TLP:WHITE

Communications
Security Establishment

Centre de la sécurité
des télécommunications

CANADIAN CENTRE FOR
CYBER SECURITY

CYBER THREAT BULLETIN: The Continued Impact of COVID-19 on Cyber Threat Activity

Canada

ABOUT THIS DOCUMENT

AUDIENCE

This Cyber Threat Bulletin is intended for the cyber security 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 Canadian Centre for Cyber Security at contact@cyber.gc.ca.

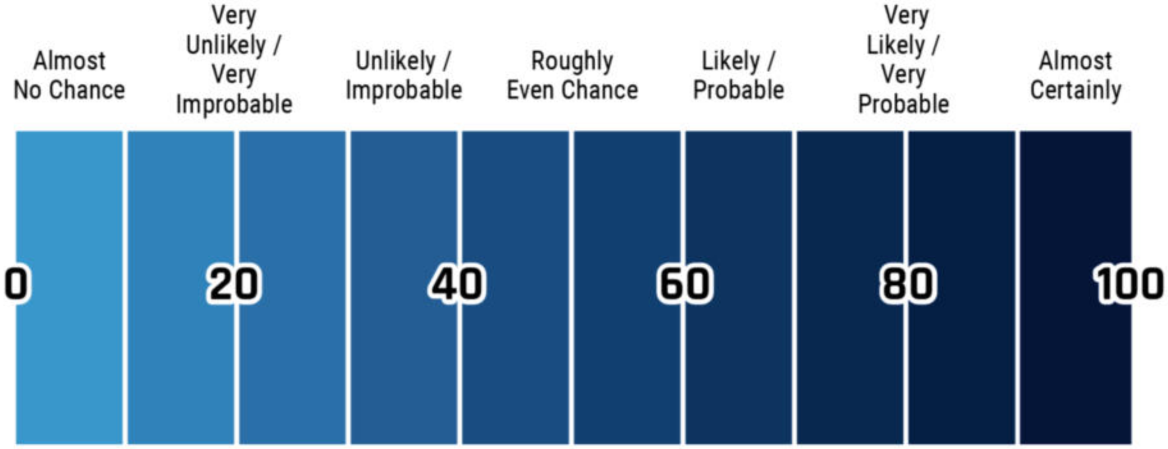
ASSESSMENT BASE AND METHODOLOGY

The key judgements in this assessment rely on reporting from multiples sources, both classified and unclassified. The judgements are based on the knowledge and expertise in cyber security of the Canadian Centre for Cyber Security (the Cyber Centre). 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 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 9 December 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.



INTRODUCTION

On 11 March 2020, the World Health Organization (WHO) officially declared the Novel Coronavirus disease 2019 (COVID-19) a global pandemic. In the panic and uncertainty of the initial spread of COVID-19, cybercriminals flooded the Internet with malware-laced phishing emails and fraudulent websites that purported to be official public health guidance or information on the emergency benefits and economic stimulus that would support Canadians while the country remained in a state of emergency. At the same time, state-sponsored cyber threat actors were quickly tasked with new intelligence requirements tied to the unfurling pandemic, including the theft of intellectual property related to the research and development of a COVID-19 vaccine candidate.

On 27 April 2020, the Canadian Centre for Cyber Security (the Cyber Centre) published *Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threat Activity*. This product informed Canadians on: cybercrime's growing preference for COVID-19-themed lures to initiate scams and distribute malware; the potential impacts of ransomware attacks on an overburdened Canadian healthcare system; and the potent cybersecurity risks of rapidly deploying a remote workforce across Canada. In June 2020, the Cyber Centre issued a follow-on assessment, *Cyber Threat Bulletin: Impact of COVID-19 on Cyber Threats to the Health Sector*, that assessed the growing vulnerability and harassment of Canada's front-line public health responses, its hospitals and medical research facilities, to cybercriminals and state-sponsored cyber threat actors during the height of the pandemic.

As of early December 2020, over 400,000 Canadians have contracted COVID-19 - nearly 13,000 have died.[1] On 9 December 2020, Health Canada authorized the first COVID-19 vaccine for use. While optimism is warranted, the Cyber Centre is aware that the global distribution of COVID-19 vaccines, including in Canada, will almost certainly face significant cyber threat activity. To this end, the Cyber Centre has released this cyber threat bulletin to assess whether past key judgements on the impact of COVID-19 on cyber threat activity hold up and what threats can be expected as Canada moves toward broadly distributing and administering the COVID-19 vaccine.

DO CYBER CENTRE'S KEY JUDGEMENTS ON COVID-19 CYBER THREAT ACTIVITY HOLD?

> *KEY JUDGEMENT:* "State intelligence collection requirements have shifted in response to COVID-19. We judge it is almost certain that cyber espionage directed at Canada will continue to attempt to steal Canadian intellectual property relating to COVID-19 medical research, as well as classified information regarding Government of Canada responses."

