Lidando com os riscos de segurança digital durante a crise da COVID-19

3 de abril de 2020

Mensagens principais

- Os riscos de segurança digital estão aumentando ao passo que atores mal-intencionados se aproveitam da epidemia do coronavírus (COVID-19). Fraudes e campanhas de *phishing* relacionadas ao coronavírus estão em alta. Também existem casos de sequestro de dados (*ransomware*) e ataques distribuídos de negação de serviço (*distributed denial of service*, DDoS) direcionados a hospitais.
- Indivíduos e empresas devem exercer cautela com comunicações relacionadas ao coronavírus e usar medidas apropriadas de "higiene" em relação à segurança digital (como, por exemplo, aplicação de *patches*, uso de senhas seguras e variadas, realização de cópias de segurança regulares etc.).
- É essencial que os que os governos ampliem esforços de conscientização, monitorem o cenário de ameaças e publiquem diretrizes de fácil acesso para a higiene de segurança digital, em particular para grupos vulneráveis, como idosos e pequenas e médias empresas (PMEs). Os governos também devem cooperar com todas as partes interessadas relevantes, inclusive para fornecer assistência aos operadores de atividades críticas, como hospitais, conforme apropriado

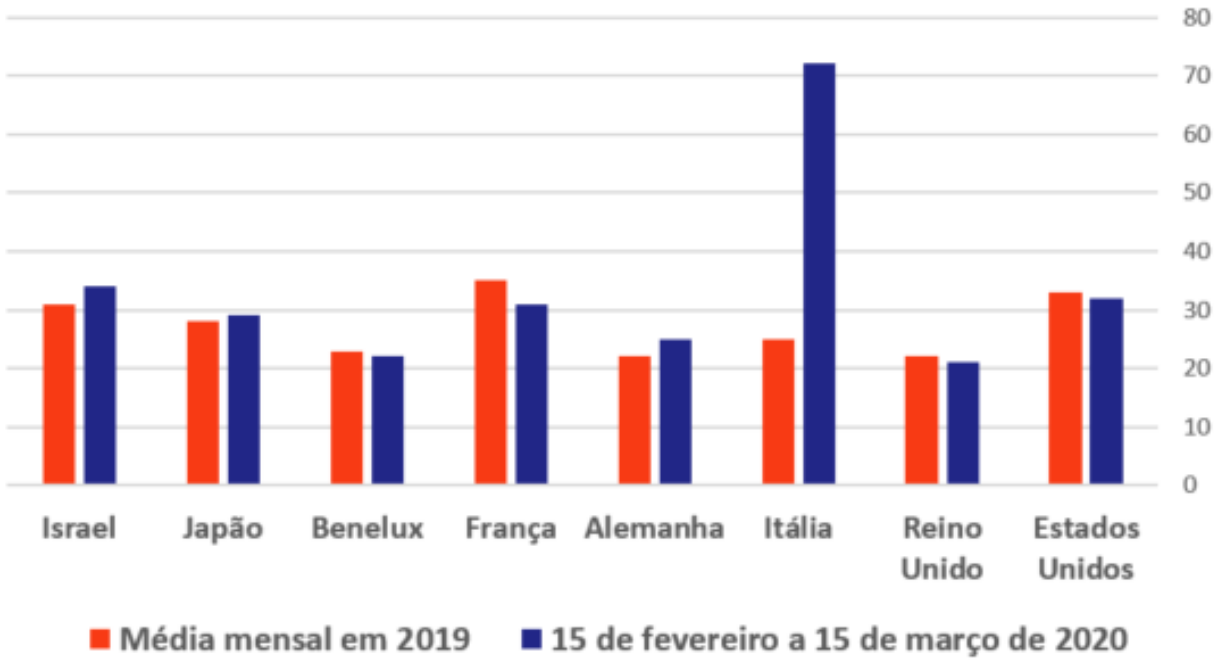
O risco à segurança digital está aumentando à medida que a crise do coronavírus (COVID-19) se desenrola

Atores mal-intencionados estão se aproveitando da epidemia para tornar seus ataques mais bem-sucedidos. Desde fevereiro de 2020, houve um aumento nas campanhas de *phishing*[1] que usam conteúdo relacionado à COVID-19, incluindo:

- e-mails com alusão ao coronavírus no campo descritor de assunto ou como nome de arquivo em anexo
- e-mails ou SMS falsamente atribuídos ao governo da Austrália e do Reino Unido
- e-mails em que os remetentes se passam por líderes ou instituições, como a Organização Mundial da Saúde
- e-mails, links ou aplicativos dissimulando iniciativas legítimas.

