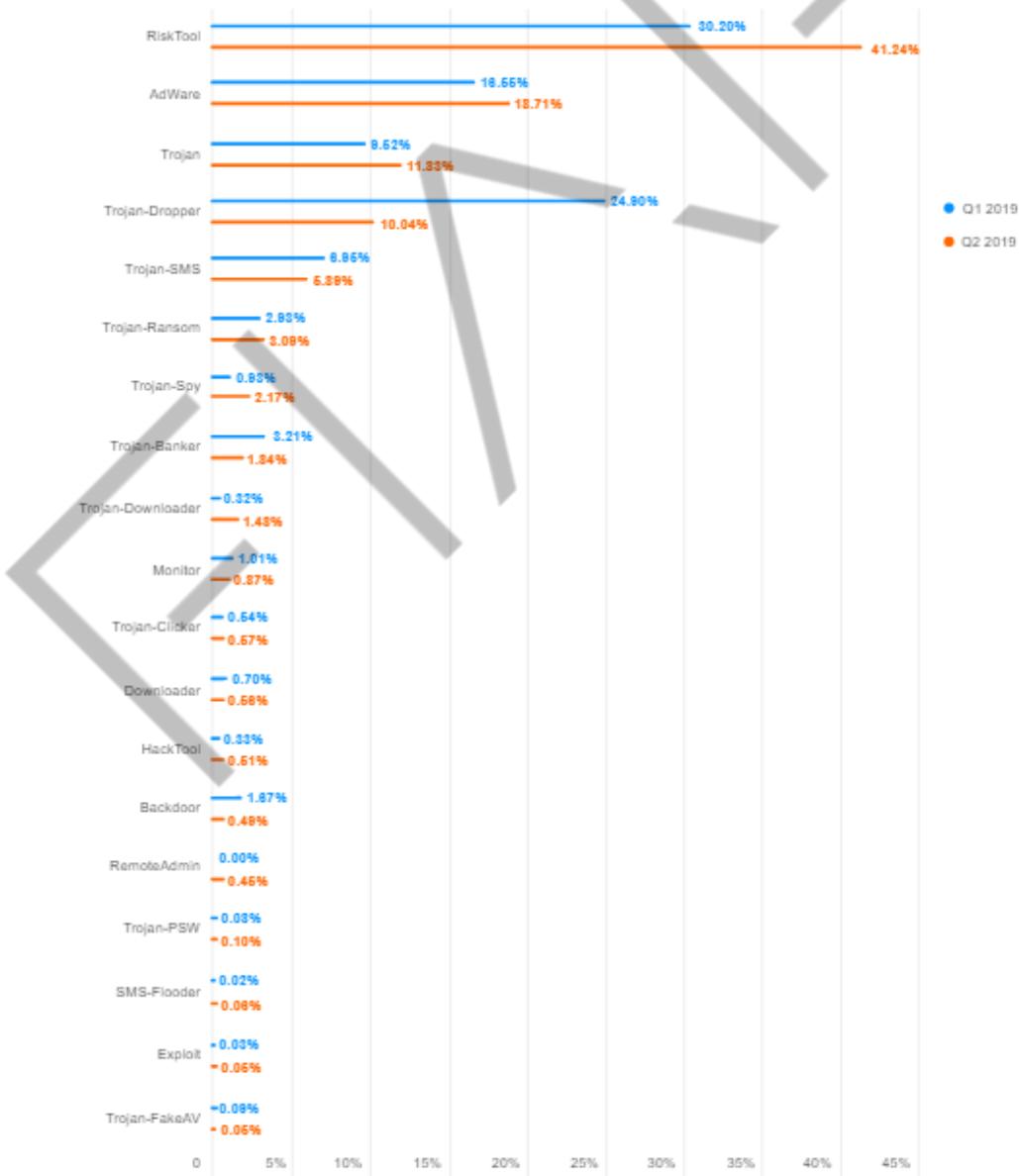


Figura 3.5 – Distribuição de aplicativos móveis detectados por tipo
Fonte: Kaspersky (2020)

3.6 Ataques e vetores de ataque

Um vetor de ataque (*attack vector*) é um caminho ou meio utilizado por um atacante para obter acesso não autorizado a um alvo, como, por exemplo: um sistema, rede ou dispositivo, permitindo, assim, que este atacante explore vulnerabilidades do sistema, incluindo o elemento humano (quando uma pessoa é enganada, para remover ou enfraquecer as defesas do sistema). Os vetores de ataque incluem vírus, anexos de e-mail, páginas web, janelas *pop-up*, mensagens instantâneas e salas de bate-papo, dentre outros ardilis.