Following our initial assessments on state-sponsored intellectual property theft, Canada and its allies observed multiple state-sponsored cyberespionage campaigns against COVID-19 medical research organizations. In July 2020, Canada released a joint advisory with the US and the UK regarding APT29, a cyber espionage group assessed to almost certainly be operated by Russian intelligence services, and its targeting of various organizations involved in COVID-19 vaccine development in Canada, the United States and the United Kingdom.[2] We assessed that it was highly likely that APT29 acted with the intention of stealing information and intellectual property relating to the development and testing of COVID-19 vaccines, and we offered advice and guidance to prevent future compromises.

We assess that COVID-19 vaccine research will continue to be a significant target for state-sponsored cyber threat activity for the foreseeable future due to the increasing competition to establish a secure supply chain for domestic vaccine production. On 13 November 2020, Microsoft stated that Russian and North Korean hackers were still actively targeting vaccine researchers in Canada, France, India, South Korea, and the United States.[3] On 9 December 2020, European Medicines Agency networks were compromised and the regulatory submission for Pfizer and BioNTech's COVID-19 vaccine candidate was illegally accessed.[4] Similarly, IBM cybersecurity

[1] "Coronavirus disease (COVID-19)," *Government of Canada*, (accessed 9 December 2020). https://www.canada.ca/en/public-health/services/diseases/coronavirus-disease-covid-19.html

[2] "Advisory: APT29 targets COVID-19 vaccine development," *National Cyber Security Centre*, 16 July 2020. https://www.ncsc.gov.uk/files/Advisory-APT29-targets-COVID-19-vaccine-development-V1-1.pdf

[3] "Cyberattacks targeting health care must stop," *Microsoft Blog*, 13 November 2020. https://blogs.microsoft.com/on-the-issues/2020/11/13/health-care-cyberattacks-covid-19-paris-peace-forum/

[4] "Statement Regarding Cyber Attack on European Medicines Agency," *BioNTech*, 9 December 2020. https://investors.biontech.de/news-releases/news-release-details/statement-regarding-cyber-attack-european-medicines-agency/

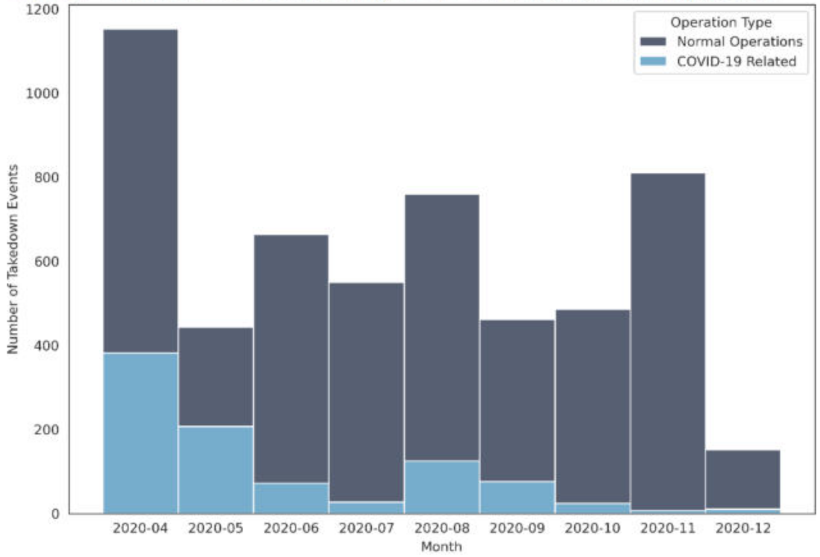
researchers revealed on 3 December a global phishing campaign directed against the COVID-19 "cold chain"—the suppliers which ensure safe transport and preservation of COVID-19 vaccines requiring temperature-controlled storage.[5]

> *KEY JUDGEMENT: "Online influence campaigns continue to erode trust in official statements and figures, weakening public health responses and exacerbating the public anxiety and uncertainty that make COVID-19-themed cyber threats so effective."*

The Cyber Centre remains aware of ongoing foreign online influence campaigns that amplify falsehoods regarding COVID-19, its origins, medical treatments, and the efficacy of ongoing public health efforts. The EU's External Action Service (EEAS) currently assesses that COVID-19-related online influence activity has decreased, but shifted in focus towards vaccine development and distribution.[6] While in many generic cases, influence activity is related to spreading and amplifying falsehoods regarding the safety of vaccines in general, the EEAS notes that Russia and China are engaging in "vaccine diplomacy," promoting their own COVID-19 vaccines while dismissing US efforts in state-controlled media.[7] While the impact of online influence activity, especially activity far-removed from Canadian media networks, is difficult to assess, **we judge that it is very likely that falsehoods related to COVID-19 vaccines that are spread or amplified by online influence campaigns will likely reduce confidence in the safety of Canada's vaccine rollout among some Canadians**.

