TLP:WHITE

Communications Security Establishment | Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

CYBER THREAT BULLETIN

Modern Ransomware and Its Evolution

18 SEPTEMBER 2020

TLP:WHITE

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 (Cyber Centre) at contact@cyber.gc.ca

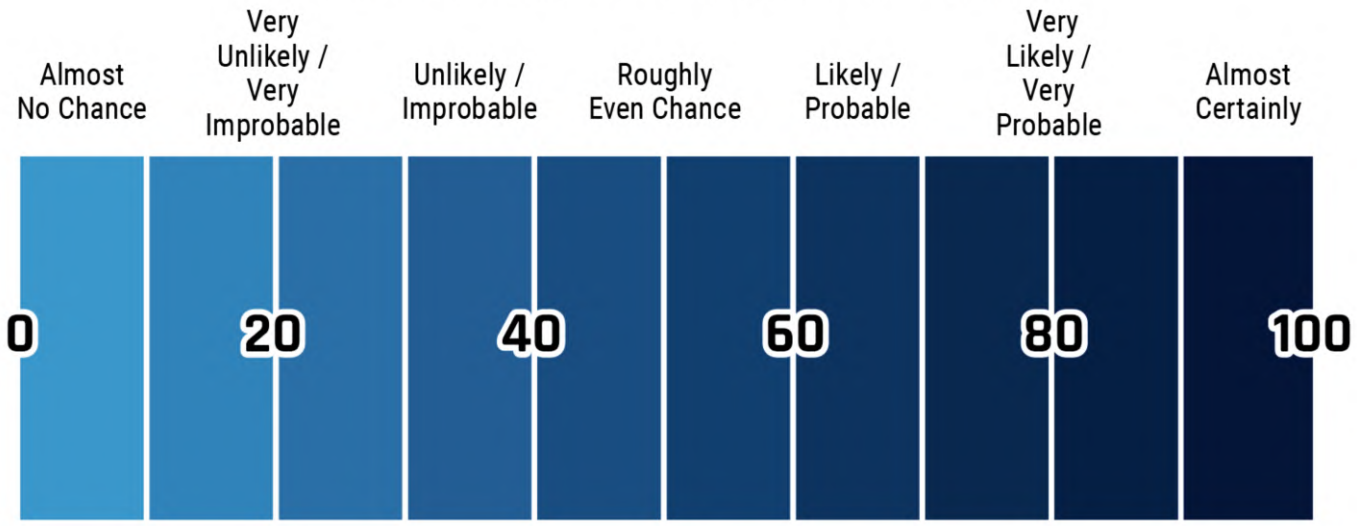
ASSESSMENT BASE AND METHODOLOGY

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 Cyber Centre. Defending the Government of Canada's information systems provides 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 13 August 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

- Canada often ranks among the top countries impacted by ransomware, although international comparisons are limited by gaps in data and contrasting methodologies. Further, we assess that it is almost certain that a majority of ransomware attacks against Canadian victims are unreported to authorities.
- Over the past two years, ransomware campaigns have impacted hundreds of Canadian businesses and critical infrastructure providers, including multiple hospitals and police departments, as well as municipal, provincial, and territorial governments.
- We judge that, almost certainly, ransomware directed against Canada in the next 12 months will continue to target large enterprises and critical infrastructure providers, as well as organizations of all different sizes. Many Canadian victims will continue to acquiesce to ransom demands due to the severe economic and potentially destructive consequences of refusing payment.
- We assess that it is almost certain that cybercriminals will continue to scale up their ransomware operations and attempt to coerce larger payments from victims by threatening to leak or sell their data online.
- Modern ransomware is dependent upon several technologies (e.g., cryptocurrencies) and services available in online criminal marketplaces, and without them we judge it almost certain that ransomware would be cost-prohibitive for cybercriminals.
- The success of modern ransomware is dependent upon locations with lax or non-existent laws and law enforcement against cybercrime. We assess that ransomware activities would be much more difficult for cybercriminals to undertake if they could not find locations from which to operate with near impunity.
- We assess that it is likely that multiple state cyber threat actors will use ransomware to obfuscate the origins or intentions of their cyber operations. Additionally, multiple states almost certainly maintain associations with cybercriminals that engage in ransomware activities. In some cases, cybercriminals provide assistance to intelligence services which allows the cybercriminals to operate free from law enforcement.