De acordo com o Sept. 2017 Quarterly Threat Report, da McAfee Labs, os oito principais tipos de ataques contra as redes locais verificados durante o segundo trimestre de 2017 foram:

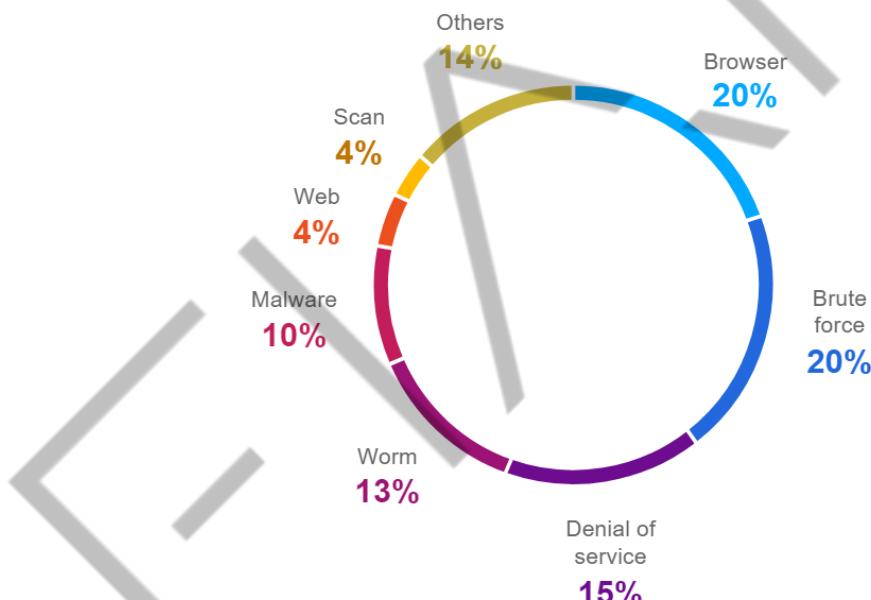


Figura 3.6 – Oito principais ataques às redes
Fonte: McAfee Labs (2020)

1º ATAQUES VIA BROWSER (20%): atacantes tentam violar uma máquina por intermédio de seu navegador web. Geralmente, estes ataques se originam em sites legítimos, porém, vulneráveis e infectados por *malwares*. A partir daí, quando visitantes navegam até estes sites, eles, por sua vez, tentarão forçar o *malware* nos sistemas dos visitantes por meio da exploração de vulnerabilidades em seus navegadores. De acordo com o Internet Security Threat Report 2017, da Symantec, os *browsers* com mais vulnerabilidades descobertas em 2016 são o Microsoft Internet Explorer / Edge, Google Chrome, Mozilla Firefox, Apple Safari e Opera.

2º ATAQUES POR FORÇA BRUTA (20%): Neste tipo de ataque, em vez de tentar enganar o usuário a fim de fazê-lo baixar um *malware*, o atacante procura descobrir suas credenciais (*username* e senha) para autenticação em um sistema ou serviço por meio de tentativa e erro. Este tipo de ataque pode ser consideravelmente demorado, razão pela qual o atacante geralmente recorre a ferramentas especializadas que automatizam o processo, como, por exemplo, o **Hydra**.

3º ATAQUES DE NEGAÇÃO DE SERVIÇO (15%): os ataques de negação de serviço – [Distributed] Denial of Service ([D]DoS) têm como objetivo sobrecarregar um recurso: site, servidor de jogos ou servidor HTTP, entre outros, inundando-os com tráfego, requisições ou pedidos de conexão, descontinuando o serviço ou causando lentidão extrema.

4º ATAQUES POR WORMS (13%): o *malware* normalmente requer algum tipo de interação do usuário para iniciar a infecção. Por exemplo, a vítima pode ter de baixar um anexo de e-mail malicioso, visitar um site infectado ou conectar um *pen drive* infectado à máquina. *Worms* são *malwares* de autopropagação que não requerem a interação do usuário, normalmente, explorando vulnerabilidades do sistema para se espalharem pelas redes locais e além.

