Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR
CYBER SECURITY

CYBER THREAT BULLETIN:
The Ransomware Threat in 2021

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 the Canadian Centre for Cyber Security at contact@cyber.gc.ca.

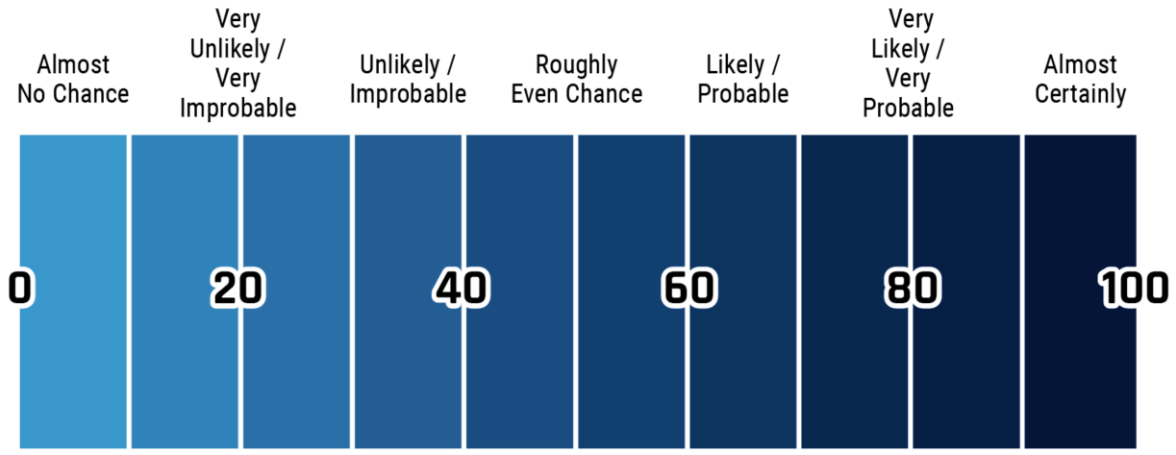
ASSESSMENT BASE AND METHODOLOGY

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. The Communications Security Establishment (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 16 November 2021.

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.



THE RANSOMWARE THREAT IN 2021

2021 has been marred by a series of high-profile ransomware attacks around the world. To many, the Colonial Pipeline attack in the US was a shocking introduction to ransomware attacks and how they can affect the lives of millions. For five days in May, this ransomware attack caused a shutdown of the largest fuel pipeline in the US, leading to price spikes and fuel shortages for millions of Americans. This attack shows some of the key trends of ransomware in 2021: brazen, sophisticated, increasing in frequency, and, for the cybercriminals, very profitable. The scale and scope of ransomware operators represent both security and economic risks to Canada and its allies.

Put simply, ransomware is a form of malware to encrypt files on a device. The threat actor then demands a ransom in exchange for decryption. Ransomware is not a new problem. Observed as early as 1989, over the past 15 years ransomware has become one of the most popular types of cybercrime.

Last year, the Cyber Centre published an assessment, *Cyber Threat Bulletin: Modern Ransomware and Its Evolution*, in which we detailed the evolution in the scale and tactics of ransomware operations and predicted the trend toward higher profile, sophisticated attacks leading to ever-increasing ransom demands.

Sadly, this prediction has become reality. In the first half of 2021, global ransomware attacks increased by 151% when compared with the first half of 2020. This year has also been marked by the highest ransoms and the highest payouts.[1] In Canada, the estimated average cost of a data breach, a compromise that includes but is not limited to ransomware, is $6.35M CAD.[2]

The Cyber Centre has knowledge of 235 ransomware incidents against Canadian victims from 1 January to 16 November 2021. More than half of these victims were critical infrastructure providers. It is important to note, however, that most ransomware events remain unreported. Once targeted, ransomware victims are often attacked multiple times.[3] The Cyber Centre continues to regularly observe high-impact ransomware campaigns that can cripple businesses and critical infrastructure providers.

The impact of ransomware can be devastating, and the severity of the financial consequences related to a ransomware attack can be profound. An increasingly common tactic by ransomware operators is to publicly release a victim's data if they do not pay the ransom.[4] In May 2021, details relating to 520 patients of Ireland's Health Service Executive were published online following a Conti ransomware attack.[5] Data breaches come with their own costs, both financial and reputational.

