Overview dos casos de ataques cibernéticos durante a pandemia de COVID-19

André Lucas Alcântara da Silva[1]
Gills Vilar-Lopes[2]

A pandemia do novo coronavírus (COVID-19), vivida pela maioria dos países nos primeiros meses de 2020, desafia governos, protocolos e políticas sanitárias de todo o mundo. A preocupação é justificada pela velocidade de propagação do vírus e por seu impacto, sobretudo em pessoas idosas e com doenças preexistentes como diabetes e hipertensão[3] .

Neste cenário, é compreensível que esforços de órgãos, instituições, empresas e da sociedade como um todo, voltem-se para conter a expansão do vírus. No entanto, em momentos de crise generalizada, áreas e setores tidos como periféricos têm sua atenção reduzida e tornam-se elementos vulneráveis a investidas de oportunistas. Exemplo disso é o próprio setor cibernético.

De acordo com a avaliação do *SecDev Group*, grupo canadense de pesquisadores em Segurança Cibernética,houve um aumento de 475% no número de ataques cibernéticos a órgãos, instituições e empresas que compõem a indústria de saúde mundial[4].

O mapa de ameaças cibernéticas da Check Point[5] (2020), empresa especializada em Segurança da Informação, revela que a indústria de Saúde figura entre os três principais alvos de ataques cibernéticos durante a pandemia do COVID-19.

Tais informações revelam que, paralelamente à luta travada pela saúde contra o novo coronavírus, há também a necessidade de posicionar-se frente a outro desafio: o cibernético.

Estima-se que o primeiro caso de COVID-19 em humanos tenha ocorrido entre os meses de novembro e dezembro de 2019, em Wuhan, na China. A partir daí, o aumento dos casos confirmados cresceu exponencialmente, extrapolando as fronteiras chinesas e atingindo outros países. A velocidade de propagação dos casos permaneceu acelerada, chegando a outros continentes, o que levou a Organização Mundial de Saúde (OMS) a declarar, em 11 de março de 2020, que se tratava de uma pandemia.

---

[1] Mestrando em Ciências Aeroespaciais pelo Programa de Pós-Graduação em Ciências Aeroespaciais (PPGCA) da Universidade da Força Aérea (UNIFA).
[2] Docente do Programa de Pós-Graduação em Ciências Aeroespaciais (PPGCA) da Universidade da Força Aérea (UNIFA).
[3] BARIFOUSE, Rafael. Coronavírus: como diabetes, hipertensão e outras doenças crônicas agravam quadro de covid-19. BBC, São Paulo, 19 mar. 2020. Disponível em: https://www.bbc.com/portuguese/brasil-51968714. Acesso em: 11 abr. 2020.
[4] BARIFOUSE, Rafael. Coronavírus: como diabetes, hipertensão e outras doenças crônicas agravam quadro de covid-19. BBC, São Paulo, 19 mar. 2020. Disponível em: https://www.bbc.com/portuguese/brasil-51968714. Acesso em: 11 abr. 2020.
[5] CHECK POINT. Live cyber threat map. [2020]. Disponível em: https://threatmap.checkpoint.com. Acesso em: 3 abr. 2020.

Desde então, autoridades tomaram ações rígidas e emergenciais na tentativa de conter a propagação do vírus, a qual poderia causar um colapso nas estruturas de saúde. Não obstante, praticamente todos os esforços governamentais foram redirecionados a essa necessidade.

Diante deste pano de fundo, caracterizado por uma crise sanitária mundial, grupos de *hackers* ampliaram seus ataques, aproveitando a desatenção de operadores e as vulnerabilidades existentes nos sistemas informacionais, especialmente dos governamentais.

Em 13 de março, a OMS foi alvo de um desses ataques. A tentativa de invasão se deu a partir da ativação de um *site* malicioso que simulava o sistema de *e-mail* da Organização e tinha como objetivo principal capturar senhas de funcionários e informações sensíveis quanto à pandemia do COVID-19. De acordo com a OMS, a tentativa foi identificada a tempo e não obteve sucesso[6].

No mesmo dia, o Hospital Universitário de *Brno*, na República Tcheca, sofreu ataques cibernéticos, com relativo sucesso, provocando atrasos na realização de testes do COVID-19. O diretor do hospital informou que os sistemas começaram a falhar lentamente e os computadores tiveram de ser imediatamente desligados[7].

Em 14 de março, o renomado centro de pesquisa inglês *Hammersmith Medicines Research* (HMR) sofreu um ataque cibernético, enquanto realizava pesquisas e testes de novos medicamentos, inclusive para conter a proliferação do COVID-19 [8]. A infecção virtual nos sistemas hospitalares foi feita com o *ramsonware* Maze, *software* malicioso (*malware*) capaz de criptografar arquivos e impedi-los de ser acessados, exigindo, para tanto, pagamento de "resgate".

