FIAP ON

CYBERSECURITY

INTRODUÇÃO, DEFINIÇÃO E RELEVÂNCIA **PARA O NEGÓCIO**

OSMANY DANTAS RIBEIRO DE ARRUDA

1

LISTA DE FIGURAS

LISTA DE TABELAS

SUMÁRIO

1 INTRODUÇÃO, DEFINIÇÃO E RELEVÂNCIA PARA O NEGÓCIO

1.1 Conceito de Cybersecurity

Ao longo dos últimos anos, é notória a crescente preocupação expressada por diferentes especialistas em relação à necessidade de proteção de sistemas de Tecnologia da Informação e Comunicação (TIC) contra-ataques cibernéticos. Eles podem ser definidos como tentativas deliberadas, por parte de pessoas não autorizadas, de obter acesso a estes sistemas, geralmente com o objetivo de “roubo”, destruição ou prática de outros tipos de ações danosas ou ilegais (FISCHER, 2016).

De acordo com Craigen et al. (2014), Cybersecurity é um termo amplamente utilizado, com definições muito diversificadas, por vezes até subjetivas e pouco informativas. No entanto, entre as definições que consideraram melhor representar a perspectiva de Cybersecurity, destacam-se:

1. Cybersecurity implica a salvaguarda das redes de computadores e das informações nelas contidas contra intrusão, danos ou descontinuidades (apud LEWIS, 2006).
2. Cybersecurity envolve a redução do risco de ataques a softwares, computadores e redes. Isso inclui ferramentas usadas para detectar invasões, contenção de vírus, bloqueio de acessos maliciosos, forçar autenticação, uso de criptografia e assim por diante (apud AMOROSO, 2006).
3. Cybersecurity é um conjunto de ferramentas, políticas, conceitos e salvaguardas de segurança, diretrizes, abordagens de gerenciamento de riscos, ações, treinamentos, melhores práticas, garantias e tecnologias que podem ser usados para proteger o ambiente cibernético, a organização e os recursos do usuário (apud ITU, 2009).

Assim sendo, pode-se concluir ser o conceito Cybersecurity mais abrangente do que apenas soluções tecnológicas, englobando também gestão, gerenciamento de riscos e continuidade de negócio, entre outros aspectos.

1.2 Cybersecurity e negócios

As notícias demonstram, como apresentado na figura a seguir, que as empresas já têm consciência do problema e que já estão tomando as medidas necessárias para mitigar riscos e garantir a continuidade de negócio. Um estudo da Cyber Security Insights, publicado no portal Terra, aponta investimento realizado na área de segurança da informação.

terra

US$ 6 trilhões até 2021: segurança move investimentos e LGPD é um dos impulsos

Nada menos do que US$ 6 trilhões até 2021. Este é o montante que deverá ser investido em todo o mundo na área de segurança da informação, com foco em evitar o vazamento de dados e invasões de sistemas e redes, segundo o estudo Cyber Security Insights.

A conta é alta, e também preocupante, já que cerca de US$ 1 bilhão/ano deste total tende a ser pago pelo chamado resgate de informações "sequestradas" por cibercriminosos.

E se o quadro global chama atenção pelo volume,no Brasil as cifras não ficam atrás: levantamento da Ponemon aponta que ciberataques geram, no país, prejuízos na casa dos R$ 3,96 milhões por ocorrência às organizações afetadas.

Um cenário que pode sofrer variações, incluindo altas nos investimentos, em função de novas legislações, como a Lei Geral de Proteção de Dados (LGPD), que entra em vigor em 2020 e traz diversas novas exigências quanto à coleta e utilização de dados, especialmente no que tange a clientes, parceiros e colaboradores de empresas.

Figura 1.1 – Investimento na área de segurança da informação
Fonte: Terra (2020)

Os gastos com gerenciamento de riscos e segurança da informação empresarial no Oriente Médio e Norte da África (MENA) totalizarão US$ 1,7 bilhão em 2020, um aumento de 10,7% em relação a 2019, de acordo com uma previsão recente da Gartner, Inc.

