TLP:WHITE

Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

CYBER THREAT BULLETIN

Impact of COVID-19 on Cyber Threats to the Health Sector

8 JUNE 2020

Canada

ABOUT THIS DOCUMENT

AUDIENCE

This Cyber Threat Bulletin is intended for the cybersecurity community. Subject to standard copyright rules, TLP:WHITE information may be distributed without restriction. For more information on the Traffic Light Protocol, see https://www.first.org/tlp/.

CONTACT

For follow up questions or issues please contact CCCS at contact@cyber.gc.ca.

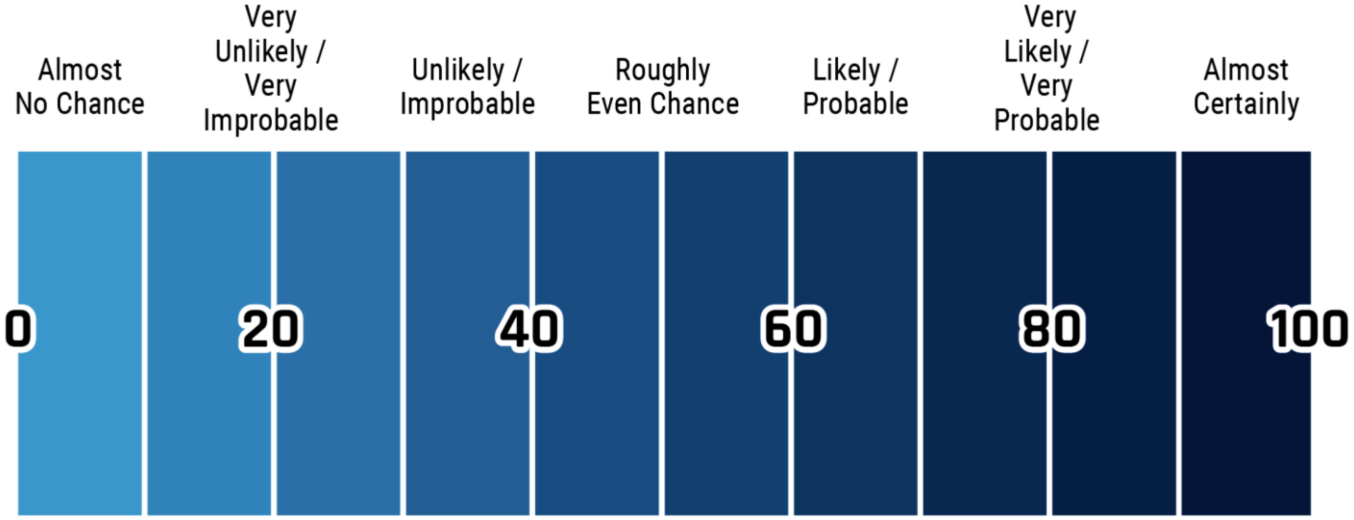
ASSESSMENT BASE AND METHODOLOGY

The key judgements in this assessment rely on reporting from multiples sources, both classified and unclassified. The judgements are based on the Canadian Centre for Cyber Security's (CCCS) knowledge and expertise in cyber security. Defending the Government of Canada's information systems provides the Cyber Centre with a unique perspective to observe trends in the cyber threat environment, which also informs our assessments. CSE's foreign intelligence mandate provides us with valuable insight into adversary behavior in cyberspace. While we must always protect classified sources and methods, we provide the reader with as much justification as possible for our judgements.

Our key judgements are based on an analytical process that includes evaluating the quality of available information, exploring alternative explanations, mitigating biases and using probabilistic language. We use terms such as "we assess" or "we judge" to convey an analytic assessment. We use qualifiers such as "possibly", "likely", and "very likely" to convey probability.

The contents of this document are based on information available as of 1 June 2020.

The chart below matches estimative language with approximate percentages. These percentages are not derived via statistical analysis, but are based on logic, available information, prior judgements, and methods that increase the accuracy of estimates.



