Ransomware e COVID-19: a necessidade da alfabetização digital

Eliezer de Souza Batista Junior
Doutorando em Ciências Militares pelo PPGCM/ECEME
Henrique Ribeiro da Rocha
Mestrando em Ciências Militares pelo PPGCM/ECEME
Breno Pauli Medeiros
Mestre e Doutorando em Ciências Militares pelo PPGCM/ECEME.
Prof. Dr. Luiz Rogério Franco Goldoni
Professor do PPGCM/ECEME

Por conta dos altos índices de contágio, a pandemia de COVID-19 demanda medidas de contenção, dentre elas, o isolamento social, que vêm modificando a forma de viver da sociedade nas últimas semanas. Isso fez com que várias atitudes que eram realizadas presencialmente tivessem que ser adaptadas ao mundo digital, como trabalhos, compras e entretenimento (PERES; ROBORTELLA, 2020). Essa adaptação do estilo de vida trouxe à tona vulnerabilidades em termos de segurança da informação, aproveitadas por cibercriminosos objetivando vantagens econômicas (PORTER, 2020). Uma dessas formas é o *ransomware*.

Após a eclosão da COVID-19, um ataque massivo de *malwares* ocorreu na Internet, tema abordado preliminarmente no artigo "Vetores Cibernéticos da Pandemia de COVID-19", publicado neste espaço. Conforme o texto, uma das ações foi direcionada ao Hospital Universitário de Brno, na República Tcheca, no dia 13 de março de 2020 (BATISTA JUNIOR et al, 2020). Como a investigação ainda está em curso, as autoridades[1] não anunciaram todos os detalhes do episódio. Entretanto, indícios mostram que por volta das 02:00 AM um funcionário do hospital sofreu um ataque de engenharia social, ao baixar um anexo enviado ao seu e-mail (NEWMAN, 2020). Esse anexo, provavelmente, estava infectado com um tipo de *malware*, chamado RAT, que proporciona controle efetivo da máquina aos criminosos. A partir desse ponto de acesso, o vírus se espalha pela rede em busca dos dispositivos que possam lhe trazer mais benefícios[2].

O efeito do *ransomware* propriamente dito inicia-se nessa fase, ao criptografar dados com uma chave. No caso do hospital de Brno, retirou-se a capacidade de transferir dados e informações clínicas de sistemas separados para um banco de dados central (ARBULU, 2020). Geralmente, os arquivos só são decriptografados mediante o pagamento de resgate em criptomoedas[3] (como o Bitcoin) que são mais difíceis de serem rastreadas (GARRET, 2020). No caso, o hospital não pagou pelo resgate e, às 08:00 AM, funcionários tiveram que desligar todos os aparelhos, transferir os enfermos e refazer as pesquisas que estavam em andamento (SCHWARTZ, 2020). A maternidade e o hospital infantil também foram afetados. Além disso, o grupo que o atacou disponibilizou os dados dos pacientes em páginas abertas (COMPUTINGNEWS, 2020).

Esse ataque gerou grande comoção na comunidade de Tecnologia da Informação e Comunicação; a ação foi repudiada em vista do avanço da pandemia. Em consequência, um dos principais grupos cibercriminosos que exploram o *ransomware* (Maze) explicou em suas páginas que não atua contra instituições que trabalham para salvar vidas (SCHWARTZ, 2020). Disseram ainda que "o foco iria mudar" e que não haveria ataques a empresas de assistência médica até o término da pandemia (WINDER, 2020).

Os cibercriminosos passaram a centrar seus esforços no cidadão comum possuidor de *smartphones*. Grupos desenvolveram o vírus COVIDLock (HARAN, 2020), que se instalava mediante o download do software COVID-19Tracker, disponível para o sistema Android[4]. Assim, criminosos se valiam de uma ferramenta (supostamente legítima, por estar em plataforma supostamente confiável) que permitia verificar o avanço do novo coronavírus no mundo, por meio de um mapa. Ao ser instalado, o aplicativo também executava um *ransomware* – metodologia conhecida como Cavalo de Tróia[5] (TELESÍNTESE,

[1] Neste caso, as autoridades que anunciaram o ataque foram o Escritório Nacional Tcheco para Cibernética e Segurança da Informação (NÚKIB) e o diretor do hospital Jaroslav Štěrba (NEWMAN, 2020).