INTRODUCTION

Ransomware is a form of malware that uses encryption to disrupt Information Technology (IT) systems, typically to impede organizational functions that depend on having unfettered access to data. These tasks can be critical to human safety or business continuity, and once disrupted, threat actors extort their victims by demanding payment to decrypt the data. In 2019, cybercriminals reportedly attempted to extort an estimated $25B CAD from victims worldwide using ransomware.[i] This dollar figure exists in addition to costs resulting from downtime, data corruption, data theft, and other expenses.

In 2019, ransomware campaigns impacted hundreds of Canadian businesses and critical infrastructure providers, including multiple hospitals and police departments, as well as municipal, provincial, and territorial governments. Although international comparisons are limited by gaps in data and contrasting methodologies, Canada often ranks among the top countries impacted by ransomware. For example, in 2019, Canadian submissions to the ID Ransomware service—an online portal that provides information and, if available, decryption tools to victims of ransomware—were closely comparable in per capita terms to submission figures from other top targeted countries such as Australia, Italy, Germany, and France.[ii] We assess that Canada's elevated level of targeting is probably due to a combination of a high level of Internet use for banking and other services, the relatively high wealth of Canadian individuals and companies, and Canadians' willingness to pay ransoms in return for their data.

Ransomware operations continually evolve, and the most recent trend is for them to target strategically important organizations, such as those involved in critical infrastructure, national defence, or technologies relevant to national security.

KEY RANSOMWARE VARIANTS AND OPERATORS

CRYPTO LOCKER	Ransomware created by Russian cybercriminal Evgeniy Bogachev in 2013, considered the first modern ransomware variant, distributed by the GameOverZeus malware, whose operators included Bogachev and Evil Corp members.
EVIL CORP	A Russia-based organized cybercriminal group responsible for the Dridex malware and multiple ransomware campaigns since 2015. In December 2019, Evil Corp members were indicted and sanctioned by the US for their ongoing cybercriminal activities and for providing assistance to a Russian intelligence service.
FIN6	An organized cybercriminal group, likely Russian-speaking, reportedly linked to multiple Ryuk and Megacortex infections since 2018, but active since 2015.
MAZE	A ransomware variant whose operators are known to leak victim data for non-payment. Active since at least November 2019.
MEGA CORTEX	A ransomware variant discovered in 2019 observed targeting Industrial Control Systems processes, reportedly linked to Trickbot and FIN6 operations.
RYUK	A ransomware variant known to target large enterprises, hospitals and critical infrastructure and demand extremely large ransoms. Active since August 2018. Ryuk is affiliated with multiple Russian-speaking cybercriminals, including the operators of Trickbot.
SAMSAM	A ransomware variant used by Iranian cybercriminals that compromised multiple municipalities, hospitals, universities, and businesses in Canada, the US, the UK, and other countries primarily during 2015-2018.
SODINOKIBI	A ransomware variant, whose Russian-speaking developers hire other cybercriminals to distribute and deploy their ransomware.
TRICKBOT	A banking trojan used to steal financial data and online banking credentials. Trickbot is affiliated with multiple Russian-speaking cybercriminals and is a primary distributor of the Ryuk ransomware.