O mercado global de segurança cibernética já vale US$ 173 bilhões em 2020, com expectativa de crescimento para US$ 270 bilhões em 2026. Até 2026, 77% dos gastos com segurança cibernética serão para serviços de segurança gerenciados externamente. Enquanto o dinheiro gasto em funções internas de segurança cibernética deve crescer 7,2% a cada ano até 2026, projeta-se que os gastos globais com produtos e serviços externos de segurança cibernética aumentem 8,4% ao ano no mesmo período, de acordo com AustCyber is the Australian Cyber Security Growth Network.

O CERT.br é o Grupo de Resposta a Incidentes de Segurança para a Internet brasileira, mantido pelo NIC.br, do Comitê Gestor da Internet no Brasil, tendo sob sua responsabilidade o tratamento dos incidentes de segurança em computadores que envolvam redes conectadas à Internet brasileira. Atua, ainda, como ponto central para notificações de incidentes de segurança no Brasil, provendo a coordenação e o apoio no processo de resposta a incidentes e, quando necessário, colocando as partes envolvidas em contato.

As estatísticas produzidas pelo CERT.br são fontes de informação confiáveis e atualizadas, podendo servir às empresas na forma de ferramentas auxiliares na identificação das principais ameaças à continuidade de seus negócios e na avaliação (*score*) dos riscos. Desta forma, pode contribuir também com o planejamento e direcionamento dos investimentos em Cybersecurity.

A tabela ilustra os incidentes reportados ao CERT.br no período de **janeiro** a **dezembro** de **2019**.

Tabela 1.1 – Incidentes reportados por tipo de ataque

Mês	Total	worm (%)		**dos** (%)		invasão (%)		web (%)		**scan** (%)		**fraude** (%)		outros (%)	
jan	**62481**	7796	12	4191	6	19	0	2594	4	46038	73	1744	2	99	0
fev	**70069**	7707	11	2192	3	27	0	4179	5	54401	77	1459	2	104	0
mar	**85409**	4476	5	29309	34	19	0	2006	2	47966	56	1521	1	112	0
abr	**59900**	7624	12	2718	4	37	0	1555	2	45774	76	2119	3	73	0
mai	**52129**	6555	12	15773	30	74	0	1425	2	25521	48	2633	5	148	0
jun	**221231**	6598	2	191593	86	52	0	1337	0	19289	8	2230	1	132	0
jul	**48836**	8230	16	3884	7	27	0	1308	2	32054	65	2994	6	339	0
ago	**61006**	11421	18	5892	9	51	0	1561	2	37521	61	4400	7	160	0
set	**52027**	9599	18	7326	14	28	0	1876	3	27654	53	5388	10	156	0
out	**53253**	10568	19	8313	15	45	0	2219	4	26153	49	5859	11	96	0
nov	**59735**	7032	11	25701	43	80	0	625	1	20450	34	5795	9	52	0
dez	**49251**	12871	26	4416	8	68	0	1649	3	26927	54	3277	6	43	0
Total	**875327**	100477	11	301308	34	527	0	22334	2	409748	46	39419	4	1514	0

Fonte: CERT.br (2019)

Worm: notificações de atividades maliciosas relacionadas com o processo automatizado de propagação de códigos maliciosos na rede.

Dos (DoS – *Denial of Service*): notificações de ataques de negação de serviço, onde o atacante utiliza um computador ou um conjunto de computadores para tirar de operação um serviço, computador ou rede.

Invasão: um ataque bem-sucedido que resulte no acesso não autorizado a um computador ou rede.

Web: um caso particular de ataque, visando especificamente o comprometimento de servidores Web ou desfigurações de páginas na Internet.

Scan: notificações de varreduras em redes de computadores para identificar quais computadores estão ativos e quais serviços estão sendo disponibilizados por eles. É amplamente utilizado por atacantes para identificar potenciais alvos, pois permite associar possíveis vulnerabilidades aos serviços habilitados em um computador.