5º ATAQUES POR MALWARES (10%): simplificadamente, *malware* é um código (software) malicioso criado para prejudicar, sequestrar ou espionar o sistema infectado. Três das formas comuns de propagação incluem:

- **Phishing (e-mails)**: e-mails fraudulentos criados para atrair vítimas e induzi-las ao *download* de anexos maliciosos (*malware*).
- **Sites maliciosos**: atacantes podem configurar sites equipando-os com códigos maliciosos destinados a encontrar vulnerabilidades no sistema de seus visitantes, forçando, então, o *malware* nos seus sistemas. Podem ainda ser usados para disfarçar o *malware* na forma de *downloads* legítimos.

- **Malvertising:** é um tipo de anúncio publicitário (*online*) utilizado para disseminação de *malwares* via Internet que, ao ser clicado, pode redirecionar usuários para um site de hospedagem de *malware*. Alguns ataques de *malvertising* nem exigem interação do usuário para infectar um sistema.

6º ATAQUES WEB (4%): são ataques direcionados a serviços na web, predominantemente, aplicações e bases de dados, geralmente tendo como objetivo a obtenção de dados ou causar algum tipo de prejuízo ao serviço, como, por exemplo, descontinuidade ([D]DoS¹¹) ou descaracterização (*defacement*).

Segundo a Positive Research, alguns dos ataques web mais comuns no segundo quadrimestre de 2017 foram:

- **Cross-Site Scripting (XSS):** violação de um site ou aplicação web vulneráveis com injeção de código malicioso que executa um *script* nos navegadores dos usuários quando a página é carregada.
- **SQL Injection (SQLi):** em vez de preencher adequadamente formulários web, o atacante aproveita-se deles para enviar comandos SQL a uma aplicação vulnerável. A partir daí, pode conseguir acesso ou manipular a base de dados desta aplicação.
- **Path Traversal:** este ataque explora diferentes vulnerabilidades nas vias que levam a arquivos e diretórios, possibilitando ao atacante acesso não autorizado a eles.. Por meio de sequências especiais, como, por exemplo “..*J*” – interpretada pelo sistema operacional como uma solicitação para descer um nível nos diretórios –, o atacante altera a via (*path*) da requisição original do usuário, podendo acessar o sistema de arquivos em um servidor web, entre outros, que execute uma aplicação vulnerável.

7º VARREDURAS (SCAN ATTACKS) (4%): são procedimentos direcionados às redes de computadores, principalmente, com o objetivo de identificar os *hosts* ativos e os serviços executados por eles. São amplamente utilizadas por atacantes

para identificar potenciais alvos, pois permitem também a associação de possíveis vulnerabilidades aos serviços disponibilizados pelo *host*.

Assim sendo, as varreduras (*scans*) subdividem-se em dois grandes grupos: *port scans* (varreduras de porta), executadas por ferramentas como o NMAP, e *vulnerability scans* (varreduras de vulnerabilidades), executadas por ferramentas como OpenVAS e Nessus.

8º OUTROS ATAQUES (14%): nesta categoria, a pesquisa apenas especula sobre os ataques mais recorrentes às redes, destacando:

- **Ataques físicos**: o atacante consegue acesso físico aos ativos da rede e, a partir daí, tenta causar danos a eles ou ao ambiente. Por exemplo, desligando servidores ou removendo os cabos que os conectam à rede, entre outros, podendo ainda chegar a subtrair ativos menores como notebooks e *access points*.
- **Insiders**: ataques promovidos por empregados insatisfeitos ou em conluio com concorrentes ou ainda terceirizados mal-intencionados são algumas das muitas possibilidades existentes. Os *insiders* representam um grande risco à instituição na medida em que podem abusar de suas credenciais e privilégios. Por exemplo, para fazer mal uso das informações de clientes sob guarda e responsabilidade da empresa ou, ainda, promover vazamentos de informações privilegiadas.
- **Advanced Persistent Threats (APT)**: as Ameaças Persistentes Avançadas (APT) são ataques avançados às redes geralmente promovidos por atacantes altamente qualificados. Eles desenvolvem ou adaptam suas técnicas sob medida para o ambiente do alvo com o objetivo de monitorá-lo e coletar informações dele por períodos prolongados, de forma persistente e furtiva.