A BRIEF HISTORY OF RANSOMWARE

From proof of concept to automation

While proof-of-concept ransomware appeared as early as 1989, the first modern campaign is typically attributed to the CryptoLocker ransomware, administered by Russian cybercriminal Evgeniy Bogachev and his associates in 2013. Bogachev used CryptoLocker as a way of extracting further value from victims of his other creation, the infamous GameOverZeus malware. From September 2013 to May 2014, according to FBI reports, CryptoLocker infected nearly 500,000 victims, earning as much as $27M CAD.[iii]

From 2014 to 2016, the CryptoLocker model of ransomware—typically emails with malicious attachments distributed through scattershot campaigns—proliferated, especially within the Russian-speaking cybercrime community, many the former associates of Bogachev. These early ransomware campaigns generally demanded $500 to $3,000 CAD per ransom and relied on scale because relatively few victims would end up paying. Threat actors realized that the labour costs required to manually compromise and extort payment from each victim were too high and looked to automated processes to reduce costs and increase profits. Ransomware evolved to incorporate a great deal of automation that ushered victims through the extortion and payment process. Threat actors also incorporated other techniques to increase the odds of payment. For example, they introduced 24/7 live chat support and opportunities to decrypt one or more files for free as a guarantee that decryption was possible. This helped provide uncertain victims with the guidance and assurance they needed to pay up.

From scattershot campaigns to hunting high-value targets

Ransomware evolved as threat actors moved away from automated, scattershot ransomware campaigns towards the manual targeting of large organizations. Although the costs of these operations were higher, threat actors learned that large organizations were more willing to pay out significantly larger ransoms to recover from disruptions as quickly as possible. In December 2015, Iranian cybercriminals began targeting hospitals, municipalities, and public institutions in Canada, the UK, and the US with ransomware known as SamSam, earning more than $7.8M CAD from over 200 victims by November 2018, including the University of Calgary.[iv] SamSam became a model for today's targeted ransomware campaigns. Also known as "Big Game Hunting", targeted ransomware attacks have hit thousands of healthcare and other critical infrastructure providers, governments, and large businesses. In March 2019, a Norwegian aluminium company shut down production facilities due to a targeted ransomware attack, resulting in nearly $100M CAD in damages.[v]

Today, successful cybercriminals in the ransomware racket are able to rapidly develop and adapt their malware to capitalize on evolving global, national, or regional contexts, and the resultant changes in the vulnerabilities of certain organizations. In March 2020, during the COVID-19 pandemic, a ransomware campaign struck 11 US hospitals; the same group had targeted three Canadian hospitals and a Canadian municipal government in fall 2019.[vi]

THE ENABLING FACTORS OF MODERN RANSOMWARE

Modern ransomware is dependent upon several technologies (e.g., cryptocurrencies) and services available in online criminal marketplaces, and without them we judge it almost certain that ransomware would be cost-prohibitive for cybercriminals. Ransomware has evolved alongside legitimate sectors of the economy such as the financial sector, to take advantage of plummeting costs in data storage and computing, increased bandwidth and connectivity, and the creation of an Internet services economy. However, in contrast with legitimate sectors, modern ransomware is dependent upon cryptocurrencies and cryptocurrency-laundering services, and jurisdictions with lax or non-existent laws and law enforcement against cybercrime.

Wild growth of data and Internet-connected systems

The trend of computing over the past decades has been towards major increases in Internet connectivity, computing power and data storage at continually decreasing costs. This has been accompanied by the creation of an ever-increasing amount of personal and proprietary data, as well as the connection to the Internet of more and more crucial IT systems for businesses, universities, industries and governments. The analog world has become digitized and connected to include online personas, shopping, banking, corporate communications, industrial control systems and more. As a result, by the 2010s, data and systems that could be held at ransom had become abundant, vulnerable to ransomware and increasingly important to organizations and people that were unprepared to cope with a loss of data.

Cryptocurrency and the payment system

The advent of cryptocurrencies such as Bitcoin created a transnational financial infrastructure that facilitates anonymous, rapid and global payments. Cryptocurrency transactions are *immutable* (i.e., transactions cannot be reversed) and *verifiable* (i.e., transactions are always public and can be automatically confirmed); these are critical features that ensure ransom payments cannot be reversed once the victim's files are decrypted. Bitcoin gained prominence in several online markets

selling illegal goods from 2011 to 2013 and cybercriminals adopted Bitcoin as the standard form of ransom payment around 2013.