Resultado: os sistemas ficaram temporariamente indisponíveis até que especialistas utilizassem *backups* para recuperar os arquivos (*restore*), sem a necessidade de pagar aos criminosos [9].

Dois dias após a tentativa de ataque à OMS, o *site* do Departamento de Saúde dos Estados Unidos (HHS) sofreu um ataque[10] conhecido como Negação de Serviço Distribuído (DDoS), que visa congestionar os serviços da vítima até que os mesmos fiquem

---

[6] SATTER, Raphael; STUBBS, Jack; BING, Christopher. Hackersatacam OMS em meio à pandemia de coronavírus: Tentativa de invasão não obteve sucesso. **Agência Brasil**, Wasington e Londres, 23 mar. 2020. Disponível em: https://agenciabrasil.ebc.com.br/internacional/noticia/2020-03/hackers-atacam-oms-em-meio-pandemia-de-covid-19. Acesso em: 2 abr. 2020.

[7] HARÁN, Juan. Site do departamento de saúde dos Estados Unidos sofre ataque DDoS. **We Live Security**, 17 mar. 2020. Disponível em: https://www.welivesecurity.com/br/2020/03/17/site-departamento-saude-estados-unidos-sofre-ataque-ddos/. Acessoem: 3 abr. 2020.

[8] GOUD, Naveen. Ransowareattack on Hammersmith Medicines Research and Ameren Missouri. **CybersecurityInsiders**, 2020. Disponível em: https://www.cybersecurity-insiders.com/ransomware-attack-on-hammersmith-medicines-research-and-ameren-missouri. Acesso em: 3 abr. 2020.

[9] GALLAGHER, Ryan. Hackers 'without conscience' target health-care providers, **Bloomberg**, 1 abr. 2020. Disponível em:https://www.bloomberg.com/news/articls/2020-04-01/hackers-without-conscience-demand-ransom-from-health-providers. Acesso em: 4 abr. 2020.

[10] STEIN, Shira. Cyber-attack hits U.S. health agency amid Covid-19 outbreak. **Bloomberg**, 16 mar. 2020. Disponível em: https://www.bloomberg.com/news/articles/2020-03-16/u-s-health-agency-suffers-cyber-attack-during-covid-19-response. Acesso em: 3 abr. 2020.

indisponíveis. O ataque conseguiu sobrecarregar os servidores temporariamente via milhões de acesso.

No dia 22 de março, o Centro Nacional de Infraestruturas e Segurança Cibernética da Espanha identificou uma série de ataques cibernéticos aos hospitais do país. A forma utilizada pelos *hackers* foi a disseminação do *ramsonware* Netwalker. Tais tentativas motivaram o governo espanhol a contratar mais profissionais da área de Segurança da Informação[11].

Ainda no mês de março, a empresa americana de biotecnologia *10x Genomics*, que integra a aliança global de instituições dedicadas à pesquisa e ao desenvolvimento de medicamentos contra o novo coronavírus, também foi alvo de ataques pelo *ramsonware* conhecido como *REvil*. A empresa disse que os dados infectados foram isolados para que as atividades pudessem continuar[12].

Os ataques cibernéticos em tempos de pandemia não se restringem às instituições de saúde. Adicionalmente, *crackers* se aproveitam de vulnerabilidades também existentes em órgãos governamentais, como foi o caso do ataque ao Instituto Nacional de Previdência Social (INPS) da Itália. Após o governo anunciar o subsídio de 600 euros a profissionais liberais, no intuito de contornar a crise econômica durante a pandemia, o *site* do INPS recebeu uma sequência de ataques que provocou um fluxo de 100 solicitações do benefício por segundo. Para conter os ataques, foi necessário tirar o *site* de operação[13].

Esses ataques cibernéticos, presentes em meio à pandemia do COVID-19, possuem características específicas que podem torná-los ainda mais difíceis de serem compreendidos. Uma delas diz respeito a identificar as origens dos ataques. O mesmo vale para as motivações, que também se tornam obscuras, prejudicando as tomadas de decisão [14].

Em tempos de confinamento e *home office* generalizados, o processo de identificação tende a se tornar ainda mais complexo, visto que milhões de profissionais utilizam suas redes particulares, muitas vezes sem nenhuma proteção mais robusta, para realizar atividades do trabalho a partir do conforto do lar. Tal situação cria níveis de vulnerabilidade maiores, gerando, inclusive, oportunidades para que *crackers* infectem seus dispositivos e utilizem-nos, por exemplo, em ataques de massa, como o DDoS. Em outras palavras, mesmo sem ciência, milhares de pessoas podem ter seus equipamentos comprometidos, os quais farão parte de um exército digital pronto para ser empregado em ataques cibernéticos.

---

[11] DOLZ, Patricia Ortega; COLOMÉ, JordiP.Lapolicía detecta unciberataque al sistema informático de loshospitales. **El País**, Madri, 23 mar. 2020. Disponível em: https://elpais.com/espana/2020-03-23/la-policia-detecta-un-ataque-masivo-al-sistema-informatico-de-los-hospitales.html. Acessoem: 3 abr. 2020.