Throughout 2021, several Canadian senior officials, including the Minister of Public Safety, the Chief of CSE, and the Head of the Cyber Centre publicly noted that ransomware was the foremost cyber threat facing Canadians and Canadian organizations.[6] In April 2021, the international Ransomware Task Force, an effort by the US-based Institute for Security and Technology in partnership with 60 cybersecurity experts from industry, government, law enforcement, and civil society—among them the Royal Canadian Mounted Police (RCMP)'s National Cybercrime Coordination Unit—reinforced the collective effort required to mitigate the ransomware threat.[7] On 13 October 2021, Canada participated in the Counter-Ransomware Initiative meetings facilitated by the White House National Security Council.

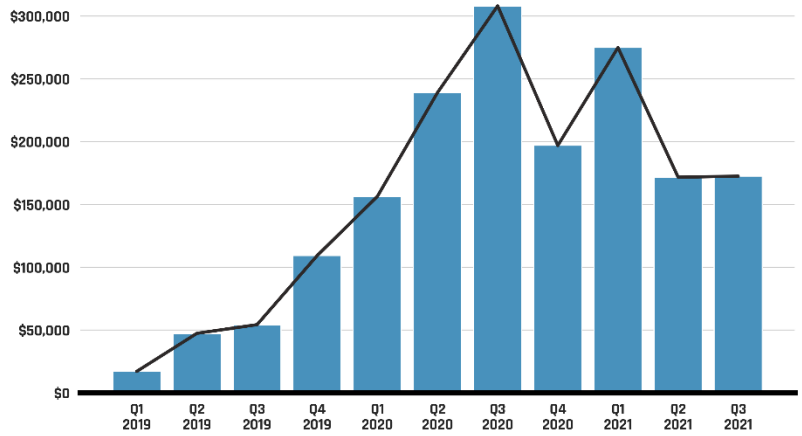
This cyber threat bulletin provides an update to Canadians about the threat from ransomware in Canada and how we expect that threat to evolve over the next year.

EVOLVING TRENDS

Ransomware-as-a-Service

The increased impact and scale of ransomware operations from 2019 to 2021 has been largely fueled by the growth of the Ransomware-as-a-Service (RaaS) business model, by which developers sell or lease ransomware to other cybercriminals. These affiliate schemes provide skilled attackers with the ability to distribute ransomware campaigns, with the developer behind the ransomware receiving a percentage of each victim's ransom payment.

Figure 1 - Average Ransom Payment Over Time



Known ransom payments, after increasing rapidly from 2019 to 2020, appear to have stabilized around $200,000 in 2021, down slightly from 2020 levels (see Figure 1).[8] At the same time, in 2021, the global average total cost of recovery from a ransomware incident (i.e., the cost of paying the ransom and/or remediating the compromised network) has more than doubled this year, increasing from $970,722 CAD in 2020 to $2.3M CAD in 2021.[9] **We assess that ransom payments are likely reaching a market equilibrium, where cybercriminals are becoming better at tailoring their demands to what their victims are most likely to pay given the growth of recovery cost and the risk of reputational damage from public data leaks.** For large enterprises and critical infrastructure providers, many sophisticated ransomware groups are still demanding increasingly exorbitant amounts, with 2021 seeing the largest ransom payment ever at $48.4M CAD.[10]

High-Impact Targeting

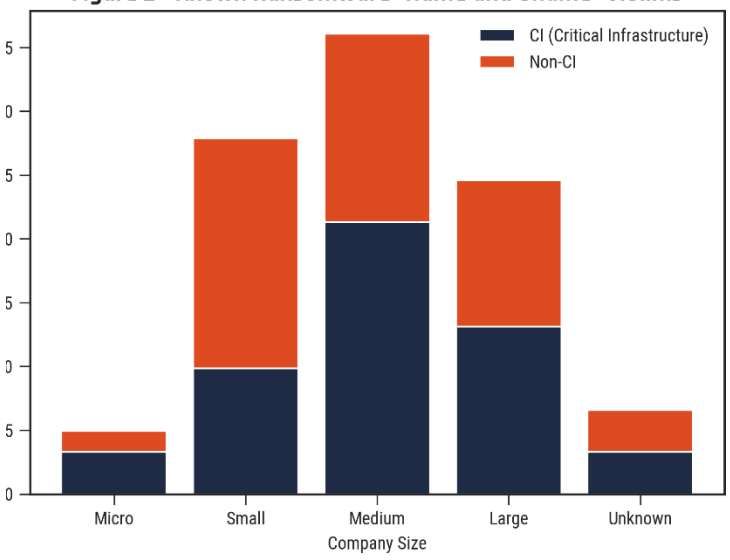
On 2 July 2021, Sodinokibi (also referred to as "REvil"), a Russian-speaking cybercriminal group that operates the ransomware of the same name, leveraged a vulnerability in Kaseya VSA, a network management software, to compromise approximately 800 to 1500 downstream organizations. Ransomware was deployed on the compromised victim networks via an automated, fake, and malicious software update.[11] **We assess that ransomware operators are likely to continue to target software supply chains in order to maximize the number of potential victims and profits.** We have also seen some cybercriminals move from indiscriminate and generic, automated campaigns to more targeted attacks that require human "hands-on-keyboard" hacking techniques.