Before cryptocurrencies and related laundering services, cybercriminals relied almost entirely on traditional money-laundering mechanisms such as wiring stolen money to intermediary accounts in the victim country and employing criminals or unwitting locals to quickly move the funds onward to foreign banks or poorly regulated online payment systems. These intermediaries could charge up to 60% of the value of the transaction. In comparison, cryptocurrency transactions typically cost under 5% of the value of the transaction.

Anonymous and secure communications with victims

Until secure communications applications and the dark web (i.e., Internet networks only accessible though specialized anonymization software) became widely trusted and easily accessible to cybercriminals and potential victims, most cybercriminals lacked the ability to securely communicate with their victims to facilitate the ransom process. Secure communications applications and dark web networks provide a place for cybercriminals to stake out the Internet property they require to undertake their criminal business.

Cybercriminal market specialization

Global cybercrime thrives on market-driven specialization. For example, a cybercriminal may be an excellent software developer but lack the hacking skills required to target and compromise victims. Cybercrime marketplaces offer the cybercriminal access to other cybercriminals who specialize in the skills they lack such as email spam campaigns, hosting malicious websites, or operating botnets of pre-compromised victims. Reflecting this specialization, it is not uncommon for a ransomware victim to be compromised by multiple pieces of malware that are purposefully designed to execute one or more steps of what is required for a "successful" ransomware event. Since ransomware renders a system inoperable, it is almost always the final malware in a chain of infections. Many of the most impactful bank fraud and ransomware campaigns, such as Trickbot and Ryuk, involve several specialised cybercriminal groups working together according to various financial and service arrangements to identify and extract as much value as possible from lucrative victims.

Protections from law enforcement

Ransomware would be much more difficult for cybercriminals to undertake if they could not find locations from which to operate that have legal structures or law enforcement regimes that tolerate cybercrime. For example, many ransomware variants will not execute on systems with Russian or other neighbouring language or location settings. We assess that this is almost certainly to avoid attracting scrutiny from law enforcement in Russia, which is known to tolerate financially-motivated cybercriminal activity so long as it is not directed domestically, and to a lesser extent, against regional allies.

EMERGING TRENDS: RANSOMWARE IN 2020-2021

We assess that ransomware in 2021 will very likely be characterized by novel methods of scaling up campaigns and coercing larger payments from victims. We expect that cybercriminals will almost certainly benefit from greater specialization within the criminal market and engage in service and financial agreements to enable their activities. Further, we assess that cybercriminals will almost certainly continue to target critical infrastructure and heavy industry due to expectations of higher and more forthcoming ransom payments regardless of the potentially destructive consequences of these activities.

Adopting more sophisticated tactics

To identify and compromise high-value targets many ransomware operators are adopting sophisticated tactics more commonly associated with state-sponsored groups than cybercriminals. For example, Cyber Centre has recently observed certain ransomware operators take advantage of publicly disclosed cyber security vulnerabilities at nearly the same speed as state-sponsored cyber threat actors.[vii]

Increasing value of ransom demands

As ransomware campaigns have become more capable of identifying and compromising high-value targets there has been a subsequent increase in the value of ransom demands. Ransomware researchers estimate that the average ransom demand increased by 33% since Q4 2019 to $111,605 CAD in Q1 2020 due to the impact of targeted ransomware operations.[viii] The average ransom demand spiked in December 2019 at $257,756 CAD and we assess that 2020 will very likely see one or more months exceed this figure.[ix]

At the more extreme end of the spectrum are multi-million-dollar ransom events, which have become increasingly common. In October 2019, a Canadian insurance company paid $1.3M CAD to recover 20 servers and 1,000 workstations.[x] In April 2020, cybercriminals demanded $15M CAD in ransom from Portuguese energy giant *Energias de Portugal* (EDP).[xi]