> *KEY JUDGEMENT: "Cyber threat actors of varying motivations and sophistication are taking advantage of the COVID-19 pandemic as a thematic lure or subterfuge for their malicious activities, such as cyberespionage and cybercrime."*

Figure 1 - Malicious website takedowns, COVID-19 related vs. Normal Operations



Cybercriminals remain opportunistic and highly attuned to what captures the attention of their targets. In March-April 2020, this was news about the spread and impact of COVID-19. Such reporting has subsided more recently and other thematic lures have taken higher prominence, such as news about the US Presidential election. As shown in figure 1, data from a Cyber Centre third-party partner responsible for taking down malicious websites clearly shows a decrease in COVID-19-themed phishing websites since April-May 2020. **While this judgement has become less valid, the Cyber Centre expects cyber threat actors to leverage COVID-19 vaccine efforts as a thematic lure or subterfuge for their malicious activities, such as cyberespionage or cybercrime. We assess that phishing emails and fake websites will almost certainly masquerade as official Government of Canada communications pertaining to a COVID-19 vaccine rollout in order to entice Canadians to download malware, click malicious links, or divulge personal and financial information.**

[5] "IBM Uncovers Global Phishing Campaign Targeting the COVID-19 Vaccine Cold Chain," *IBM Security Intelligence*, 3 December 2020. https://securityintelligence.com/posts/ibm-uncovers-global-phishing-covid-19-vaccine-cold-chain/

[6] "EEAS SPECIAL REPORT UPDATE: Short Assessment of Narratives and Disinformation Around the COVID-19 Pandemic (UPDATE MAY - NOVEMBER),"*EUvsDisInfo*, EU External Action Service, 2 December 2020. https://euvsdisinfo.eu/eeas-special-report-update-short-assessment-of-narratives-and-disinformation-around-the-covid-19-pandemic-update-may-november/

[7] *Ibid*.

KEY JUDGEMENT: "The global health sector is under extreme pressure to mitigate the COVID-19 pandemic. We assess that, almost certainly, ransomware will continue to target healthcare and medical research facilities, jeopardizing patient outcomes and wider public health efforts."

The threat of ransomware to front-line healthcare and medical research facilities has only increased during the pandemic. Multiple Canadian hospitals have suffered ransomware attacks in recent months, including an attack on a local health board that caused Montreal's Jewish General Hospital to disconnect from the Internet.[8] The attack was very likely part of an ongoing campaign of sophisticated ransomware activity targeting North America's health sector by organized cybercriminal groups known to operate the TrickBot, Bazar, Ryuk, and Conti malware sets.[9] Most significantly, German prosecutors argue that cybercriminals contributed to the death of a patient who suffered a fatal aortic aneurysm after her ambulance was significantly delayed due to a ransomware attack in September.[10] **We assess that cybercriminals will almost certainly continue to jeopardize patient outcomes and wider public health efforts by deploying ransomware for financial gain against a vulnerable health sector, including the COVID-19 vaccine supply chain.**

KEY JUDGEMENT: "We expect the remote workforce almost certainly to be increasingly targeted by foreign intelligence services and cybercriminals. Cyber threat actors are already attempting to identify individuals working at home employed in areas of strategic interest and exploiting technologies deployed in support of a remote workforce, such as virtual private networks (VPNs) or video-conferencing platforms."

The Cyber Centre's assessments regarding the increasing cybersecurity risks associated with rapidly migrating large portions of Canada's workforce to remote work have largely borne out, and we assess that cybercriminals and state cyber actors alike have very likely become increasingly adept at compromising poorly managed or vulnerable VPN and cloud infrastructure. Since March 2020, the Cyber Centre and its international partners have issued several technical alerts and advisories regarding the active exploitation by sophisticated cyber threat actors of VPN and cloud appliances. These products are commonly used by remote workers to access sensitive corporate networks and assets. Most recently, on 7 December 2020, the US National Security Agency issued a cybersecurity advisory regarding ongoing state-sponsored exploitation of VMware identity management products commonly used to secure remote access to corporate and government networks.[11]

[8] "Quebec Health Network Targeted by Cyberattack," *The Globe and Mail*, 29 October 2020. https://www.theglobeandmail.com/canada/article-quebec-health-network-targeted-by-cyberattack/

[9] "Alert (AA20-302A) Ransomware Activity Targeting the Healthcare and Public Health Sector," *US-CERT*, 2 November 2020. https://us-cert.cisa.gov/ncas/alerts/aa20-302a

[10] "The untold story of a cyberattack, a hospital and a dying woman," *Wired*, 11 November 2020. https://www.wired.co.uk/article/ransomware-hospital-death-germany

[11] "Cybersecurity Advisory: Russian State-Sponsored Actors Exploiting Vulnerability in VMware® Workspace ONE Access Using Compromised Credentials," *National Security Agency*, 7 December 2020. https://media.defense.gov/2020/Dec/07/2002547071/-1/-1/0/CSA_VMWARE%20ACCESS_U_OO_195076_20.PDF