As in other forms of financially motivated crime, ransomware operators seek to maximize their profits. While attacks on larger, better-defended targets take more time and expertise to execute, larger organizations continue to be targeted as they are more able to pay higher ransom demands, and are therefore a more lucrative target for skilled ransomware operators. As the Chief of CSE noted in May 2021: "Critical infrastructure and large enterprises are the most lucrative ransomware targets, because they are the least able to tolerate operating disruptions and they have the deepest pockets."[12]

From 1 January to 30 June 2021, more than half of all Canadian victims impacted by ransomware belonged to a critical infrastructure sector, such as energy, health, and manufacturing. The COVID-19 pandemic has made organizations like hospitals, governments, and universities more mindful of the risks tied to losing access to their networks and often feeling resigned to pay ransoms. Cybercriminals have taken advantage of this situation by significantly increasing the value of their ransom demands.

We assess that ransomware operators will almost certainly continue to target large organizations with operational technology (OT) assets, including organizations in Canada, to try to extract ransom, steal intellectual property and proprietary business information, and obtain personal data about customers. Even if the cyber activity is contained in the information technology (IT) network of an OT asset owner, there is still a possibility of an OT shutdown.[13] For example, in May 2021, Colonial Pipeline, operator of one of the largest refined products pipelines in the US, suffered an incident attributed to the Russia-based DarkSide RaaS cybercriminal group. Although the activity was reported to be restricted to the IT systems, the company's operations were affected, resulting in record price increases, panic-buying, and gasoline shortages.[14]

Figure 2 - Known Ransomware "Name and Shame" Victims



Leveraging the COVID-19 pandemic

Ransomware groups have also increased their targeting of emergency medical services and law enforcement agencies, which have struggled to manage the COVID-19 pandemic. For example, on 14 June 2021, Humber River Hospital in Ontario was forced to shut down its IT systems in order to prevent a ransomware attack, leaving staff unable to access electronic patient records and diagnostic test results, and leading to long waits in the emergency department; the hospital also canceled a variety of clinics and redirected some ambulances to other hospitals.[15]

As shown in Figure 2, data from ransomware "name and shame" blogs—websites where cybercriminals leak data from victims that do not meet ransom demands—show that almost two thirds of Canadian victims impacted by this type of ransomware from 1 January to 30 June 2021 were small- and medium-sized organizations. Since March 2020, nearly a quarter of Canadian small businesses—many of which were forced to increase their use of online platforms during the COVID-19 pandemic—experienced some type of malign cyber incidents.[16] **We assess this amount likely to be higher than reported.**

RANSOMWARE ENABLERS

Ransom demands are made using cryptocurrencies as a medium for payment. Cryptocurrencies are easily accessible and hard to trace. In the first six months of 2021, ransomware payments totaling $590M USD in cryptocurrency were made, more than the $416M USD reported for the whole of 2020.[17] While Bitcoin has long been the payment method of choice and still dominates ransomware demands, **we assess that it is very likely that cybercriminals will increasingly demand ransom payments in privacy coins, such as Monero, to further conceal their identity and obfuscate their activity from law enforcement.**

Privacy coins like Monero allow cybercriminals greater freedom from some of the tracking tools and mechanisms supported by the Bitcoin blockchain and other popular cryptocurrencies. In March 2021, a ransomware attack on Taiwan-based PC manufacturer Acer resulted in the highest known ransom demand ever: $50 USD million in Monero.[18] Sodinokibi has removed the option of paying in Bitcoin, demanding Monero only.[19] Ransomware operators also use cryptocurrencies to pay several other types of third-party providers they rely on to conduct attacks, including penetration testing services, exploit sellers, and bulletproof hosting providers.

Ransomware attackers move most of the funds received from their victims to mainstream cryptocurrency exchanges, high-risk exchanges (meaning those with loose to non-existent compliance standards), and mixers (services that let users mix their coins with other users) to launder and cash out their profits.