Key Judgements

- We assess that national and international public health organizations will almost certainly continue to be targeted by cyber threat activity such as ransomware, information and credential theft, and distributed denial of service (DDoS) attacks.
- We assess that cyber threat actors will almost certainly continue to target hospitals, medical clinics, and other front-line services involved in COVID-19 responses around the world. While there have been many ransomware attacks against hospitals abroad, the Cyber Centre has not been engaged to provide assistance related to a major ransomware event against a Canadian hospital during the pandemic as incidents were likely localized and managed by hospital cybersecurity teams. However, we assess that Canadian hospitals are very likely to be as attractive to threat actors as other hospitals, particularly if they are at the centre of a local outbreak.
- We assess that foreign intelligence agencies will almost certainly continue to use their cyber capabilities to pursue intelligence related to COVID-19 medical research and intellectual property. Intellectual property, especially related to vaccine development, treatments, COVID-19 testing, and medical devices such as ventilators or personal protective equipment (PPE), would offer public health, economic, and national security benefits.
- We judge that online influence campaigns will almost certainly continue to spread falsehoods and foment greater skepticism of official statistics and statements regarding the COVID-19 pandemic.
- Although we do not assess that Canada is a high priority target for online influence activities, that could change quickly, especially in response to increased political tensions with some states. In addition, many Canadian allies are a target for online influence campaigns and their information ecosystems are closely intertwined with that of Canada.
- We judge that pandemic response efforts will almost certainly continue to be negatively impacted by online fraud activity related to COVID-19, which diverts resources from legitimate responses and distributes counterfeit and substandard goods.

COVID-19-Related Targeting of the Health Sector

On 11 March 2020, the World Health Organization (WHO) officially declared the novel coronavirus disease 2019 (COVID-19) a global pandemic. In a previous Cyber Threat Bulletin, we assessed that cyber threat actors have taken advantage of this context to conduct a range of cyber threat activities.[4] The health sector—which we define as including public health institutions, hospitals and other front-line medical providers, research organizations, and pharmaceutical and medical equipment companies—is being targeted by both cyber criminals and state-sponsored cyber threat actors. The Cyber Centre assesses that in Canada and many other countries health sector organizations almost certainly face increased threats to their cyber security due to the COVID-19 pandemic.[5]

Remote Work Introduces Vulnerabilities

Health sector organizations face an increasing threat surface as employees shift to remote work arrangements.[1] In March 2020, Microsoft found several dozen hospitals with vulnerable remote work infrastructure, such as gateway appliances and virtual private networks (VPNs).[2] The Cyber Centre has issued alerts regarding vulnerabilities in remote work software provided by companies such as Citrix, Fortinet, Palo Alto, and Pulse that are being actively targeted by cyber criminals and state-sponsored actors.[3]

Public Health Institutions

We assess that national and international public health organizations will almost certainly continue to be targeted by cyber threat activity such as ransomware, information and credential theft, and distributed denial of service (DDoS) attacks. State-sponsored actors are interested in the information related to pandemic responses held by national and international public health institutions. Cyber criminals recognize that these institutions are under pressure to continuously coordinate response efforts and provide information to the public and therefore have a high willingness to pay for the restoration of their systems. In late-March, threat actors sent COVID-19-themed malicious emails attempting to deliver ransomware to a Canadian government health organization engaged in pandemic response.[6] Earlier in March, the WHO's chief information security officer stated that the organization had experienced an increase in cyber threat activity during the COVID-19 pandemic.[7] Malicious emails sent to the WHO attempted to gather credentials, which could then have been used to access sensitive information or to target additional victims.

When cyber criminals successfully conduct ransomware and DDoS attacks against public health institutions, they can disrupt efforts to slow the spread of COVID-19 by hampering information dissemination and coordination. For example, a DDoS attack against a Dutch government website temporarily took down the webpage that provided COVID-19 information to the public.[8] DDoS attacks can be used as a means of extortion by cyber criminals, and state-sponsored actors may use DDoS attacks as part of an online influence campaign to embarrass their targets or remove legitimate sources of information.

Front-line Medical Providers

We assess that cyber threat actors will almost certainly continue to target hospitals, medical clinics, and other front-line services involved in COVID-19 responses around the world. Although several ransomware operators promised to refrain from targeting front-line medical providers during the pandemic,[10] between March and April 2020, hospitals and healthcare centres in the Czech Republic,[11] the US,[12] Spain,[13] and Germany[14] were targeted in ransomware attacks. While there have been many ransomware attacks against hospitals abroad, the Cyber Centre has not been engaged to provide assistance related to a major ransomware event against a Canadian hospital during the pandemic, as incidents were likely localized and managed by hospital cybersecurity teams. However, we assess that Canadian hospitals are very likely to be as attractive to threat actors as other hospitals, particularly if they are at the centre of a local outbreak. One ransomware campaign targeted eleven front-line healthcare providers in the US.[15] Brno University Hospital, a facility that conducts COVID-19 testing in the Czech Republic, had to disconnect hospital systems as a result of a cyber intrusion on 11 March, and hospital operations were disrupted.[16] A medical centre in Colorado was forced to use paper and manual records on 21 April due to a ransomware attack.[17]