[2] Os servidores que têm mais benefícios em ataques são aqueles que contém banco de dados ou gerenciam processos considerados importantes.

[3] Criptomoedas são carteiras de dinheiro nas quais a transferência ocorre de forma que nenhum dado pessoal seja compartilhado. Geralmente, as informações sobre a transação não deixam rastros, o que dificulta que essa seja investigada posteriormente pela polícia (GARRET, 2017).

[4] Conforme Grustniy (2019), haveria vulnerabilidades no Google Play, uma vez que os verificadores de *malware* dessa loja virtual não são instantâneos.

[5] O Cavalo de Tróia usa mecanismo considerado fidedigno e nele embarca códigos para efetuar o ataque propriamente dito. Na história, o Exército de Tróia presenteou os Aqueus com um cavalo de madeira porque não conseguia adentrar na fortaleza aquiana. Dentro do cavalo, havia combatentes que saíram na madrugada e abriram os portões (SOHISTORIA). Da mesma forma, o *ransomware* é instalado dentro de um arquivo considerado normal para os padrões

64498.003462/2020-79

2020). O efeito é a modificação da senha de entrada do sistema Android e a exibição de uma mensagem para que o dono do *smarphone* pague um resgate que varia entre US$ 100 e US$ 250.

Apesar de dizerem que não iriam atacar instituições de saúde, o *Affordacare Urgent Care*, que trabalha com diagnósticos de exames do COVID-19, foi atacado pelo grupo Maze. Essa empresa não pagou pelo resgate, pois possuía sistema de *backup*, que permitiu que os bancos de dados fossem restaurados. Entretanto, os dados de seus clientes foram expostos em um website (TRUTA, 2020).

Outro exemplo de utilização de *ransomware* durante a pandemia da COVID-19 ocorreu no *Campaign-Urbana Public Health District* (CUPHD), em Illinois, EUA. A autoria é atribuída ao grupo NetWalker, que batizou o *malware* com seu nome. Os criminosos se aproveitaram de vulnerabilidades de navegadores Internet Explorer desatualizados (WINDER, 2020) e criptografaram o Banco de Dados, inviabilizando o CUPHD operacionalmente. Ressalta-se que o grupo NetWalker não havia firmado acordo para não atacar instituições de saúde. O CUPHD tinha backup e não foi severamente afetado (NICHOLS, 2020).

Na contraposição desses ataques, há os sistemas defensivos. Conforme já mencionado no artigo "vetores cibernéticos da pandemia de COVID-19", empresas constituíram alianças para tentar mitigar os efeitos dos cibercriminosos, como ocorreu com a empresa C5 (BROWN, 2020). Mais um exemplo é a iniciativa do grupo *National Cyber Security Alliance* e seus parceiros que disponibilizaram uma biblioteca gratuita e atualizada contendo informações sobre golpes atuais, ameaças e auxílio em desastres cibernéticos (NSCA, 2020). Outra iniciativa defensiva é a assistência gratuita fornecida por empresas de segurança cibernética, como a Emsisoft, para o setor de saúde enquanto perdurar a pandemia (WINDER, 2020).

Destaca-se, também, o papel de grupos de engenharia reversa, sem fins lucrativos, que "dissecam" o *ransomware*. Um exemplo é o grupo *MalwareHunterTeam* que conseguiu detalhar o *modus operandi* do COVIDLock e do NetWalker[6]. As descobertas são expostas em sua conta do Twitter e são aproveitadas por grandes empresas para o desenvolvimento de vacinas[7] (MALWAREHUNTERTEAM, 2020).

Independente das ações empreendidas pelas empresas de segurança cibernética, o usuário é o maior responsável por evitar ataques virtuais. Como boas práticas ao alcance de todos, destacam-se: realizar backups (ARCSERVE, 2020), atualizar os sistemas operacionais sempre que possível; baixar softwares de repositórios[8] com idoneidade; não clicar em anexos ou links de e-mails; possuir ferramentas de segurança da informação (como antivírus e firewall) com credibilidade (ALVES, 2020); e, alertar familiares e pessoas próximas sobre essa conscientização.