Moreover, the commercial sale of cyber tools, coupled with a global pool of talent, has resulted in more threat actors and more sophisticated threat activity. For example, Cobalt Strike, a commercial tool used to test network security, has been co-opted by cyber threat actors to facilitate sophisticated cybercriminal activities as well as very likely state-sponsored cyberespionage campaigns. Malicious use of Cobalt Strike increased 161% from 2019 to 2020 and remains a high-volume threat in 2021.[20] Ransomware operators and their affiliates continuously recruit programmers from freelance job websites, including experienced people who are familiar with tools used by legitimate penetration testers, such as Cobalt Strike.[21] Illegal online markets for cyber tools and services have also allowed cybercriminals to conduct more complex and sophisticated campaigns.

THE STATE-RANSOMWARE NEXUS

We stand by our assessment on the likely use of ransomware by state cyber threat actors to obfuscate the origins or intentions of their cyber operations. There are several examples of this activity. In 2019, individuals behind Chinese state-sponsored cyber threat activity were charged with conducting explicit financially motivated activity, which included the use of ransomware.[22] According to third-party industry reporting, between late July 2020 and early September 2020, Iran's Islamic Revolutionary Guard Corps (IRGC) operated a state-sponsored ransomware campaign through an Iranian contracting company, mimicking the tactics, techniques, and procedures (TTPs) of financially-motivated ransomware groups to avoid attribution and maintain plausible deniability.[23]

We assess that Russian intelligence services and law enforcement almost certainly maintain relationships with cybercriminals, either through association or recruitment, and allow them to operate with near impunity—as long as they focus their attacks against targets located outside Russia and the former Soviet Union. Subsequently, many of the most sophisticated and prolific ransomware variants are operated by Russia-based cybercriminals. In 2019, the US Department of Justice indicted Maksim Yakubets, leader of the Russia-based EvilCorp cybercriminal group, for providing direct assistance to the Russian Federation's malicious cyber efforts.[24] In April 2021, the US Department of the Treasury stated that the Russian Federal Security Service (FSB) cultivates and co-opts cybercriminals, including EvilCorp, enabling them to engage in disruptive ransomware attacks.[25]

Following the US-Russia summit in June 2021, the cybercriminal groups DarkSide and Sodinokibi—responsible for the string of significant ransomware attacks against Colonial Pipeline, JBS USA, and Kaseya—shut down their infrastructure and ceased their operations. However, by September 2021, both BlackMatter—a successor to several ransomware groups, including DarkSide—and Sodinokibi had returned and renewed their malicious activities–though Sodinokibi was subsequently forced offline after a multi-country operation led by the US compromised its servers in October 2021.[26] The BlackMatter ransomware group initially said that it would not allow its ransomware to be deployed against critical infrastructure, but has since done just that.[27]

OUTLOOK

Despite a temporary lull following international action, we assess that ransomware will continue to pose a threat to the national security and economic prosperity of Canada and its allies in 2022 as it remains a profitable activity for cybercriminals. Mitigating the increasing risks will require concerted national efforts to improve cyber security and adopt best practices to harden critical systems, as well as coordinated international actions to undermine criminal infrastructure and tactics.

For example, on 27 January 2021, a worldwide coalition of law enforcement agencies from the US, Canada, the UK, the Netherlands, Germany, France, Lithuania, and Ukraine, in coordination with private security researchers, disrupted Emotet—a botnet used by cybercriminals to deploy ransomware—and took over its command-and-control infrastructure. At least two of the cybercriminal group's members in Ukraine were also arrested.[28] On the same day, charges were laid by the US Department of Justice against a Canadian national in relation to NetWalker ransomware attacks.[29]

We assess that ransomware operators will likely become increasingly aggressive in their targeting, including against critical infrastructure. The collective response to the ransomware epidemic includes limiting the degree to which cybercriminals can rely upon safe haven jurisdictions, such as Russia, that protect them from consequences.[30] Many ransomware operators and their affiliates are based in countries with lax or non-existent laws and law enforcement against cybercrime and continue to target Canada, the US, and other allies. For example, following the June 2021 Sodinokibi ransomware attack against JBS USA, the world's largest meatpacker, a spokesperson for the Russia-based cybercriminal group said that it would not restrict itself from future attacks against the US.[31] One month later, on 2 July 2021, Sodinokibi compromised the Kaseya VSA supply chain, the largest ransomware attack in history.