[12] GALLAGHER (2020).

[13] AMANTE, Angelo. Italy's social security website hit by hacker attack. **Reuters**, Roma, 1 abr. 2020. Disponível em: https://www.reuters.com/article/us-health-coronavirus-italy-cybercrime/italys-social-security-website-hit-by-hacker-attack-idUSKBN21J5U1. Acesso em: 4 abr. 2020.

[14] KREMER, J.; MÜLLER, B. SAM: a framework to understand emerging challenges to states in an interconnected world. In: _____ (Ed.). **Cyberspace and international relations**: theory, prospects and challenges. Heidelberg: Springer, 2014. p. 41-58.

Quanto às motivações de um ataque, existem inúmeras possibilidades. Desde um simples acirramento entre grupos *hackers*, na tentativa de demonstrar seus conhecimentos, passando pelo aspecto financeiro e indo até ao objetivo de desestabilizar uma nação, a partir de investidas contra instituições e infraestruturas críticas[15].

O fato é que, em meio a esses ataques cibernéticos durante a atual pandemia, surgem especulações que retratam seu momento político internacional. De acordo com a *FireEye*, empresa norte-americana de Segurança Cibernética, as atividades do grupo *hacker* chinês conhecido como "APT41" têm aumentado desde o início deste ano, com vários países alvos de espionagem e indústrias de Defesa, finanças, energia e saúde sendo afetadas[16].

Os empecilhos encontrados para identificar com precisão a origem e a motivação de ataques cibernéticos ampliam o nível de complexidade das decisões a serem tomadas pelos órgãos de Segurança e Defesa, visto que uma resposta militar, para tais casos, torna-se problemática tanto do ponto de vista estratégico quanto legal. Para se ter uma dimensão desse problema, o Ministério da Defesa francês apregoou que "a França se reserva o direito de responder a qualquer operação cibernética que constitua uma violação do direito internacional da qual seja vítima" [17](tradução nossa).

Diante disso, é cada vez mais importante o trabalho conjunto de instituições governamentais, intergovernamentais, privadas e da Academia para atuar nos domínios dos ataques cibernéticos. Ademais, esta junção de esforços colabora no processo de reduzir potenciais danos resultantes dos ataques, ainda mais em tempos de pandemia. Exemplo desse trabalho coordenado é o canadense *SecDev Group*, que tem como objetivo reunir especialistas em Segurança da Informação no intuito de proteger os serviços-chave e as infraestruturas críticas de ataques cibernéticos durante a pandemia de COVID-19. A missão do grupo se resume nos seguintes tópicos:

- Ramsonwares não devem impedir o funcionamento de hospitais;
- Ataques cibernéticos não devem afetar pacientes em tratamento; e
- Serviços essenciais não devem ser afetados por ataques cibernéticos[18] .

Outra importante iniciativa foi aplicada na Europa: a *C5 Capital*, empresa de investimentos em soluções de Segurança da Informação, criou a *C5 Alliance*, grupo composto por outras reconhecidas instituições do setor e com o objetivo de proteger sistemas e bancos de dados de hospitais, clínicas e indústrias farmacêuticas [19](C5 CAPITAL, 2020).

---

[15] BRASIL. Presidência da República. **Livro verde**: segurança cibernética no Brasil. Brasília, DF: Gabinete de Segurança Institucional, 2010.
[16] GLYER, Christopher*et al*. Threat research: this is not a test: APT41 initiates global intrusion campaign using multiple exploits. **FireEye**, 25 mar. 2020. Disponível em: https://www.fireeye.com/blog/threat-research/2020/03/apt41-initiates-global-intrusion-campaign-using-multiple-exploits.html. Acesso em: 4 abr. 2020.
[17] FRANÇA. Ministère des Armées. **Droit international appliqué aux opérations dans le cyberespace**. Paris: Délégation à l'information et à la communication de la défense, 2019, p. 6.
[18] SECDEV. Cyber Defense. [2020]. Disponível em: https://www.secdev.com/. Acesso em: 8 abr. 2020.
[19] C5 CAPITAL. Leaders in cyber security have united to combat an unprecedented level of cyber attacks targeting the healthcare sector. [2020]. Disponível em: https://www.c5capital.com/leaders-in-cybersecurity-

Nosso breve olhar pelos principais ataques cibernéticos a infraestruturas e órgãos de saúde pública reforça a ideia de que um cenário caótico pode não só potencializar ataques cibernéticos, como também estreitar laços entre setores públicos e privados para buscarem proteger ativos informacionais em comum. Ficam os exemplos para o Brasil.

have-united-to-combat-an-unprecedented-level-of-cyberattacks-targeting-the-healthcare-sector/. Acesso em 8 abr. 2020.