3.7 Controles para mitigação de riscos cibernéticos

O Center for Internet Security (CIS) elaborou e mantém um guia com 20 controles para mitigação de riscos cibernéticos, o **CIS Controls**, dos quais

destacam-se aqui os cinco primeiros. De acordo com diferentes estudos, estes cinco citados a seguir, poderão mitigar até 85% dos *cyber attacks*:

- a. Inventário de dispositivos autorizados e não autorizados.
- b. Inventário de softwares autorizados e não autorizados.
- c. Implementação e gerenciamento da configuração segura dos ativos.
- d. Processos para avaliação e remediação continuada de vulnerabilidades.
- e. Uso apropriado de privilégios administrativos.

Naturalmente, a implementação de tais controles deverá ser bem planejada e alinhada com as particularidades e necessidades de cada organização. A criação e a manutenção de um sistema de inventário para dispositivos e softwares, especialmente em pequenas e médias empresas, podem não ser uma tarefa muito simples.

Enquanto, notoriamente, grandes corporações precisarão de ferramentas sofisticadas e considerável quantidade de colaboradores para execução de tal tarefa, pequenas e médias organizações poderão optar por soluções mais simples. Ressalta-se, entretanto, que a eficácia e a confiabilidade do controle deverão satisfazer adequadamente as necessidades de qualquer negócio (pequeno, médio ou grande).

Uma boa opção de ferramenta para inventário, especialmente para o segmento SMB (*Small and Midsized Business* – pequenas e médias empresas), pode ser o OCS Inventory.

Por sua vez, o gerenciamento de configurações também é altamente relevante para a segurança da rede, não apenas em relação à prevenção contra ataques e mitigação dos riscos inerentes a eles, mas também quanto à rápida restauração do ambiente de produção e manutenção da continuidade de negócios. Tome-se como exemplo um servidor de produção que deva ser substituído em regime de urgência diante de algum incidente, como avarias em seu disco rígido.

Sem a adequada gestão das configurações deste ativo, o tempo necessário para restabelecimento do serviço após a substituição do dispositivo avariado será

consideravelmente prolongado em decorrência da necessidade de apuração do sistema operacional. Para isso, medidas deverão ser tomadas: a respectiva versão a ser reinstalada; a identificação dos patches de segurança a serem instalados; a reconfiguração dos serviços a serem disponibilizados, a reconfiguração dos sistemas de proteção locais, como, por exemplo, antivírus e *firewall* local; a recriação de contas/perfis de usuários, entre vários outros itens.

Há que se observar ainda que as mesmas publicações sobre novas vulnerabilidades, utilizadas por profissionais da área de segurança para *hardening* de seus sistemas, e o desenvolvimento de novas soluções e contramedidas para correção destas vulnerabilidades também são empregados pelos atacantes para a construção de novas ferramentas destinadas à exploração delas.