Targeting managed service providers to get at their clients

We judge it very likely that ransomware campaigns will increasingly target managed service providers (MSPs)—companies that host and manage their clients' IT—for the purpose of targeting their downstream clients as a means of efficiently scaling targeted ransomware campaigns in the future. Since at least 2019, ransomware operators have compromised MSPs and used remote management software to automatically install ransomware payloads on multiple client networks at once.[xii] In August 2019, Sodinokibi affiliates compromised TSM Consulting, a Texas-based MSP, to infect 22 US municipalities and demand over $3M CAD.[xiii]

Innovative tactics to coerce payment

We assess that an increasing number of ransomware operators will leak victim data to punish payment refusals. Targeted ransomware attacks often allow cybercriminals to access trade secrets, intellectual property, and databases of sensitive employee and customer data. Since November 2019, operators of the Maze ransomware have demanded ransom for the decryption of locally-stored data as well as the destruction of exfiltrated copies. Victims unwilling to pay have had their data leaked or sold online. Maze is also known to publish victim data during negotiations to prove they have it and likely pressure payment via media attention. As of August 2020, at least sixteen ransomware campaigns have fulfilled threats to leak victim data.[xiv]

Disrupting industrial control systems

In recent years, ransomware has increasingly impacted industrial control systems (ICS) responsible for the control and monitoring of physical equipment used by heavy industry and critical infrastructure providers. We assess that ransomware operators have almost certainly become so adept at propagating through corporate IT networks that adjacent ICS environments are increasingly vulnerable to disruption. For example, in February 2020, ransomware impacted a US natural gas compression facility, traversing Internet-facing networks into ICS assets responsible for monitoring pipeline operations.[xv]

In some cases, victims have chosen to disable their industrial processes as a precautionary measure during a significant ransomware event. For example, in March 2019, Norsk Hydro, a Norwegian aluminum company, was impacted by ransomware that disrupted its logistical and production data so severely that it prompted the shutdown of ICS and reversion to manual operations.[xvi]

We assess that it is almost certain that at least seven ransomware variants have exhibited motivations to target ICS environments. Since January 2019, these ransomware families have contained instructions to terminate multiple, in one case, over a hundred, ICS processes.[xvii] The impact of these attacks vary according to the specific circumstances of the ICS processes and the reaction of the site staff.[xviii]

HOW STATES USE AND BENEFIT FROM RANSOMWARE

We assess that it is likely that multiple state cyber threat actors will use ransomware to obfuscate the origins or intentions of their cyber operations. Additionally, multiple states almost certainly maintain associations with cybercriminals that engage in ransomware activities. In some cases, cybercriminals provide assistance to intelligence services which allows the cybercriminals to operate free from law enforcement.

Ransomware as a weapon

The Democratic People's Republic of Korea (DPRK) was responsible[xix] for the introduction of WannaCry ransomware into cyberspace on 12 May 2017, which infected more than 200,000 machines in over 150 countries, including the UK National Health Service.[xx]

On 27 June 2017, cyber threat actors launched destructive cyber attacks masquerading as ransomware against Ukraine that quickly proliferated globally. Ukraine's public and private infrastructure, including banking, transport, and other critical infrastructure, was severely disrupted. Dubbed the NotPetya ransomware, the attacks caused over ten billion CAD in global damages. Pharmaceutical giant Merck reportedly incurred losses exceeding a billion CAD and Danish shipping company, A.P. Møller-Maersk, lost $390M CAD.[xxi] Canada has assessed that Russian actors developed the NotPetya ransomware.[xxii] Australia[xxiii], New Zealand[xxiv], the UK[xxv], and the US[xxvi] assess that Russia was directly responsible for the June 2017 attack.