Vulnerabilities from Medical Devices

Hospitals and other healthcare providers face unique cyber security challenges stemming from the diverse medical devices connected to their networks, especially medical Internet of Things (IoT) devices. According to a survey released in March 2020 by Palo Alto Networks, 83% of medical imaging devices in the United States are running unsupported operating systems.[9] Cyber threat actors can use unpatched devices or legacy systems to compromise hospital networks and steal data or undertake a ransomware attack.

Front-line medical providers are popular ransomware targets because they have significant financial resources and network downtime can have life-threatening consequences for patients. Cybercriminals view this as good odds for a substantial ransom payment. Beyond immediate disruptions, organizations hit by ransomware may also face data breaches, a threat used by many ransomware operators to coerce victims into paying. Since November 2019, the Cyber Centre has observed multiple ransomware campaigns exfiltrate and leak victim data after ransom payments were refused. This is a serious threat for front-line medical providers who possess sensitive personal health information that would have legal and reputational consequences if leaked.

Intellectual Property and Supply Chains

We assess that foreign intelligence agencies will almost certainly continue to use their cyber capabilities to pursue intelligence related to COVID-19 medical research and intellectual property. Given the unexpected spread and severity of the disease, governments almost certainly feel they are operating with inadequate information to craft effective public health and economic responses to the COVID-19 pandemic. As such, foreign intelligence agencies are almost certainly being tasked with new intelligence collection requirements related to the COVID-19 pandemic. It is also likely that cybercriminals affiliated with affected governments are targeting the health sector to supplement official intelligence collection efforts. Intellectual property, especially related to vaccine development, treatments, COVID-19 testing, and medical devices such as ventilators or personal protective equipment (PPE), would almost certainly offer public health, economic, and national security benefits. For example, stolen intellectual property could give countries a faster path to large-scale inoculation and economic growth, and thereby usher in domestic stability and garner international praise.

The Cyber Centre is aware of cyber threat activity directed against Canada that we assess is almost certainly tied to Canada's status as a world leader in health and biotechnology. Many of Canada's companies and research universities are leading global efforts to develop COVID-19 tests, treatments, and vaccines, making them attractive targets.

In mid-April 2020, a Canadian biopharmaceutical company was compromised by a foreign cyber threat actor almost certainly attempting to steal its intellectual property. State-sponsored actors have targeted medical companies and research universities in South Korea,[19] China,[20] the US,[21] and the UK.[22] as well. On 13 May 2020, the Federal Bureau of Investigation (FBI) and the Cybersecurity and Infrastructure Security Agency (CISA) in the US issued an announcement warning healthcare, pharmaceutical, and research organizations working on the COVID-19 response that they are prime targets for state-sponsored cyber threat actors.[23]

Pharmaceutical and medical equipment companies, as well as medical research organizations, have also been targeted in ransomware attacks. As with front-line medical providers, these organizations are attractive targets for cyber criminals due to the time-sensitivity of their work and their ability to pay the ransom. Between March and April 2020, ransomware attacks were directed at organizations such as these in Canada,[24] the US,[25] the UK, [26] Belgium,[27] and Germany[28].

Supercomputers Compromised

Cyber criminals have hijacked supercomputers throughout Europe to mine cryptocurrency. Some of these supercomputers were involved in COVID-19 research efforts, such as modelling the spread of the virus and assisting with the development of treatments and vaccines. As a result, the systems had to be taken offline to be repaired, interrupting the research efforts.[18]

Online Influence and Fraud

We judge that online influence campaigns will almost certainly continue to spread falsehoods and foment greater skepticism of official statistics and statements regarding the COVID-19 pandemic. Although we do not assess that Canada is a high priority target for online influence activities, that could change quickly, especially in response to increased political tensions with some states. In addition, the US,[29] UK,[30] and other countries are a target for online influence campaigns and their information ecosystems are closely intertwined with that of Canada. Canadian law enforcement officials are currently investigating possible links between attacks on cell phone towers in Canada and a COVID-19-related conspiracy theory that ties the disease to 5G technology, which has resulted in attacks on cell phone towers globally.[31] In April 2020, a disinformation campaign targeted a Canadian-led NATO battle group in Latvia, falsely claiming that one of their contingents had “a high number” of cases of COVID-19.[32] This activity was almost certainly intended to increase hostility between the Latvian public and the Canadian-led forces stationed there.