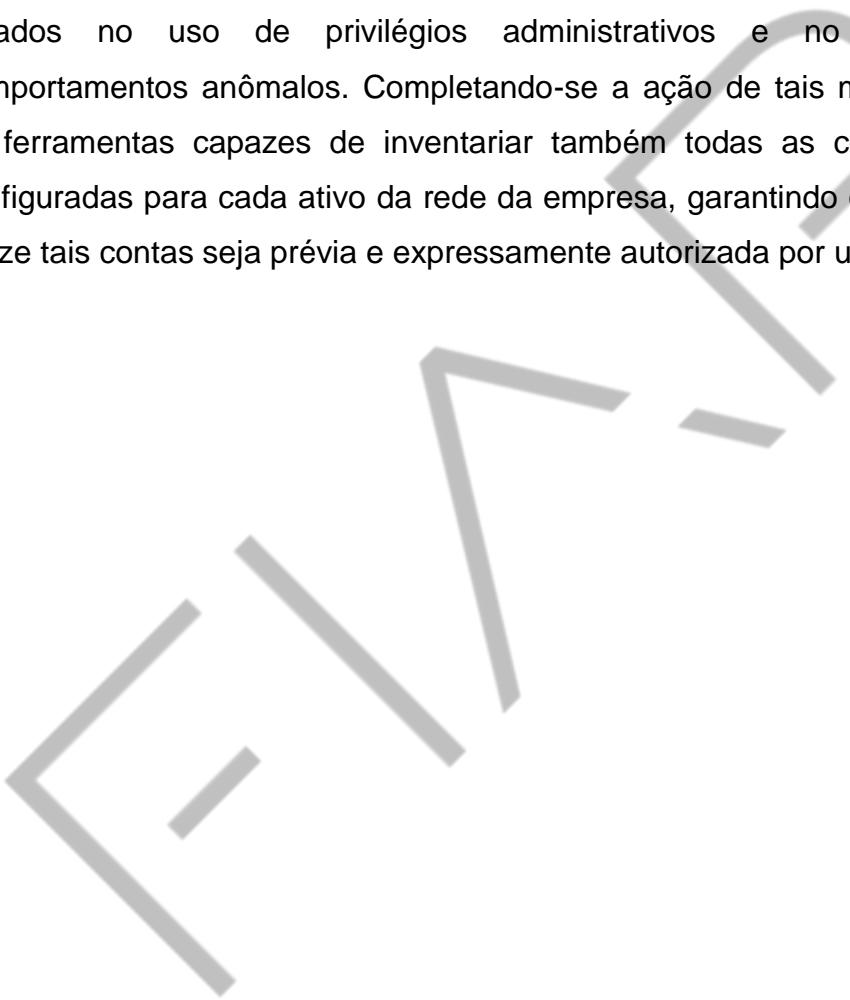
Assim sendo, tem-se o início de uma corrida entre os dois lados, com desdobramentos que podem impactar significativamente o negócio. Portanto, entre as diferentes práticas aplicáveis, torna-se uma boa opção para as empresas a adoção de um **Security Content Automation Protocol** (SCAP) para auxiliar no planejamento e execução de varreduras de vulnerabilidades automatizadas e periódicas em seus ambientes. Desta forma, são produzidos relatórios que listam individualmente as vulnerabilidades mais críticas verificadas em cada sistema, juntamente com os respectivos scores de risco. O que permite que seus administradores tenham informações atualizadas e precisas para direcionar a implementação de controles eficazes para remediação.

É importante ainda que os *logs* de eventos sejam correlacionados com as informações produzidas pelas referidas varreduras para certificar-se de que as atividades das próprias ferramentas que as executam estejam sendo adequadamente registradas. Além disso, para que seja possível também relacionar eventos de detecção de ataques com os resultados de varreduras prévias. E desta maneira, verificar se dado *exploit* foi utilizado contra um alvo já sabidamente vulnerável.

Não obstante, é notório ainda que o uso inadequado de privilégios administrativos pode permitir a um atacante a instalação, geralmente sem conhecimento do usuário, de ferramentas como *keyloggers* ou softwares para acesso remoto, os quais deixarão o *host* alvo do ataque (*target*) suscetível ao monitoramento e outras ações clandestinas por parte do atacante.

Assim sendo, alguns princípios básicos deverão ser sempre observados. Iniciando-se pelo rigoroso controle do uso de privilégios (administrativos) e contas administrativas, seguindo-se atentamente o princípio dos privilégios mínimos (**Least Privileges**). Com base nele, garantir que o usuário utilize apenas credenciais administrativas alinhadas com seu perfil de trabalho estritamente quando necessário (evitando-se a divulgação e o uso das credenciais do administrador do sistema).

Por fim, recomenda-se ainda a implementação de mecanismos de auditoria focados no uso de privilégios administrativos e no monitoramento de comportamentos anômalos. Completando-se a ação de tais mecanismos por meio de ferramentas capazes de inventariar também todas as contas administrativas configuradas para cada ativo da rede da empresa, garantindo que cada pessoa que utilize tais contas seja prévia e expressamente autorizada por um executivo.



REFERÊNCIAS

BEEK, C. et al. **The WannaCry malware attack infected more than 300,000 computers in over 150 countries in less than 24 hours.** McAfee Labs. 2017. Disponível em: <<https://www.mcafee.com/ca/resources/reports/rp-quarterly-threats-sept-2017.pdf>>. Acesso em: 21 abr. 2020.

CIS. **First 5 CIS Controls Guide.** 2017. Disponível em: <<https://www.cisecurity.org/controls/>>. Acesso em: 21 abr. 2020.

DANTAS, M. L. **Segurança da Informação:** uma abordagem focada em gestão de riscos. Olinda: Livro Rápido, 2011.

DEWDNEY, A. K. **Computer Recreations:** of Worms, Viruses and Core War. Disponível em: <spaf.cerias.purdue.edu/quotes.html>. Acesso em: 21 abr. 2020.