Fraude: segundo o Houaiss, é "qualquer ato ardiloso, enganoso, de má-fé, com o objetivo de lesar ou ludibriar outrem, ou de não cumprir determinado dever; logro". Esta categoria engloba as notificações de tentativas de fraudes, ou seja, de incidentes em que ocorre uma tentativa de obter vantagem.

Outros: notificações de incidentes que não se enquadram nas categorias anteriores.

Entre os ataques de maior repercussão nesses últimos anos, há que se destacar dois ataques de proporções mundiais, com o WannaCry e Petya, ocorridos em 2017.

Na sexta-feira, 12 de maio de 2017, 74 países, entre eles, o Brasil, foram afetados pelo WannaCry, um tipo de *ransomware* autopropagável capaz de criptografar os arquivos dos sistemas afetados.

Figura 1.2 – Tela do WannaCry
Fonte: Google Imagens (2017)

O WannaCry adiciona a extensão .WCRY aos arquivos infectados, exigindo um resgate de US$ 300 ou $ 600 (em bitcoin) para decodificá-los, estimando-se que os prejuízos globais tenham chegado a US$ 1 bilhão.

Diferentemente da maioria dos *ransomwares*, ele não se propaga por intermédio de spam, mas explora uma vulnerabilidade no protocolo do Server Message Block (SMB) da Microsoft conhecida como EternalBlue.

O WannaCry explora uma vulnerabilidade do SMBv.1, protocolo que, diante disso, deveria ser imediatamente abandonado pelos usuários tanto das versões do

Windows destinadas a servidores quanto das versões voltadas a desktops (Figura Tela de recursos do Windows), conforme alertado por Ned Pyle (Microsoft) em setembro de 2016.

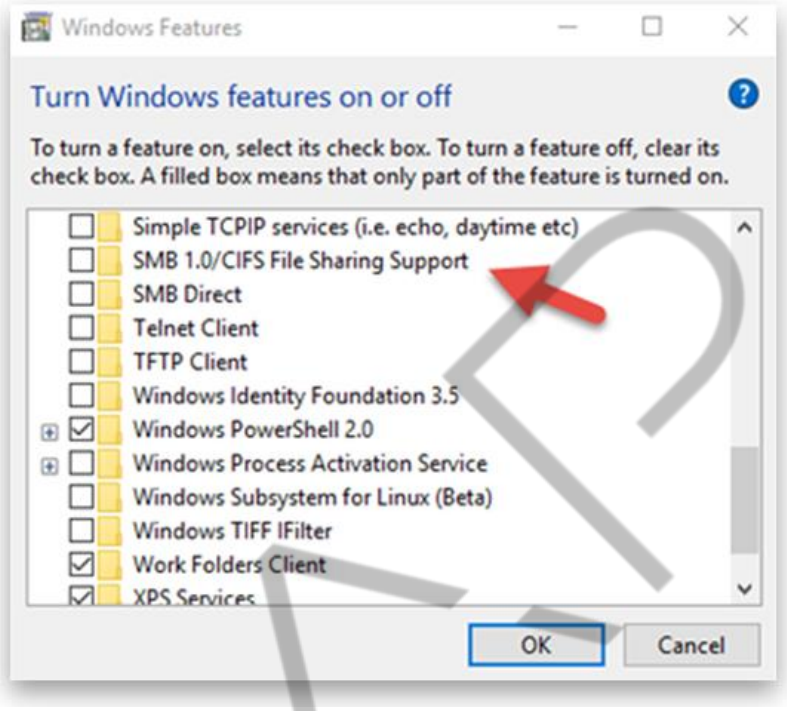

Figura 1.3 – Tela de recursos do Windows
Fonte: Blog Technet – Microsoft (2017)

Após a ampla contaminação, várias empresas e órgãos governamentais, tais como o Serviço Nacional de Saúde do Reino Unido, a Telefônica, o Tribunal de Justiça e o Ministério Público de São Paulo foram paralisados. E uma atualização foi disponibilizada pela Microsoft, em regime de urgência, aos usuários do sistema operacional Windows.