Typically, online influence campaigns are aimed at domestic audiences to diffuse dissatisfaction with national pandemic responses or at international audiences in order to blunt and counter international criticism. This can be achieved by spreading false and distorted information, or otherwise shaping narratives on social media that portray rival governments as untrustworthy or inept in their handling of the COVID-19 pandemic. According to an April 2020 report by EUvsDisinfo, a European Union project analyzing disinformation, online influence activity includes the spread of theories that COVID-19 is a hoax, contradictions of official WHO guidance, and incorrect information about potential treatments.[33] The immediate goal of this type of online influence is to sow confusion and anger, induce mistrust and doubt, and weaken the ability of targeted nations to manage the pandemic. Beyond that, individuals believing these malicious messages may end up putting themselves and others at risk.

The COVID-19 pandemic has also been harnessed by cyber criminals to advertise counterfeit medical supplies[34] and elicit fraudulent donations.[35] The Canadian Anti-Fraud Centre has issued a warning listing many scams related to COVID-19, including fraudulent offers of fast COVID-19 tests for sale, counterfeit products that claim to treat or prevent the disease, and fake online advertisements offering high demand cleaning products.[36] The FBI has noted multiple cases of government agencies transferring funds to fraudulent sellers in attempts to purchase PPE and other medical equipment and supplies.[37] In one week, INTERPOL seized more than 34,000 counterfeit and substandard masks alongside other fake products like “corona spray” and “coronavirus medicine”, many of which were being sold online.[38]

Fraud has immediate costs for the victims of these schemes and causes additional losses due to the diversion of resources from legitimate COVID-19 efforts. In many cases, victims never receive any goods, but in others, the distribution of counterfeit and substandard products dangerously diminishes the health sector’s efforts to protect its staff and the public from COVID-19.[39] We assess that pandemic response efforts will almost certainly continue to be negatively impacted by online fraud activity related to COVID-19, which diverts resources and distributes counterfeit and substandard goods.

USEFUL RESOURCES

For more information on how to mitigate cyber threats, including those related to COVID-19 lures or remote workforce deployments, we recommend visiting the following websites:

- Cyber Threats to Canadian Health Organizations (https://cyber.gc.ca/en/alerts/cyber-threats-canadian-health-organizations)
- Cyber Security Advice and Guidance for Research and Development Organizations during COVID-19 (https://cyber.gc.ca/en/guidance/cyber-security-advice-and-guidance-research-and-development-organizations-during-covid-19)
- Canadian Shield – Sharing the Cyber Centre's Threat Intelligence to Protect Canadians During the COVID-19 Pandemic (https://cyber.gc.ca/en/canadian-shield-sharing-cyber-centres-threat-intelligence-protect-canadians-during-covid-19)
- COVID-19 Malicious Websites (https://cyber.gc.ca/en/guidance/covid-19-and-malicious-websites-itsap00103)
- Cyber Centre's Advice on Cyber Hygiene (https://cyber.gc.ca/en/guidance/cyber-hygiene)
- Spotting Malicious E-mails (https://cyber.gc.ca/en/guidance/spotting-malicious-email-messages-itsap00100)
- Staying Cyber Safe while Teleworking (https://cyber.gc.ca/en/staying-cyber-safe-while-teleworking)
- Considerations when Using Video-Teleconference Products and Services (https://cyber.gc.ca/en/alerts/considerations-when-using-video-teleconference-products-and-services)
- Video-Teleconferencing (https://cyber.gc.ca/en/guidance/video-teleconferencing-itsap10216)
- Cyber Security Tips for Remote Work (https://cyber.gc.ca/en/guidance/cyber-security-tips-remote-work-itsap10116)
- Security Tips for Organizations with Remote Workers (https://cyber.gc.ca/en/guidance/telework-security-issues-itsap10016)
- Virtual Private Networks (https://cyber.gc.ca/en/guidance/virtual-private-networks-itsap80101)
- Active Exploitation of VPN Vulnerabilities (https://cyber.gc.ca/en/alerts/active-exploitation-vpn-vulnerabilities-0)
- Active Exploitation of Citrix Vulnerabilities (https://cyber.gc.ca/en/alerts/active-exploitation-citrix-vulnerabilities)
- Continued Threat Actor Exploitation Post Pulse Secure VPN Patching (CISA) (https://cyber.gc.ca/en/alerts/continued-threat-actor-exploitation-post-pulse-secure-vpn-patching-cisa)
- How to Spot Misleading Information Online and What to do About it (https://www.getcybersafe.gc.ca/cnt/blg/pst-20181023-en.aspx)
- Ransomware: How to Prevent and Recover (https://cyber.gc.ca/en/guidance/ransomware-how-prevent-and-recover-itsap00099)
- Protect Your Organization from Malware (https://cyber.gc.ca/en/guidance/protect-your-organization-malware-itsap00057)
- IoT Security for Small and Medium Organizations (https://cyber.gc.ca/en/guidance/internet-things-security-small-and-medium-organizations-itsap00012)