Ransomware as a smokescreen for state-sponsored cybercriminal activity

In February 2016, DPRK-sponsored cybercriminals reportedly purchased and installed ransomware on Taiwan-based Far Eastern International Bank's networks.[xxvii] Cyber security researchers who subsequently analyzed samples of the malware, determined that the encrypted data was not recoverable. They assessed that the ransom aspect of the malware was almost certainly a ruse, and that the true purpose was to destroy evidence and impede an investigation into allegations that DPRK-linked cybercriminals had stolen money through fraudulent SWIFT transfers.[xxviii]

State links to operators of ransomware

On 5 December 2019, the US Department of Treasury sanctioned the Evil Corp organized cybercrime group for, among other things, collecting information and conducting cyber operations on behalf of Russian intelligence services since at least 2017.[xxix]

Evil Corp and its criminal associates have been attributed by industry sources to multiple high-profile ransomware variants commonly known as Locky, BitPaymer, DoppelPaymer, and, most recently, WastedLocker. Since April 2020, WastedLocker has compromised multiple high-value targets in Canada, the UK, and the US, chiefly affecting large-scale manufacturing and

technology companies. In July 2020, Garmin, an American company focused on GPS technology, reportedly paid millions of dollars in ransom to WastedLocker's operators to recover its data and halt disruption of its services.[xxx]

RANSOMWARE ACTIVITY AGAINST CANADA

We expect that, almost certainly, ransomware directed against Canada in the next 12 months will continue to target large enterprises and critical infrastructure providers, as well as organizations of all different sizes. Further, many Canadian victims will almost certainly acquiesce to ransom demands due to the severe economic and potentially destructive consequences of refusing payment.

- In 2019, ransomware compromised multiple Canadian municipal, provincial, and territorial governments, including the Ontario City of Woodstock that incurred over $660,000 CAD in damages after refusing to pay its attackers.[xxxi]
- In December 2019, Bird Construction, a Toronto-based construction company that has secured 48 contracts with Canada's Department of National Defence since 2006, was comprised by Maze ransomware. [xxxii]
- In April 2020, Northwest Territories Power Corporation was compromised by ransomware and its corporate services disrupted.[xxxiii]

Since late 2019, multiple Canadian businesses and a provincial government have had their data publicly leaked by ransomware operators for refusing payment. The Maze ransomware operators that compromised Bird Construction allegedly published the company's stolen data online after the company refused to pay a ransom. In June 2020, a consortium of Canadian agricultural companies had its corporate data made available for auction on the Sodinokibi ransomware group's website.

While public services and healthcare providers are often the most visibly impacted, we assess that it is almost certain that the majority of high impact ransomware attacks against Canada affect medium or large private sector organizations and are unreported to authorities. Throughout 2019-2020, Cyber Centre became aware of hundreds of Canadian victims across a wide range of commercial sectors as well as multiple municipalities, police services, and education providers that were compromised by the Ryuk ransomware variant. As of Q1 2020, the Ryuk ransomware's average ransom payment (worldwide) is estimated at $1.7M CAD.[xxxiv]