IIROC – Investment Industry Regulatory Organization of Canada. **Cybersecurity Best Practices Guide.** 2016. Disponível em: <http://www.iirc.ca/industry/Documents/CybersecurityBestPracticesGuide_en.pdf#search=cybersecurity>. 21 abr. 2020.

_____. **Cyber Incident Management Planning Guide.** 2016. Disponível em: <http://www.iirc.ca/industry/Documents/CyberIncidentManagementPlanningGuide_en.pdf#search=cybersecurity>. Acesso em: 21 abr. 2020.

KASPERSKY. **IT threat evolution Q2 2019. Statistics.** Disponível em: <<https://securelist.com/it-threat-evolution-q2-2019-statistics/92053/>>. Acesso em: 21 abr. 2020.

NIST Special Publication (SP) 800-30 Revision 1. **An Introduction to Information Security.** National Institute of Standards and Technology, Gaithersburg, Maryland, 2017, 101 pp. Disponível em: <<https://csrc.nist.gov/publications/detail/sp/800-12/rev-1/final>>. Acesso em: 21 abr. 2020.

_____. **Guide for Conducting Risk Assessments.** National Institute of Standards and Technology, Gaithersburg, Maryland, 2012, 95 pp. Disponível em: <<https://csrc.nist.gov/publications/detail/sp/800-30/rev-1/final>>. Acesso em: 21 abr. 2020.

O'DONNELL, A. **Security Content Automation Protocol (SCAP). What does SCAP mean?** 2017. Disponível em: <<https://www.lifewire.com/what-is-scap-2487459>>. Acesso em: 21 abr. 2020.

OWASP. **Category: Attack.** 2017. Disponível em: <<https://www.owasp.org/index.php/Category:Attack>>. Acesso em: 13 out. 2017 .

POSITIVE RESEARCH. **Web Application Attack Statistics:** Q2 2017. 14 set. 2017. Disponível em: <<http://blog.ptsecurity.com/2017/09/web-application-attack-statistics-q2.html>>. Acesso em: 13 out. 2017.

PURDUE UNIVERSITY. **Quotable Spaf.** 2017. Disponível em:
<<http://spaf.cerias.purdue.edu/quotes.html>>. Acesso em: 13 out. 2017.

SÊMOLA, M. **Gestão da segurança da informação:** visão executiva da segurança
da informação. Rio de Janeiro: Campus, 2003.

SIMPLICABLE. **Display image:** security vulnerabilities. Disponível em:
<<https://arch.simplifiable.com/arch/photo/178/security-vulnerabilities.html>>. Acesso
em: 13 out. 2017.



GLOSSÁRIO

Hardening	Processo de mapeamento das ameaças, mitigação de riscos e efetivação das atividades corretivas necessárias ao fortalecimento do ativo para torná-lo adequadamente preparado contra eventuais tentativas de ataque.
BCP	Business Continuity Plan – Plano de Continuidade de Negócios.
Score de risco	Simplificadamente, pode ser descrito como a pontuação que expressa a gravidade de um risco em relação aos demais analisados sob o mesmo contexto.
SCAP	Acrônimo para Security Content Automation Protocol, tem como objetivo aplicar um padrão de segurança já aceito às organizações que ainda não possuem um ou àquelas cujas implementações são deficientes.
Log	Expressão utilizada para se referir ao processo de registro de eventos relevantes ocorridos em um sistema computacional.
Exploit	Simplificadamente, pode ser entendido como uma peça de software especialmente desenvolvida para explorar as vulnerabilidades de um sistema-alvo com as mais diversas finalidades, como, por exemplo, a invasão deste sistema para a coleta de informações de seus usuários.
Keylogger	Tipo de <i>spyware</i> especificamente desenvolvido para registrar tudo o que for digitado no sistema onde vier a ser executado com o objetivo de obter informações dos usuários.
Spyware	Tipo de software especificamente desenvolvido para coletar clandestinamente informações dos usuários do sistema onde for executado.
Trojan	Tipo de código malicioso geralmente disfarçado de software legítimo com o objetivo

	de ganhar acesso aos sistemas dos usuários e, a partir daí, executar as funções para as quais foi programado, por exemplo, coletar dados do usuário e enviá-los ao <i>hacker</i> .
--	--