[1] Bob Bragdon. “Pandemic impact report: Security leaders weigh in.” *CSO*. 1 April 2020. https://www.csoonline.com/article/3535195/pandemic-impact-report-security-leaders-weigh-in.html/.

[2] “Microsoft works with healthcare organizations to protect from popular ransomware during COVID-19 crisis: Here’s what to do.” *Microsoft*. 1 April 2020. https://www.microsoft.com/security/blog/2020/04/01/microsoft-works-with-healthcare-organizations-to-protect-from-popular-ransomware-during-covid-19-crisis-heres-what-to-do/.

[3] “Active Exploitation of Citrix Vulnerabilities.” *Canadian Centre for Cyber Security*. 17 January 2020. https://cyber.gc.ca/en/alerts/active-exploitation-citrix-vulnerabilities; “Active Exploitation of VPN Vulnerabilities.” *Canadian Centre for Cyber Security*. 17 September 2019. https://cyber.gc.ca/en/alerts/active-exploitation-vpn-vulnerabilities-0.

[4] See CCCS’s previous publication, CCCS-SCTA20200427*: Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threat Activity*, for an assessment of the broader impacts of the pandemic on cyber security. https://cyber.gc.ca/en/guidance/cyber-threat-bulletin-impact-covid-19-cyber-threat-activity

[5] “Alert: Cyber threats to Canadian health organizations.” *Canadian Centre for Cyber Security*. 20 March 2020. https://www.cyber.gc.ca/en/alerts/cyber-threats-canadian-health-organizations.

[6] “Malicious Attackers Target Government and Medical Organizations With COVID-19 Themed Phishing Campaigns.” *Palo Alto Networks, Unit 42*. 14 April 2020. https://unit42.paloaltonetworks.com/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/

[7] Raphael Satter, Jack Stubbs, and Christopher Bing. “Exclusive: Elite hackers target WHO as coronavirus cyberattacks spike.” *Reuters*. 23 March 2020. https://www.reuters.com/article/us-health-coronavirus-who-hack-exclusive/exclusive-elite-hackers-target-who-as-coronavirus-cyberattacks-spike-idUSKBN21A3BN.

[8] “Police Arrest Suspect for DDoS Attack on MijnOverheid.nl.”(Translated from original language). *Netherlands Police*. 10 April 2020. https://www.politie.nl/nieuws/2020/april/10/03-politie-houdt-verdachte-aan-voor-ddos-aanval-op-mijnoverheid.nl.html.

[9] “2020 Unit 42 IoT Threat Report.” *Palo Alto Networks, Unit 42*. 10 March 2020. https://unit42.paloaltonetworks.com/iot-threat-report-2020/.

[10] Zack Whittacker. “Hackers publish ExecuPharm internal data after ransomware attack.” *Tech Crunch*. 27 April 2020. https://techcrunch.com/2020/04/27/execupharm-clop-ransomware/; Lawrence Abrams. “Ryuk Ransomware Keeps Targeting Hospitals During the Pandemic.” *Bleeping Computer*. 26 March 2020. https://www.bleepingcomputer.com/news/security/ryuk-ransomware-keeps-targeting-hospitals-during-the-pandemic/.

[11] Ionut Ilascu. “COVID-19 Testing Center Hit by Cyberattack.” *Bleeping Computer*. 14 March 2020. https://www.bleepingcomputer.com/news/security/covid-19-testing-center-hit-by-cyberattack/.