[i] "Report: The Cost of Ransomware in 2020. A Country by Country Analysis," Emsisoft Malware Lab, 11 February 2020
[ii] "Report: The Cost of Ransomware in 2020. A Country by Country Analysis," Emsisoft Malware Lab, 11 February 2020
[iii] "U.S. Leads Multi-National Action Against GameOver Zeus Botnet and Cryptolocker Ransomware, Charges Botnet Administrator," US Department of Justice, Office of Public Affairs, 2 June 2014
[iv] "Two Iranian Men Indicted for Deploying Ransomware to Extort Hospitals..." US Department of Justice Office of Public Affairs, 28 November 2018
[v] "Hackers hit Norsk Hydro with Ransomware. The Company Responded with Transparency," Microsoft, 16 December 2019
[vi] "Ryuk Keeps Targeting Hospitals During the Pandemic," Bleepingcomputer, 26 March 2020
[vii] For example, active exploitation of multiple gateway and VPN vulnerabilities discovered in 2019 and 2020. See: "Active Exploitation of F5 BIG-IP Vulnerability," Canadian Centre for Cyber Security, 5 July 2020; "Active Exploitation of Citrix Vulnerabilities," Canadian Centre for Cyber Security, 17 January 2020; and, "Active Exploitation of VPN Vulnerabilities," Canadian Centre for Cyber Security, 17 September 2019
[viii] "Q1 2020 Ransomware Marketplace Report," Coveware, 29 April 2020
[ix] "Ransomware Attacks Grow, Crippling Cities and Businesses," The New York Times, 9 February 2020
[x] "Canadian insurance company lost nearly US$1M in ransomware attack," CTV News, 30 January 2020
[xi] "RagnarLocker Ransomware Hits EDP Energy Giant, Asks for 10M," Bleepingcomputer, 14 April 2020
[xii] "Ransomware Gang Hacks MSPs to Deploy Ransomware on Customer Systems," ZDNet, 20 June 2019
[xiii] "Managed Service Providers are Ransomware Hacker's New Gold Mine," Houston Chronicle, 16 September 2019
[xiv] "List of Ransomware that Leaks victims' stolen files if not paid" Bleepingcomputer, 26 May 2020 (Updates)
[xv] "Alert (AA20-049A): Ransomware Impacting Pipeline Operations," US DHS/CISA Alert, 18 February 2020
[xvi] "Ransomware Against the Machine: How Adversaries Are Learning to Disrupt Industrial Production by Targeting IT and OT," FireEye, 24 February 2020
[xvii] "Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families," FireEye, 15 July 2020
[xviii] "EKANS Ransomware and ICS Operations," DRAGOS, 3 February 2020
[xix] "CSE Statement on the Attribution of WannaCry Malware," Communications Security Establishment of Canada, 19 December 2017
[xx] "Investigation: WannaCry cyber attack and the NHS," Report by the Comptroller and Auditor General, Department of Health, National Audit Office, HC 414 SESSION 2017–2019, 25 APRIL 2018
[xxi] "The Untold Story of NotPetya, the Most Devastating Cyberattack in History," WIRED, 22 August 2018
[xxii] "CSE Statement on the NotPetya Malware," Communications Security Establishment of Canada, 18 February 2018
[xxiii] "Australian Government attribution of the 'NotPetya' cyber incident to Russia," Statement by Minister for Law Enforcement and Cyber Security Angus Taylor, 16 February 2018
[xxiv] "New Zealand joins international condemnation of NotPetya cyber-attack," Government Communications Security Bureau, 16 February 2018
[xxv] "Russian military 'almost certainly' responsible for destructive 2017 cyber attack," National Cyber Security Centre, 16 February 2018
[xxvi] "*In June 2017, the Russian military launched the most destructive and costly cyber-attack in history.*" See: "Statement from the Press Secretary of the White House on NotPetya," The White House, 15 February 2018
[xxvii] "North Korean Hackers Used Hermes Ransomware to Hide Recent Bank Heist," Bleepingcomputer, 17 October 2017
[xxviii] "North Korean Hackers Used Hermes Ransomware to Hide Recent Bank Heist," Bleepingcomputer, 17 October 2017
[xxix] "Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware," US Department of the Treasury Press Release, 5 December 2019
[xxx] "Garmin Pays Up to Evil Corp After Ransomware Attack – Reports," ThreatPost, 3 August 2020
[xxxi] "Cyber attack costs Woodstock more than 660k Report," Woodstock Sentinel-Review, 9 December 2019
[xxxii] "Ransomware attack on construction company raises questions about federal contracts," CBC News, 26 January 2020
[xxxiii] "NTPC confirms cyber attack from unknown source on Thursday, RCMP investigating," CBC News, 30 April 2020
[xxxiv] "Ransomware payments up 33% as Maze and Sodinokibi Proliferate in Q1 2020" Coverware, 29 April 2020