Os ataques com *ransomware* continuarão com outros métodos, vetores e formas. Há de se melhorar a consciência sobre o tema de segurança cibernética. Um dos efeitos colaterais da pandemia, em decorrência da transposição de serviços cotidianos para plataformas digitais, pode ser o aumento da preocupação com a segurança cibernética, especialmente nas pessoas que eram reticentes na utilização do ciberespaço. Essa "alfabetização digital" é um dos caminhos para mitigar os vírus virtuais que se aproveitam da pandemia.

Rio de Janeiro – RJ, 30 de março de 2020.

Como citar este documento:

BATISTA JUNIOR, Eliezer de Souza et al. Ransomware e COVID-19: A necessidade da alfabetização digital. **Observatório Militar da Praia Vermelha**. Rio de Janeiro: ECEME. 2020.

Referências:

ALVES, Paulo. **Golpes com coronavírus distribuem malware no celular; como se proteger.** Disponível em: https://www.techtudo.com.br/listas/2020/03/golpes-com-coronavirus-distribuem-malware-no-celular-como-se-proteger.ghtml. Acessado em 27 de março de 2020.

ANSCOMBE, Tony. **Criminosos por trás do ransomware Maze reduzem ataques diante da crise causada pela Covid-19.** Disponível em: https://www.welivesecurity.com/br/2020/03/25/criminosos-por-tras-do-ransomware-maze-reduzem-ataques-diante-da-crise-causada-pela-covid-19/. Acessado em 27 de março de 2020.

normais, como um arquivo com extensão pdf, doc ou img (REAGAN, 2019).

[6] Tratado sob o nome técnico de "smcovid19.apk".

[7] A vacina pode ser incorporada a ferramenta de antivírus, impedindo, assim, que ocorra, novamente, a infecção nos mesmos cenários (RODRIGUES, 2015). Em alguns casos, a vacina pode corrigir os efeitos causados pelo *malware* nos computadores infectados.

[8] Locais que armazenam softwares. Podem ser sites ou servidores específicos.

ARBULU, Rafael. **Ciberataque faz hospital que tratava pacientes do coronavírus fechar as portas.** Disponível em: https://canaltech.com.br/seguranca/ciberataque-faz-hospital-que-tratava-pacientes-do-coronavirus-fechar-as-portas-161881/. Acessado em 20 de março de 2020.

ARCSERVE. **Esta é a proteção de dados contra ransomware mais inteligentes e simples.** Disponível em: https://www.arcserve.com/br/. Acessado em 27 de março de 2020.

BATISTA JUNIOR, Eliezer de Souza; MEDEIROS, Breno Pauli; ROCHA, Henrique Ribeiro da; GOLDONI, Luiz Rogério Franco. **Vetores Cibernéticos da Pandemia de COVID-19.** Disponível em: http://ompv.eceme.eb.mil.br/masterpage_assunto.php?id=194. Acessado em 30 de março de 2020.

COMPUTINGNEWS. **More ransomware groups threaten to publish data stolen data from non-payers.** Disponível em: https://www.computing.co.uk/news/4013035/ransomware-data-publication. Acessado em 27 de março de 2020.

GARRET, Filipe. **Entenda por que hackers pedem resgate de ataque ransomware em bitcoin.** Disponível em https://www.techtudo.com.br/noticias/2017/05/entenda-por-que-hackers-pedem-resgate-de-ataque-ransomware-em-bitcoin.ghtml. Acessado em 27 de março de 2020.GRUSTNIY, Leonid. **Verdadeiro ou falso: Todos os aplicativos da Google Play são seguros.** Disponível em: https://www.kaspersky.com.br/blog/google-play-malware/12318/. Acessado em 27 de março de 2020.

HARAN, Juan Manuel. **Campanhas de Malware e aproveitam do medo causado pelo coronavírus (COVID-19)**. Disponível em: https://www.welivesecurity.com/br/2020/03/19/campanhas-malware-aproveitam-medo-pelo-coronavirus-covid-19/. Acessado em 27 de março de 2020.

JORNALCONTÁBIL. **Alerta: identificado disseminação de malware usando a epidemia do Corona Vírus como isca.** Disponível em: https://www.jornalcontabil.com.br/https-www-jornalcontabil-com-br-alerta-identificado-disseminacao-de-malware-usando-a-epidemia-do-corona-virus-como-isca-amp/.