Uma empresa de segurança descobriu que as empresas italianas registraram um aumento nos ataques de *phishing* em março de 2020. Na Itália, uma campanha de *phishing* com o tema COVID-19 atingiu mais de 10% das organizações através de um e-mail cujo teor convidava os destinatários a abrirem um anexo malicioso.

Figura 1. **Pico de ataques de *phishing* na Itália**



Fonte: Cynet

O painel interativo da Universidade Johns Hopkins, que rastreia as infecções por coronavírus, foi replicado pelos cibercriminosos para espalhar um programa malicioso (*malware*) de roubo de senhas. O kit para o programa malicioso está à venda em fóruns ilegais na Internet obscura (*dark web*) por 200 dólares.

Uma campanha de e-mail direcionada aos setores de saúde e manufatura nos Estados Unidos no início de março de 2020 abusou de um projeto legítimo de computação distribuída para pesquisa de doenças. O e-mail solicitava aos destinatários que instalassem um anexo para ajudar a encontrar uma cura para o coronavírus. O anexo continha um programa malicioso que roubava credenciais e carteiras frias de criptomoeda (carteiras de criptomoeda armazenadas offline).

Os cibercriminosos também estão aproveitando a popularidade de ferramentas usadas para o tele-trabalho, como Zoom para videoconferência. Os especialistas detectaram campanhas de *phishing* com anexos maliciosos contendo a palavra "zoom" no nome do arquivo e mais de 1 700 novos nomes de domínio com o termo foram registrados desde o início da pandemia, provavelmente para usos maliciosos. Outros exemplos incluem novos domínios dissimulados como o site legítimo do Google Classroom.

Também houve casos de ataque de *ransomware*[2] e DDoS[3] direcionados a atividades essenciais como hospitais na França, Espanha e República Tcheca, entre outros.

- O segundo maior hospital da República Tcheca, o Hospital Universitário de Brno, foi atacado nos dias 12 e 13 de março, causando a queda imediata dos computadores em pleno surto do coronavírus. O hospital, que abriga uma das maiores instalações de testes COVID-19 do país, foi forçado a suspender as operações e realocar pacientes graves para outros hospitais.
- O hospital universitário que opera em Paris e arredores (AP-HP) enfrentou um ataque DDoS de uma hora de duração no domingo, dia 22 de março, paralisando dois de seus sites de Internet. O ataque não afetou a infraestrutura de saúde.
- Na Espanha, um ataque de *ransomware* foi lançado contra instituições de saúde em 23 de março de 2020.
- Nos Estados Unidos, o departamento governamental Health and Human Services (HHS) enfrentou um ataque DDoS em 15 de março de 2020.
- Na França, o sistema de informações do governo local de Marselha enfrentou um ataque de *ransomware* em 14 de março de 2020, véspera das eleições locais. Todos os aplicativos voltados ao público, assim como vários sistemas internos, ficaram offline.

Os cibercriminosos confiam na probabilidade de que indivíduos e organizações caiam mais facilmente em fraudes ou paguem resgates em períodos de estresse e crise, em particular aqueles que não possuem boas práticas de segurança digital ou que enfrentam perturbações no nível organizacional. **No entanto, como suas técnicas de ataque e programas maliciosos não são novos, a aplicação de uma "higiene" básica de segurança digital é uma maneira eficaz de mitigar esses ataques.**

Os países já estão tomando medidas para combater o aumento dos riscos de segurança digital

Nos países da OCDE, as agências governamentais responsáveis pela segurança digital estão respondendo à crise, através da conscientização, monitoramento do cenário de ameaças, prestação de assistência quando apropriado e cooperação com todas as partes interessadas, inclusive em nível internacional.

- A agência norte-americana Cyber and Infrastructure Security Agency (CISA) criou em seu site uma nova seção inteiramente dedicada aos riscos de segurança relacionados à crise COVID-19 (www.cisa.gov/coronavirus). A página inclui alertas e recomendações sobre campanhas de fraude

e *phishing* relacionadas à COVID-19, orientações sobre tele-trabalho e uma nota sobre gerenciamento de riscos.