[12] Filip Truta. “Maze Ransomware Continues to Hit Healthcare Units amid Coronavirus (COVID-19) Outbreak.” *Security Boulevard*. 19 March 2020. https://securityboulevard.com/2020/03/maze-ransomware-continues-to-hit-healthcare-units-amid-coronavirus-covid-19-outbreak/.

[13] “Capitalizing on Coronavirus Panic, Threat Actors Target Victims Worldwide.” *Recorded Future, Insikt Group*. 12 March 2020. https://go.recordedfuture.com/hubfs/reports/cta-2020-0312-2.pdf.

[14] Brian Krebs. “Europe’s Largest Private Hospital Operator Fresenius Hit by Ransomware.” *Krebs on Security*. 6 May 2020. https://krebsonsecurity.com/2020/05/europes-largest-private-hospital-operator-fresenius-hit-by-ransomware/.

[15] Lawrence Abrams. “Ryuk Ransomware Keeps Targeting Hospitals During the Pandemic.” *Bleeping Computer*. 26 March 2020. https://www.bleepingcomputer.com/news/security/ryuk-ransomware-keeps-targeting-hospitals-during-the-pandemic/.

[16] “Brno University Hospital in Czech Republic Suffers Cyberattack During COVID-19 Outbreak.” *Security Magazine*. 17 March 2020. https://www.securitymagazine.com/articles/91921-brno-university-hospital-in-czech-republic-suffers-cyberattack-during-covid-19-outbreak.

[17] Brandon Thompson. “IT incident under investigation at Parkview Medical Center.” *Fox21 News*. 24 April 2020. https://www.fox21news.com/top-stories/it-incident-under-investigation-at-parkview-medical-center/.

[18] “Europe’s supercomputers hijacked by attackers for cryptomining.” *BBC*. 18 May 2020. https://www.bbc.com/news/technology-52709660; Phil Muncaster. “Crypto-Miners Take Out Supercomputers Working on #COVID-19.” *Infosecurity Magazine*. 18 May 2020. https://www.infosecurity-magazine.com/news/cryptominers-out-supercomputers/.

[19] Shin Eun-byeol. “Attempting to hack into a domestic corona diagnostic kit company…almost leaking technology.” (Translated from original language.) *Hankook Ilbo*. 31 March 2020. https://www.hankookilbo.com/News/Read/202003311798732396?did=NA&dtype=&dtypecode=&prnewsid= .

[20] Zak Doffman. “Chinese ‘Frontline’ COVID-19 Research Firm Reported Hacked: Data Now on Dark Web.” *Forbes*. 26 April 2020. https://www.forbes.com/sites/zakdoffman/2020/04/26/chinese-covid-19-detection-firm-just-got-hacked-data-for-sale-on-dark-web-new-report/#5b9db7395dec.

[21] Davey Winder. “FBI Says Foreign States Hacked Into U.S. COVID-19 Research Centers: Report.” *Forbes*. 17 April 2020. https://www.forbes.com/sites/daveywinder/2020/04/17/fbi-says-foreign-states-hacked-into-us-covid-19-research-centers-

report/#4dbde9573c29; "APT Groups Target Healthcare and Essential Services." Cybersecurity and Infrastructure Security Agency and National Cyber Security Centre. 5 May 2020. https://www.us-cert.gov/ncas/alerts/AA20126A; Jack Stubbs. "Exclusive: Iran-linked Hackers Recently Targeted Coronavirus Drugmaker Gilead – sources." *Reuters*. 8 May 2020. https://www.reuters.com/article/us-healthcare-coronavirus-gilead-iran-ex/exclusive-iran-linked-hackers-recently-targeted-coronavirus-drugmaker-gilead-sources-idUSKBN22K2EV.

[22] "APT Groups Target Healthcare and Essential Services." Cybersecurity and Infrastructure Security Agency and National Cyber Security Centre. 5 May 2020. https://www.us-cert.gov/ncas/alerts/AA20126A.

[23] "FBI and CISA Warn Against Chinese Targeting of COVID-19 Research Organizations." *Federal Bureau of Investigation.* 13 May 2020. https://www.fbi.gov/news/pressrel/press-releases/fbi-and-cisa-warn-against-chinese-targeting-of-covid-19-research-organizations.

[24] "Malicious Attackers Target Government and Medical Organizations with COVID-19 Themed Phishing Campaigns." *Palo Alto Networks, Unit 42*. 14 April 2020. https://unit42.paloaltonetworks.com/covid-19-themed-cyber-attacks-target-government-and-medical-organizations/.