Em sua versão inicial, o Petya difere dos *ransomware* mais tradicionais na medida em que, em vez de criptografar arquivos um a um, ele impede completamente o acesso ao sistema, atacando estruturas de baixo nível do disco.

Seus autores não apenas criaram um bootloader próprio, como também uma versão reduzida de *kernel* malicioso, que ocupa apenas 32 setores no disco. Assim, este *malware* subverte o MBR de forma que carrega seu próprio *kernel* malicioso na inicialização do sistema, criptografando, então, o disco.

Embora a mensagem enviada ao usuário afirme que o disco tenha sido totalmente criptografado, na verdade, apenas a tabela de arquivos mestre (MFT) foi atacada a fim de tornar o sistema de arquivos ilegível.

O Petya passou por atualizações, retornando em uma combinação com outro *ransomware,* o Mischa, no mesmo *dropper*, e passou a empacotado com o nome de GOLDENEYE, distribuído por *phishing e-mails*.

Enquanto o Petya é responsável pelos ataques em baixo nível, dependentes de privilégios elevados – já que envolve a subversão do MBR –, o Mischa é implementado como um *payload* alternativo, caso o *dropper* seja executado sem privilégios administrativos e o ataque em baixo nível não seja possível.

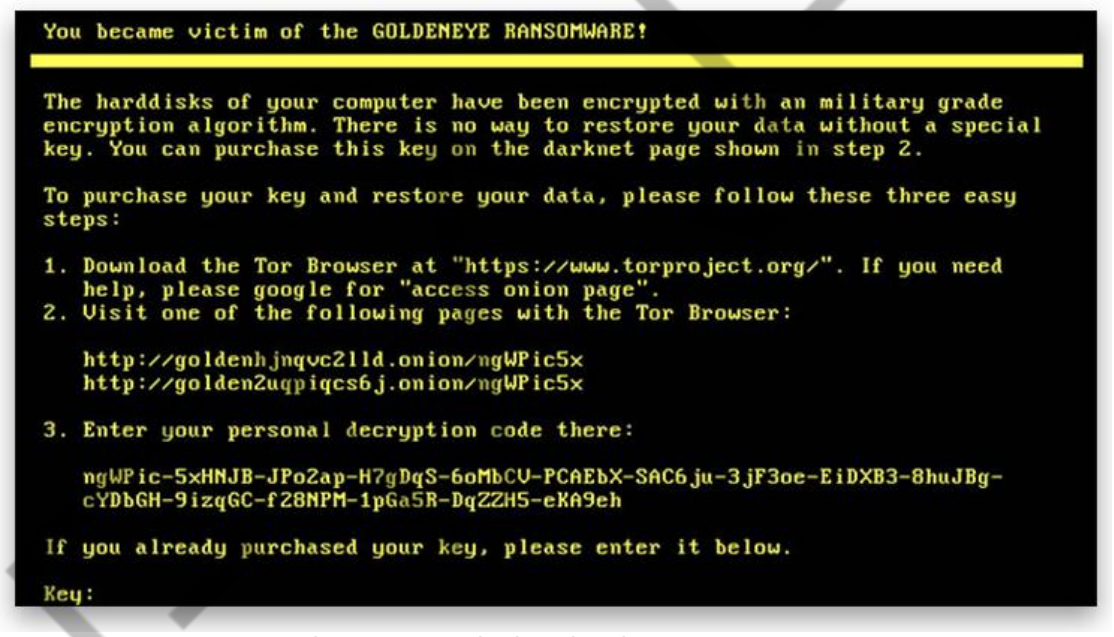

Figura 1.4 – Tela de aviso do GOLDENEYE
Fonte: Blog Malwarebytes (2017)

1.3 Vetores de ataques

Simplificadamente, um vetor de ataque pode ser descrito como o meio utilizado pelo agente da ameaça para atacar o sistema-alvo.