KASPERSKY. **Engenharia social – definição.** Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-social-engineering. Acessado em 18 de março de 2020.

MALWAREHUNTERTEAM. **Seen some more "smcovid19.apk" (no "beta" in filename anymore) files, here is a recent one.** Disponível em: https://twitter.com/malwrhunterteam/status/1242735514148634627. Acessado em 27 de março de 2020.

NEWMAN, Lily Hay. **Coronavirus Sets the Stage for Hacking Mayhem.** Disponível em: https://www.wired.com/story/coronavirus-cyberattacks-ransomware-phishing/. Acessado em 27 de março de 2020.

NICHOLS, Shaun. **Fresh virus misery for Illinois: Public health agency taken down by… web ransomware. Great timing, scumbags.** Disponível em: https://www.theregister.co.uk/2020/03/12/ransomware_illinois_health/. Acessado em 27 de março de 2020.

NSCA. **COVID-19 Security Resource Library.** Disponível em: https://staysafeonline.org/covid-19-security-resource-library/. Acessado em 30 de março de 2020.

PERES, Antonio Galvão; ROBORTELLA, Luiz Carlos Amorim. **Artigo: Coronavirus e relações de trabalho.** Disponível em: https://www.correiobraziliense.com.br/app/noticia/opiniao/2020/03/17/internas_opiniao,834746/artigo-coronavirus-e-relacoes-de-trabalho.shtml. Acessado em 18 de março de 2020.

PORTER, Sophie. **Cyberattack on Czech hospital forces tech shutdown during coronavirus outbreak.** Disponível em: https://www.healthcareitnews.com/news/europe/cyber attack-czech-hospital-forces-tech-shutdown-during-coronavirus-outbreak. Acessado em 27 de março de 2020.

REAGAN, Joseph. **O que é um Cavalo de Troia? É malware ou vírus?** Disponível em: https://www.avg.com/pt/signal/what-is-a-trojan. Acessado em 27 de março de 2020.

RODRIGUES, Diego. **Antivírus, Malware e Firewall... Você sabe a diferença de cada um?** Disponível em: https://www.microgate.info/single-post/2015/09/15/Antiv%C3%ADrus-Malware-e-Firewall-Voc%C3%AA-sabe-a-diferen%C3%A7a-de-cada-um. Acessado em 27 de março de 2020.

SCHWARTZ, Mathew J. **COVID-19 Complication:** Ransomware Keeps Hitting Healthcare. Disponível em: https://www.bankinfosecurity.com/covid-19-complication-ransomware-keeps-hitting-hospitals-a-13941. Acessado em 27 de março de 2020.

SOHISTORIA. **Guerra de Troia.** Disponível em: https://www.sohistoria.com.br/ef2/guerratroia/. Acessado em 27 de março de 2020.

TELESINTESE. **Arcserve alerta para Ransomware que explora medo ao COVID-19.** Disponível em: http://www.telesintese.com.br/arcserve-alerta-para-ransomware-que-explora-medo-ao-covid-19/. Acessado em 27 de março de 2020.

TRUTA, Filip. **Maze Ransomware Continues to Hit Healthcare Units amid Coronavirus (COVID-19) Outbreak.** Disponível em: https://securityboulevard.com/2020/03/maze-ransomware-continues-to-hit-healthcare-units-amid-coronavirus-covid-19-outbreak/. Acessado em 27 de março de 2020.

WINDER, Davey. **COVID-19 Vaccine Test Center Hit By Cyber Attack, Stolen Data Posted Online.** Disponível em: https://www.forbes.com/sites/daveywinder/2020/03/23/covid-19-vaccine-test-center-hit-by-cyber-attack-stolen-data-posted-online/#273db97718e5. Acessado em 27 de março de 2020.

WINDER, Davey. **Healthcare Workers Targeted By Dangerous New Windows Ransomware Capaign Using Coronavirus As Bait.** Disponível em: https://www.forbes.com/sites/daveywinder/2020/03/22/healthcare-workers-targeted-by-dangerous-new-windows-ransomware-campaign-using-coronavirus-as-bait/#259a0d602212. Acessado em 27 de março de 2020.