[25] "Form 8-K 10x Genomics, Inc.: Current report, item 7.01." *U.S. Securities and Exchange Commission*. 1 April 2020. https://sec.report/Document/0001193125-20-094606/; Zack Whittacker. "Hackers publish ExecuPharm internal data after ransomware attack." *Tech Crunch*. 27 April 2020. https://techcrunch.com/2020/04/27/execupharm-clop-ransomware/.

[26] Barth. "Maze ransomware attackers extort vaccine testing facility." *SC Media*. 23 March 2020. https://www.scmagazine.com/home/security-news/ransomware/maze-ransomware-attackers-extort-vaccine-testing-facility/.

[27] Ionut Ilascu. "Russian-Speaking Hackers Attack Pharma, Manufacturing Companies in Europe." *Bleeping Computer*. 27 March 2020. https://www.bleepingcomputer.com/news/security/russian-speaking-hackers-attack-pharma-manufacturing-companies-in-europe/.

[28] Brian Krebs. "Europe's Largest Private Hospital Operator Fresenius Hit by Ransomware." *Krebs on Security.* 6 May 2020. https://krebsonsecurity.com/2020/05/europes-largest-private-hospital-operator-fresenius-hit-by-ransomware/; Ionut Ilascu. "Russian-Speaking Hackers Attack Pharma, Manufacturing Companies in Europe." *Bleeping Computer*. 27 March 2020. https://www.bleepingcomputer.com/news/security/russian-speaking-hackers-attack-pharma-manufacturing-companies-in-europe/.

[29] Mark Scott. "Chinese diplomacy ramps up social media offensive in COVID-19 info war." *Politico*. 29 April 2020. https://www.politico.eu/article/china-disinformation-covid19-coronavirus/.

[30] "Coronavirus: Fake news crackdown by UK government." *BBC News*. 30 March 2020. https://www.bbc.com/news/technology-52086284.

[31] Andrea Bellemare, Jason Ho, and Katie Nicholson. "Quebec Police Investigating Possible Link Between Cell Tower Fires and 5G Coronavirus Conspiracy Theories." *CBC News*. 8 May 2020. https://www.cbc.ca/news/canada/coronavirus-conspiracy-theory-5g-fires-quebec-1.5560570.

[32] Murray Brewster. "Canadian-led NATO Battlegroup in Latvia Targeted by Pandemic Disinformation Campaign." *CBC News*. 24 May 2020. https://www.cbc.ca/news/politics/nato-latvia-battle-group-pandemic-covid-coronavirus-disinformation-russia-1.5581248.

[33] "EEAS Special Report Update: Short Assessment of Narratives and Disinformation Around the COVID-19/Coronavirus Pandemic (Updated 2-22 April)." *EUvsDisinfo*. 24 April 2020. https://euvsdisinfo.eu/eeas-special-report-update-2-22-april/.

[34] "FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic." *Federal Bureau of Investigation*. 13 April 2020. https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic.

[35] "COVID-19 Fraud." *Canadian Anti-Fraud Centre*. 9 April 2020. https://antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-eng.htm; Mark Townsend. "Fraudsters exploiting COVID-19 fears have scammed £1.6m." *The Guardian*. 4 April 2020. https://www.theguardian.com/world/2020/apr/04/fraudsters-exploiting-covid-19-fears-have-scammed-16m . .

[36] "COVID-19 Fraud." *Canadian Anti-Fraud Centre*. 9 April 2020. https://antifraudcentre-centreantifraude.ca/features-vedette/2020/covid-19-eng.htm.

[37] "FBI Warns of Advance Fee and BEC Schemes Related to Procurement of PPE and Other Supplies During COVID-19 Pandemic." *Federal Bureau of Investigation*. 13 April 2020. https://www.fbi.gov/news/pressrel/press-releases/fbi-warns-of-advance-fee-and-bec-schemes-related-to-procurement-of-ppe-and-other-supplies-during-covid-19-pandemic.

[38] Tristan de Souza. "COVID-19 Critical Infrastructure Cyber Threat Brief." *Cyjax*. 4 May 2020. https://www.cyjax.com/download/covid-19-critical-infrastructure-cyber-threat-brief/.

[39] Tristan de Souza. "COVID-19 Critical Infrastructure Cyber Threat Brief." *Cyjax*. 4 May 2020. https://www.cyjax.com/download/covid-19-critical-infrastructure-cyber-threat-brief/.