O website HACKMAGEDDON, especializado em *timelines* e estatísticas em Cybersecurity, publicou a seguinte estatística, referente aos vetores de ataque de maior destaque em abril de 2020:

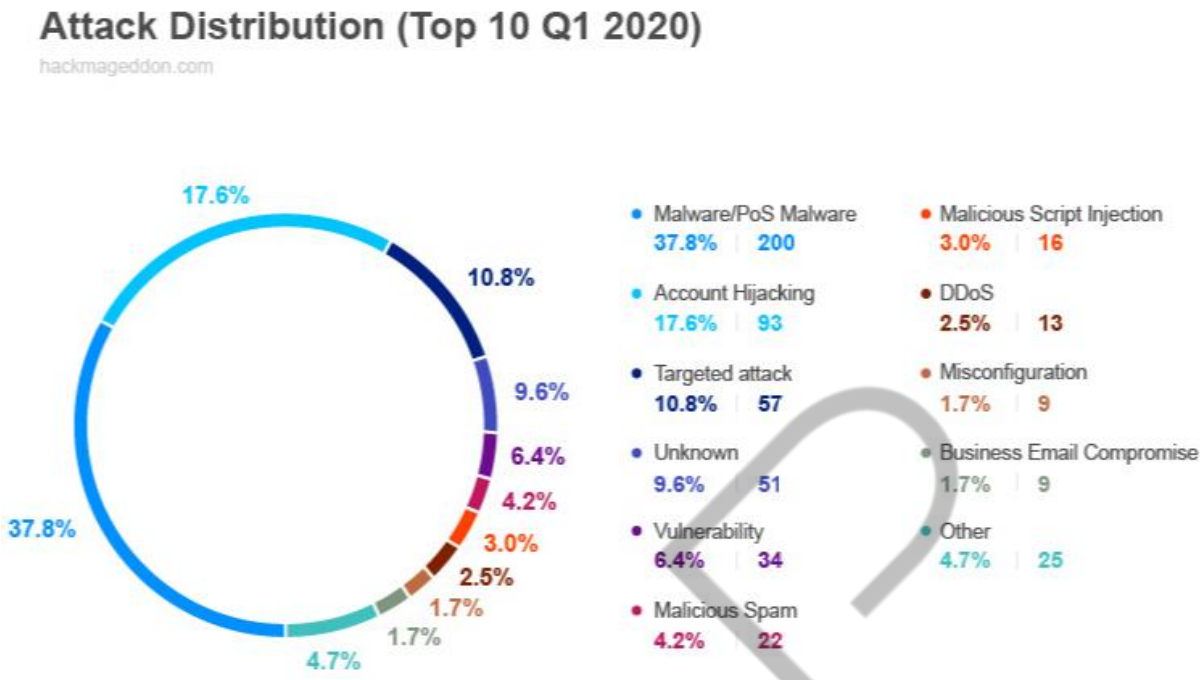

Figura 1.5 – Principais vetores de ataque
Fonte: Hackmageddon (2020)

Pode-se observar com base no gráfico (Figura Principais vetores de ataque), que os vetores de ataque mais evidentes são os *Malwares*/PoS *Malwares* (37,8%).

Logo em seguida, com 17,6%, vem o *Accounting Hijacking* (sequestro da conta), o qual consiste, em linhas gerais, das ações de um atacante com o objetivo de obter as credenciais de um usuário legítimo (por exemplo, *username* e senha de uma conta de e-mail ou computador) para a execução de atividades não autorizadas.

Os ataques direcionados (*Targeted Attacks*) surgem na terceira posição (10,8%), constituindo-se, basicamente, de ataques dirigidos a alvos específicos, como, por exemplo, uma dada instituição ou entidade.

Logo, pode-se concluir que, a partir de análises estatísticas adequadas a cada contexto, é possível identificar-se apropriadamente os principais vetores de ataque utilizados contra um alvo e, desta forma, contribuir para o desenvolvimento de estratégias e contramedidas de segurança, não apenas efetivas, mas também aderentes às necessidades de negócio.

Essencialmente, *Point-of-Sale malwares* constituem uma família específica de códigos maliciosos, cujos principais objetivos remetem à obtenção de informações relacionadas a transações financeiras, incluindo dados de cartões de crédito.

