O impacto econômico do crime cibernético: sem indícios de desaceleração

O crime cibernético custa ao mundo quase US$ 600 bilhões atualmente, 0,8% do PIB global, segundo um novo relatório do Centro de Estudos Estratégicos e Internacionais (CSIS) e da McAfee. Programado para ser lançado em 21 de fevereiro, o relatório "The Economic Impact of Cybercrime: No Slowing Down" (O impacto econômico do crime cibernético: sem indícios de desaceleração) dá prosseguimento ao popular relatório de 2014 que quantificou as perdas globais por volta de US$ 500 bilhões, 0,7% da receita global.

Colocando a estatística mais recente em perspectiva, isso é mais que a receita de quase todos os países, salvo algumas exceções. Quando examinamos o custo do crime cibernético em relação à economia mundial da Internet (US$ 4,2 trilhões em 2016), o crime cibernético pode ser encarado como um imposto de 14% sobre o crescimento[1].

No ranking dos crimes com impacto global, o crime cibernético está em terceiro lugar, atrás de corrupção governamental e drogas, como um flagelo econômico global[2] e as razões disso são as seguintes:

- **Ele afeta a todos:** quase dois terços das pessoas que utilizam serviços on-line (mais de dois bilhões de indivíduos) tiveram seus dados pessoais roubados ou comprometidos.
- **Risco baixo e retorno elevado:** a probabilidade de ser preso e condenado é baixa. Nenhum dos perpetradores das violações mais notórias foi processado. As autoridades policiais estão se empenhando cada vez mais, mas muitos criminosos cibernéticos operam fora de suas jurisdições.

O relatório atribui o crescimento de US$ 100 bilhões do crime cibernético à rápida adoção de novas tecnologias por parte dos criminosos, à facilidade de se entrar no crime cibernético (incluindo o número crescente de centros de crime cibernético) e à sofisticação financeira cada vez maior dos criminosos cibernéticos de alto nível.

Quando examinamos o custo do crime cibernético em relação à economia mundial da Internet (US$ 4,2 trilhões em 2016), o crime cibernético pode ser encarado como um imposto de 14% sobre o crescimento[1].

Conecte-se conosco

Principais descobertas

- O ransomware é a ferramenta de crime cibernético de mais rápido crescimento, com mais de 6.000 mercados criminosos on-line vendendo produtos e serviços de ransomware e com a popularidade cada vez maior do "ransomware como serviço".
- O "crime cibernético como serviço", em geral, tornou-se mais sofisticado, com mercados emergentes oferecendo uma ampla gama de ferramentas e serviços, tais como kits de exploração, malware personalizado e aluguel de redes de bots.
- A ameaça de ação policial levou muitas negociações do crime cibernético para a Dark Web, onde o anonimato e as criptomoedas (por exemplo, Tor e Bitcoin) dificultam a identificação dos envolvidos.
- O malware popular na Dark Web inclui injeções de Web, kits de exploração e "infraestrutura como serviço", como hospedagem confiável e aluguel de redes de bots.
- O roubo de contas de propriedade intelectual responde por pelo menos um quarto do custo do crime cibernético e, quando envolve tecnologia militar, também acarreta riscos à segurança nacional.

Elementos do crime cibernético

O relatório não tenta medir o custo de toda atividade maliciosa na Internet, mas se concentra em criminosos que obtêm acesso ilícito ao computador ou rede da vítima. Os elementos do crime cibernético identificados pelos autores são:

- A perda de IPs ou informações confidenciais corporativas
- Fraude on-line e crimes financeiros, frequentemente em decorrência do roubo de informações de identificação pessoal
- Manipulação financeira direcionada a empresas cotadas em bolsa
- Custos de oportunidades, incluindo interrupção de produção e de serviços, e redução da confiança em atividades on-line
- O custo de se proteger redes, adquirir seguros cibernéticos e pagar pela recuperação de ataques cibernéticos
- Danos à reputação e riscos de responsabilidade jurídica da empresa afetada e sua marca

A ameaça de mais rápido crescimento

O ransomware visa a todos: de grandes corporações a simples consumidores. Nem todas as vítimas pagam o resgate, mas muitas o fazem.

Segundo o FBI, US$ 209 milhões foram pagos em resgate no primeiro trimestre de 2016, contra US$ 24 milhões em todo o ano de 2015.[3] Eis a razão por trás desse crescimento explosivo do ransomware[4]:

- A disponibilidade de kits de ransomware no submundo da Web, com mais de 6.000 mercados criminosos on-line oferecendo um total de 45.000 produtos e serviços diferentes
- Plataformas de "ransomware como serviço" (RaaS) que oferecem aos autores de ransomware a oportunidade de ampliar o seu alcance compartilhando seu código com a comunidade criminosa mediante uma taxa e recebendo uma parte dos pagamentos de resgate obtidos

No ranking dos crimes com impacto global, o crime cibernético está em terceiro lugar, atrás de corrupção governamental e drogas, como um flagelo econômico global.[2]

- Worms de ransomware, como o WannaCry, que podem se espalhar pela rede e travar vários computadores

Outras tendências que deverão surgir no ransomware são capacidades de vazamento de dados e ataques contra dispositivos móveis e da Internet das coisas (IoT), que não costumam ter defesas fortes.