Cybercriminals will almost certainly continue to rely on digital currencies to facilitate ransomware operations. International efforts to counter ransomware also come in the form of greater scrutiny and regulation of cryptocurrency exchanges that fail to report suspicious transactions, with a particular focus on mixing services that obfuscate criminal transactions with local traffic.[32] For example, in September 2021, the US Department of the Treasury imposed sanctions on the virtual cryptocurrency exchange Suex for its role in facilitating ransomware payments.[33] Hindering ransomware operations would be similar to how the enactment and enforcement of "know your customer" policies and the filing of "suspicious activity reports" by financial institutions have for many years been used to fight money laundering, drug trafficking, and terrorist financing.[34]

As Canada and the international community pursue efforts to disrupt the incentive structures that make it attractive and possible for cybercriminals to mount ransomware attacks and for their victims to pay up, the ransomware threat will very likely continue to grow and evolve in ways that have significant impacts on organizations and the critical infrastructure of Canada and its international partners.

While ransomware attacks will almost certainly continue to increase in scale, frequency and sophistication, the vast majority can be prevented by implementing basic cyber security measures. As Canada's national technical authority for cyber security, the Cyber Centre provides extensive resources that Canadians and Canadian organizations can use to mitigate the threat of ransomware. Consult our dedicated ransomware web page or contact the Cyber Centre for more information at contact@cyber.gc.ca.

[1] "Ransomware Volumes Hit Record Highs as 2021 Wears On," Threatpost, 3 August 2021. https://threatpost.com/ransomware-volumes-record-highs-2021/168327/.
[2] "The Cost of a Data Breach Report 2021," IBM, 28 July 2021. https://www.ibm.com/security/data-breach.
[3] "The Hiscox Cyber Readiness Report 2021," Hiscox, April 2021. https://www.hiscox.co.uk/cyberreadiness.
[4] "Another Ransomware Will Now Publish Victims' Data If Not Paid," Bleeping Computer, 12 December 2019. https://www.bleepingcomputer.com/news/security/another-ransomware-will-now-publish-victims-data-if-not-paid.
[5] "HSE Confirms Data of 520 Patients Published Online," The Irish Times, 28 May 2021. https://www.irishtimes.com/news/crime-and-law/hse-confirms-data-of-520-patients-published-online-1.4578136.
[6] Bill Blair, Minister of Public Safety, Five Country Ministerial Statement Regarding the Threat of Ransomware, 8 April 2021; "Enhancing Cybersecurity Readiness in an Era of Digital Disruption: A Discussion with Shelly Bruce, Chief, Communications Security Establishment," 18 May 2021; Scott Jones, former Head of the Canadian Centre for Cyber Security, Government Operations and Estimates Committee, 31 May 2021.
[7] "Combating Ransomware," Ransomware Task Force, 29 April 2021. https://securityandtechnology.org/wp-content/uploads/2021/04/IST-Ransomware-Task-Force-Report.pdf.
[8] "Ransomware Recovery Blog," Coveware, accessed on 9 November 2021. https://www.coveware.com/blog.
[9] "The State of Ransomware 2021," Sophos, 27 April 2021. https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf?cmp=120469.
[10] "CNA Financial Paid $40 Million in Ransom After March Cyberattack," Bloomberg, 20 May 2021. https://www.bloomberg.com/news/articles/2021-05-20/cna-financial-paid-40-million-in-ransom-after-march-cyberattack.
[11] "Updated Kaseya Ransomware Attack FAQ: What We Know Now," ZDNet, 23 July 2021. https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/.
[12] "Enhancing Cybersecurity Readiness in an Era of Digital Disruption: A Discussion with Shelly Bruce, Chief, Communications Security Establishment," 18 May 2021.
[13] "Ransomware Against the Machine: How Adversaries Are Learning to Disrupt Industrial Production by Targeting IT and OT." *FireEye*. 24 February 2020. https://www.fireeye.com/blog/threat-research/2020/02/ransomware-against-machine-learning-to-disrupt-industrial-production.html.
[14] Krauss, C., N. Chokshi, and D.E. Sanger. "Gas Pipeline Hack Leads to Panic Buying in the Southeast." *New York Times*. 11 May 2021. https://www.nytimes.com/2021/05/11/business/colonial-pipeline-shutdown-latest-news.html.
[15] "Cyberattack leads to computer system failure at Humber River Hospital, impacting patient care," Toronto Star, 15 June 2021. https://www.thestar.com/news/gta/2021/06/15/computer-system-failure-at-humber-river-hospital-impacts-patient-care.html.
[16] "Small Businesses were Forced Online Because of the Pandemic — Now a Quarter Say They've Experienced a Cyber Attack," Toronto Star, 4 February 2021. https://www.thestar.com/business/2021/02/04/small-businesses-pivoting-online-because-of-covid-19-are-vulnerable-to-cyber-attacks-cfib-report.html.
[17] "U.S. Treasury Puts Crypto Industry on Notice over Rising Ransomware Attacks," Reuters, 15 October 2021. https://www.reuters.com/business/finance/us-treasury-warns-crypto-industry-preventing-sanctions-violations-2021-10-15/.
[18] "Computer Giant Acer Hit by $50 Million Ransomware Attack," Bleeping Computer, 19 March 2021. https://www.bleepingcomputer.com/news/security/computer-giant-acer-hit-by-50-million-ransomware-attack/.
[19] "Monero Emerges as Crypto of Choice for Cybercriminals," Financial Times, 22 June 2021. https://www.ft.com/content/13fb66ed-b4e2-4f5f-926a-7d34dc40d8b6.
[20] "Cobalt Strike: Favorite Tool from APT to Crimeware," Proofpoint, 29 June 2021. https://www.proofpoint.com/us/blog/threat-insight/cobalt-strike-favorite-tool-apt-crimeware.
[21] "Amid an Embarrassment of Riches, Ransom Gangs Increasingly Outsource Their Work," Krebs on Security, 8 October 2020. https://krebsonsecurity.com/2020/10/amid-an-embarrassment-of-riches-ransom-gangs-increasingly-outsource-their-work/.
[22] "Justice Department Charges Five Chinese Members of APT41 over Cyberattacks on US Companies," TechCrunch, 16 September 2020. https://techcrunch.com/2020/09/16/justice-department-charges-apt41-chinese-hackers/.
[23] "A Second Iranian State-sponsored Ransomware Operation "Project Signal" Emerges," Flashpoint, 30 April 2021
[24] "Russian National Charged with Decade-Long Series of Hacking and Bank Fraud Offenses," US Department of Justice, 5 December 2019. https://www.justice.gov/opa/pr/russian-national-charged-decade-long-series-hacking-and-bank-fraud-offenses-resulting-tens.
[25] "Treasury Sanctions Russia with Sweeping New Sanctions Authority," US Department of the Treasury, 15 April 2021. https://home.treasury.gov/news/press-releases/jy0127.
[26] "Governments Turn Tables on Ransomware Gang REvil by Pushing it Offline," Reuters, 21 October 2021. https://www.reuters.com/technology/exclusive-governments-turn-tables-ransomware-gang-revil-by-pushing-it-offline-2021-10-21/.
[27] "BlackMatter Strikes Iowa Farmers Cooperative, Demands $5.9M Ransom," Threatpost, 21 September 2021. https://threatpost.com/blackmatter-strikes-iowa-farmers-cooperative-demands-5-9m-ransom/174846/.