Para mais detalhes, visite:
https://www.trendmicro.com/vinfo/us/security/definition/PoS-(point-of-sale)-malware

1.4 Motivação dos ataques e o enquadramento jurídico

Não obstante, também a identificação da motivação dos ataques é de grande importância, dentre outras razões, dada a necessidade de mitigação dos riscos aos quais um alvo poderá vir a ser exposto. Além disso, ainda a necessidade de constante aprimoramento das políticas de segurança da informação vigentes, no caso dos ambientes corporativos.

No gráfico (Figura Motivações de ataque), são identificados os principais motivadores dos ataques observados em 2020.

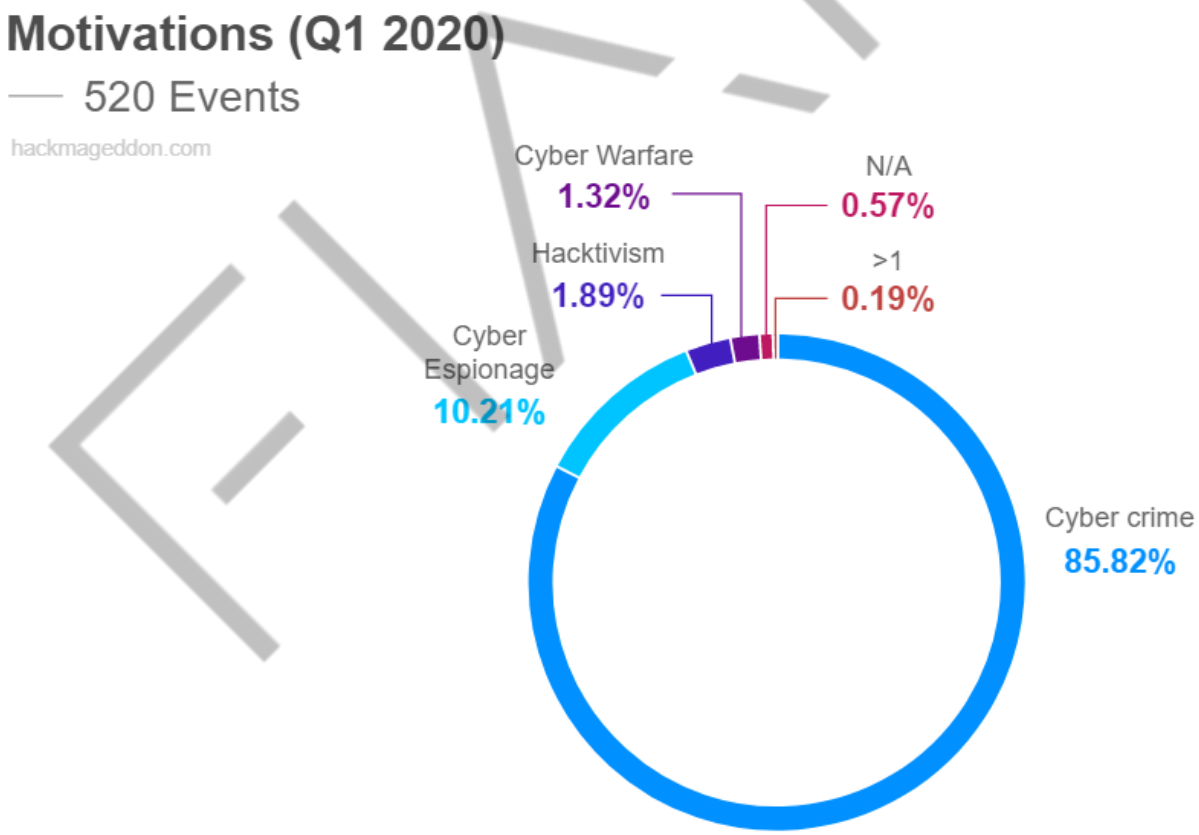

Figura 1.6 – Motivações de ataque
Fonte: Hackmageddon (2020)

Em relação às motivações de ataque, observa-se 85,82% dos ataques registrados tiveram como motivação a prática de cybercrimes: simplificadamente, quando sistemas ou recursos informáticos são utilizados como meio, ou alvo, para a

prática de condutas antijurídicas, tendo-se o uso de *ransomwares* como um exemplo de uma das mais disseminadas destas práticas.