- A Comissão Europeia, ENISA, CERT-EU e Europol divulgaram uma declaração em 20 de março, pontuando a sua cooperação no rastreamento de atividades maliciosas relacionadas à COVID-19, no alerta de suas respectivas comunidades e na proteção de cidadãos confinados.
- O Centro Canadense de Segurança Cibernética publicou um alerta avaliando que a pandemia COVID-19 representa um elevado risco para a segurança digital das organizações de saúde canadenses envolvidas na resposta nacional à pandemia. O Centro recomenda que essas organizações continuem vigilantes e dediquem tempo para assegurar que as melhores práticas em defesa cibernética foram engajadas. O centro dedica-se, ainda, a conscientizar as demais organizações no Canadá.
- À luz das evidências encontradas durante a resolução do incidente do Hospital de Brno, o Escritório Nacional Tcheco de Segurança Cibernética e da Informação (NÚKIB) ordenou que algumas entidades de saúde selecionadas adotassem medidas para melhorar a segurança dos seus principais sistemas de tecnologia e informação. O NÚKIB ofereceu consultas e apoio a essas entidades.

Além dessas medidas, muitas empresas, bem como grupos industriais e profissionais, têm informado o público sobre os riscos à segurança digital relacionados à crise da COVID-19. Foram criados serviços de atendimento (on-stop shop) e bibliotecas de recursos. Iniciativas também foram criadas para fornecer conselhos sobre tópicos específicos, como segurança no tele-trabalho.

Principais recomendações

Incentiva-se o público em geral a adotar medidas de segurança pessoal para proteger a si mesmo e aos outros:

- Tratar com cautela todas as comunicações relacionadas à crise do coronavírus, mesmo que indiretamente (como pelo uso de ferramentas de tele-trabalho), incluindo e-mails, mensagens nas mídias sociais, links, anexos e SMS.
- Manter computadores, smartphones e outros dispositivos atualizados com os *patches* de segurança mais recentes.
- Realizar cópias de segurança (*backup*) de conteúdo regularmente, especialmente de dados críticos.

Os governos e outras partes interessadas são incentivados a:

- Promover maior conscientização sobre os crescentes riscos de segurança digital relacionado à COVID-19, principalmente associados a campanhas de *phishing*, *ransomware* e ataques *DDoS*. Fornecer orientações práticas e ferramentas (pôsteres, diagramas, estudos de caso) que possam ser facilmente absorvidos por outras partes interessadas.
- Publicar informações e diretrizes para organizações do setor público, empresas e indivíduos, inclusive sobre ameaças emergentes e boas práticas de higiene de segurança digital e tele-trabalho.
- Apoiar grupos vulneráveis, principalmente idosos e PMEs, tendo em vista que eles provavelmente passarão mais tempo conectados à Internet, mas podem estar menos conscientes das ameaças.

- Monitorar o cenário de ameaças (*phishing*, *ransomware* etc.) e alertar as comunidades-alvo.
- Incentivar os operadores de atividades críticas, em particular no setor da saúde, a aumentar o nível de segurança digital e fornecer assistência específica, conforme apropriado, de acordo com a *Recomendação do Conselho sobre Segurança Digital de Atividades Críticas* (OCDE, 2019).
- Facilitar a cooperação e o intercâmbio de informações sobre riscos à segurança digital entre as principais partes interessadas, nacional e internacionalmente, e em nível setorial (como, por exemplo na área de saúde).

Leitura adicional

OCDE (2019), Recomendação do Conselho sobre Segurança Digital de Atividades Críticas, OCDE, Paris, https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0456 .

OCDE (2015), Recomendação do Conselho sobre Gerenciamento de Riscos de Segurança Digital para *Prosperidade Econômica e Social* , OCDE, Paris, https://www.oecd.org/sti/ieconomy/digital-security-risk-management.pdf .

A OCDE está compilando dados, informações, análises e recomendações sobre os desafios de saúde, econômicos, financeiros e sociais colocados pelo impacto do coronavírus (COVID-19).

Visite nossa página dedicada para obter um conjunto completo de informações relacionadas ao coronavírus.

Notas

← 1. Phishing é a prática fraudulenta de enviar e-mails que pretendem ser de organizações respeitáveis para atrair indivíduos a revelar dados pessoais, fornecer credenciais, abrir anexos maliciosos etc.

← 2. O ransomware é um tipo de malware que geralmente criptografa os dados dos usuários e ameaça bloquear o acesso aos dados, a menos que um resgate seja pago.

← 3. Um ataque DDoS inunda o serviço de um alvo (por exemplo, um site) com solicitações de um grande número de endereços IP, resultando na indisponibilidade do serviço para usuários legítimos, com duração de alguns minutos a dias inteiros.

Publicado originalmente pela OCDE sob o título: *Dealing with digital security risk during covid-19.* Traduzido com o apoio da Delegação do Brasil na OCDE. Os textos oficiais são os textos em inglês e/ou francês. A qualidade da tradução e sua coerência com o texto no idioma original são de exclusiva responsabilidade da Delegação do Brasil na OCDE.