[28] "Cops Disrupt Emotet, the Internet's 'Most Dangerous Malware'," Wired, 27 January 2021. https://www.wired.com/story/emotet-botnet-takedown/.
[29] "Canadian man charged in U.S. with NetWalker ransomware attacks," Toronto Star, 27 January 2021. https://www.thestar.com/news/canada/2021/01/27/canadian-man-charged-in-us-with-netwalker-ransomware-attacks.html.
[30] "How the Kremlin provides a safe harbor for ransomware," Associated Press, 6 April 2021. https://apnews.com/article/business-technology-general-news-government-and-politics-c9dab7eb3841be45dff2d93ed3102999.
[31] "REvil Ransomware Gang Spill Details on US Attacks," Threatpost, 4 June 2021. https://threatpost.com/revil-spill-details-us-attacks/166669/.
[32] "The Ransomware Problem Is a Bitcoin Problem," Lawfare, 27 May 2021. https://www.lawfareblog.com/ransomware-problem-bitcoin-problem.
[33] "Treasury Takes Robust Actions to Counter Ransomware," US Department of the Treasury, 21 September 2021. https://home.treasury.gov/news/press-releases/jy0364.
[34] "How A New Team of Feds Hacked the Hackers and Got Colonial Pipeline's Ransom Back," NPR, 8 June 2021. https://www.npr.org/2021/06/08/1004223000/how-a-new-team-of-feds-hacked-the-hackers-and-got-colonial-pipelines-bitcoin-bac.

CAT. D96-78/2021E-PDF
ISBN 978-0-660-41160-6