O crime cibernético ao redor do mundo

O relatório avalia o crime cibernético na América do Norte, na Europa e na Ásia Central, no leste da Ásia e no Pacífico, no sul da Ásia, na América latina e no Caribe, na África subsaariana e na região do Oriente Médio e Norte da África (MENA). As descobertas do relatório sugerem que o custo do crime cibernético nas diversas regiões varia, dependendo do nível da maturidade da segurança cibernética de cada país, o qual é medido em relação aos seguintes indicadores fundamentais: medidas jurídicas, medidas técnicas, medidas organizacionais, construção de capacitação e cooperação.

Os resultados foram categorizados assim: países avançados com economias digitais e segurança cibernética consolidada, países intermediários com suas economias digitais e segurança cibernética em evolução e países cujas iniciativas em economia digital e segurança cibernética estão nos estágios iniciais. Como se pode esperar, nações mais prósperas sofrem perdas maiores com o crime cibernético. Os países mais fortemente atingidos são os intermediários.

- **Alemanha:** o país é sede da economia de Internet clandestina mais sofisticada da União Europeia.
- **Brasil:** é a segunda fonte de ataques cibernéticos e o terceiro alvo mais atingido.
- **Emirados Árabes Unidos:** é o segundo país mais visado do mundo, com um custo de crime cibernético estimado em US$ 1,4 bilhão por ano.
- **Japão:** antes protegido do crime cibernético pela barreira do idioma e pela falta de infraestrutura para lavagem de dinheiro, o Japão está tendo um aumento, especialmente em ataques contra bancos.
- **Reino Unido:** a fraude on-line e o crime cibernético perfazem quase metade de todos os crimes, chegando a mais de 5,5 milhões de violações por ano.

Conclusão e recomendações

Embora a análise feita pela CSIS e pela McAfee tenha se concentrado nos custos do crime cibernético, existem várias providências que organizações e países podem tomar como uma maneira de reduzir perdas:

- A implementação consistente de medidas de segurança essenciais, como atualizações e correções regulares do software de segurança e arquiteturas de segurança abertas, juntamente com investimentos em defesas avançadas que se estendam dos dispositivos endpoint à nuvem

O relatório atribui o crescimento de US$ 100 bilhões do crime cibernético à rápida adoção de novas tecnologias por parte dos criminosos, à facilidade de se entrar no crime cibernético (incluindo o número crescente de centros de crime cibernético) e à sofisticação cada vez maior dos criminosos cibernéticos de alto nível.

- Maior cooperação internacional entre as autoridades policiais dos países e o setor privado, bem como investimentos em mais recursos para investigação, especialmente entre nações em desenvolvimento
- Modernização dos processos atuais, como o Mutual Legal Assistance Treaty (MLAT), que permite aos governos pedir a ajuda de outros governos em investigações de crimes cibernéticos e coleta de evidências
- Coleta de dados agregados mais eficiente por parte de autoridades nacionais
- Padronização de informações sobre ameaças e coordenação dos requisitos de segurança cibernética para incrementar a segurança em setores críticos, como o financeiro
- Adoção acelerada de tratados como a Convenção de Budapeste, que estabelece as responsabilidades dos países e termos de cooperação e policiamento do crime cibernético
- Imposição de penalidades temporárias ou outras consequências aos governos que falharem no combate ao crime cibernético

Sobre a McAfee

A McAfee é uma das maiores empresas independentes de segurança cibernética do mundo. Inspirada pelo poder do trabalho em equipe, a McAfee cria soluções que tornam o mundo um lugar mais seguro para as empresas e os consumidores. **www.mcafee.com/br**

1. https://www.bcg.com/documents/file100409.pdf
2. www.imf.org/external/pubs/ft/sdn/2016/sdn1605.pdf
3. Max Metzger. “FBI says Ransomware soon becoming a billion dollar business.” (O FBI affirma que o ransomware logo se tornará um negócio de um bilhão de dólares), SC Media UK, 10 de janeiro de 2017. https://www.scmagazineuk.com/fbi-says-ransomware-soon-becoming-a-billion-dollar-business/article/630615/
4. “Relatório do McAfee Labs sobre ameaças,” McAfee, dezembro de 2017

McAfee
Together is power.

Av. Nações Unidas, 8.501 – 16º andar
Pinheiros – São Paulo – SP
CEP 05425-070, Brasil
+(11) 3711-8200
www.mcafee.com/br

McAfee e o logotipo da McAfee são marcas comerciais ou marcas registradas da McAfee, LLC ou de suas afiliadas nos EUA e em outros países. Outros nomes e marcas podem ser propriedade de terceiros. Copyright © 2018 McAfee, LLC. 3747_0218
FEVEREIRO DE 2018