Especialistas afirmam haver, ao menos, três crimes envolvidos em um ataque por *ransomware*: extorsão (Art. 158, Decreto Lei nº 2.848 – 07/12/1940), crime de ameaça (Art. 147, Decreto Lei nº 2.848 – 07/12/1940) e, no caso de um indivíduo, o delito de invasão de dispositivo informático (Art. 154-A, Lei nº 12.737 – 20/12/2012).

Hacktivismo é o ato de “piratear”, ou invadir, um sistema informático por motivos políticos ou sociais. O hacktivista utiliza as mesmas técnicas e ferramentas de um *hacker*, porém, com a finalidade de interromper serviços e chamar a atenção para uma causa política ou social, como observado na Figura Ataque ao site da Assembleia Legislativa (RN).

Figura 1.7 – Ataque ao site da Assembleia Legislativa (RN)
Fonte: al.rn.gov.br (2017)

Por exemplo, um hacktivista poderia deixar uma mensagem bem visível em um website com grande volume de acessos e que defenda algum ponto de vista do qual ele diverge; ou ainda, poderia lançar um ataque de negação de serviço (*denial of service* – DoS) contra este website a fim de tirá-lo do ar, caso ele não se retratasse em relação a este ponto de vista.

Figura 1.8 – Ataque DDoS derruba serviço do Telegram
Fonte: G1 (2020)

Mesmo motivado por diferentes razões, os resultados práticos das ações do hacktivista seriam os mesmos: na primeira hipótese, a desfiguração do website *(defacement)*; e na segunda, a indisponibilidade deste (DoS).

Em função das circunstâncias sob as quais tais ações foram praticadas, diferentes dispositivos previstos na legislação brasileira poderão ser aplicados para fins de encaminhamento e tratativa legal destas ações.

Neste aspecto, vale destacar as palavras do ex-ministro Sepúvelda Pertence - Primeira Turma, julgado em 22/09/1998: "... a invenção da pólvora não reclamou redefinição do homicídio para tornar explícito que nela se compreendia a morte dada

a outrem mediante arma de fogo...”, o que significa dizer, de forma bem simplificada, que, mesmo sendo os cybercrimes posteriores à edição de maior parte da lei, esta ainda pode ser aplicável para julgá-los.

REFERÊNCIAS

AUSTCYBER. **SCP - Chapter 1 - The global outlook for cyber security**. [s.d.]. Disponível em: <https://www.austcyber.com/resources/sector-competitiveness-plan/chapter1>. Acesso em: 21 abr. 2020.

CANAL TECH. Entenda os ciberataques feitos pelo ransomware WannaCry na última sexta-feira (12). 2017. Disponível em: <https://canaltech.com.br/hacker/entenda-os-ciberataques-feitos-pelo-ransomware-wannacry-na-ultima-sexta-12-93724/>. Acesso em: 21 abr. 2020.

CERT.BR. **Sobre o CERT.br**. 2020. Disponível em: <https://www.cert.br/sobre/>. Acesso em: 21 abr. 2020.

_____. **Incidentes reportados ao CERT.br – janeiro a dezembro de 2016.** 2017. Disponível em: <https://www.cert.br/stats/incidentes/2016-jan-dec/total.html>. Acesso em: 21 abr. 2020.

CRAIGEN, D.; DIAKUN-THIBAULT, N.; PURSE, R. Defining Cybersecurity. **Tim Review,** 2014. Disponível em: <https://timreview.ca/sites/default/files/article_PDF/Craigen_et_al_TIMReview_October2014.pdf>. Acesso em: 20 abr. 2020.

DELOITTE. **Hacktivism:** a defender's playbook. 2016. Disponível em: <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/risk/us-aers-hacktivism.pdf>. Acesso em: 20 abr. 2020.

FERRARI, Bruno. Ransomware: o crime quase perfeito. **Época,** 30 mar. 2017. Disponível em: <http://epoca.globo.com/tecnologia/experiencias-digitais/noticia/2017/03/ransomware-o-crime-quase-perfeito.html>. Acesso em: 21 abr. 2021.

FERREIRA, Lóren Pinto. **Os "crimes de informática" no Direito Penal Brasileiro**. 2013. Disponível em: <http://www.egov.ufsc.br/portal/conteudo/os-%E2%80%9Ccrimes-de-inform%C3%A1tica%E2%80%9D-no-direito-penal-brasileiro>. Acesso em: 21 abr. 2020.

FISCHER, Eric A. **Cybersecurity issues and challenges:** in brief. 2016. Disponível em: <https://fas.org/sgp/crs/misc/R43831.pdf>. Acesso em: 21 abr. 2020.

GARTNER. **Gartner Forecasts Enterprise Security and Risk Management Spending in MENA to Grow 11% in 2020**. 28 out. 2019. Disponível em: <https://www.gartner.com/en/newsroom/press-releases/2019-10-28-gartner-forecasts-enterprise-security-and-risk-manage>. Acesso em: 21 abr. 2020.

G1. **Telegram enfrenta 'poderoso ataque de negação de serviço'**. 12 jun. 2019. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2019/06/12/telegram-diz-estar-sob-poderoso-ataque-de-negacao-de-servico.ghtml>. Acesso em: 21 abr. 2020.

MALWAREBYTES. **Ransom.WannaCryCrypt**. 2017. Disponível em: <https://blog.malwarebytes.com/detections/ransom-wannacrypt/>. Acesso em: 21 abr. 2020.

ROVER, Tadeu. Internet facilita crimes e dificulta investigação, estimulando a impunidade. **Revista Consultor Jurídico,** 5 fev. 2017. Disponível em: <http://www.conjur.com.br/2017-fev-05/entrevista-daniel-burg-especialista-crimes-virtuais>. Acesso em: 21 abr. 2020.

TECHNET MICROSOFT**. Stop using SMB1**. 2016. Disponível em: <https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>. Acesso em: 21 abr. 2020.

TERRA. **US$ 6 trilhões até 2021: segurança move investimentos e LGPD é um dos impulsos**. 1 nov. 2019. Disponível em: <https://www.terra.com.br/noticias/dino/us-6-trilhoes-ate-2021-seguranca-move-investimentos-e-lgpd-e-um-dos-impulsos,1009c1869ab026e2e65753c685bd9984uerdbjvr.html>. Acesso em: 21 abr. 2020.

GLOSSÁRIO

Malware	Abreviatura de *malicious software*, refere-se a um de tipo software destinado a infiltrar-se em sistemas computacionais alheios de forma ilícita com o objetivo de causar danos, promover alterações ou “roubar” informações armazenadas neste sistema.
Ransomware	É um tipo de *malware* que tem como objetivo tornar os dados armazenados em um equipamento inacessíveis, normalmente por intermédio de criptografia, exigindo pagamento de resgate (*ransom*), geralmente em bitcoins, para restabelecimento do acesso ao usuário.
Bitcoin	Bitcoin é uma criptomoeda e sistema online baseado em protocolo de código aberto que é independente de qualquer autoridade central.
Bootloader	Programa especificamente desenvolvido para permitir a inicialização do sistema operacional. Normalmente, apresenta múltiplos estágios nos quais vários outros pequenos programas se complementam em sequência até a carga efetiva do sistema operacional.
Dropper	É o “inoculador”, parte do software que instala o código malicioso no sistema.
Payload	Refere-se à parte realmente útil dos dados, por exemplo, após descartados cabeçalhos e metadados ou, ainda, a parte maliciosa do código de um *malware*.
Phishing	Técnicas utilizadas para a obtenção de informações, ou cooperação, da vítima de maneira fraudulenta.