Communications Security Establishment
Centre de la sécurité des télécommunications

CANADIAN CENTRE FOR CYBER SECURITY

The Cyber Threat to Canada's Oil and Gas Sector

Canada

About this document

Audience

This report is part of a series of cyber threat assessments focused on advice about the cyber threats to Canada's critical infrastructure. It is intended for leaders in the oil and gas sector, cyber security professionals with an oil and gas asset to protect, and the general reader with an interest in the cyber security of critical infrastructure. For guidance on technical mitigation of these threats, see the Useful Resources section or contact the Canadian Centre for Cyber Security (the Cyber Centre).

Sources may use TLP:CLEAR when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release. Subject to standard copyright rules, TLP:CLEAR information may be shared without restriction. For more information, see Traffic Light Protocol.

Contact

For follow-up questions or issues please contact Canadian Centre for Cyber Security at contact@cyber.gc.ca.

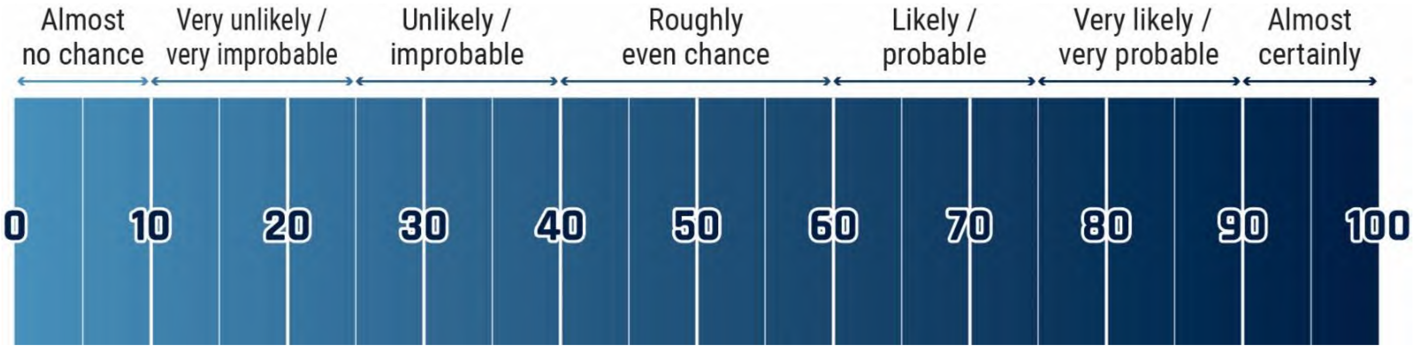
Assessment base and methodology

The key judgements in this assessment rely on reporting from multiple sources, both classified and unclassified. The judgements are based on the knowledge and expertise in cyber security of 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's foreign intelligence mandate provides us with valuable insight into adversary behaviour 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 assessments and analysis are based on information available as of March 31, 2023.

Estimative language guide



The cyber threat to Canada's oil and gas sector

Key judgements

- We assess that financially-motivated cybercrime, particularly business email compromise and ransomware, is almost certainly the main cyber threat facing the Canadian oil and gas sector. Ransomware is almost certainly the primary cyber threat to the reliable supply of oil and gas to Canadians.

- We assess that the oil and gas sector in Canada will very likely continue to be targeted by state-sponsored cyber espionage for commercial or economic reasons. At risk are proprietary trade secrets, research, and business and production plans.

- We assess that since the oil and gas sector is Critical Infrastructure (CI), it is very likely a strategic target for state-sponsored cyber activity to project state power, especially in times of geopolitical tension. We assess that the primary target for state-sponsored actors is very likely the operational technology (OT) networks that monitor and control the sectors' large industrial assets. State-sponsored actors are almost certainly striving to improve their capability to sabotage the OT in critical infrastructure. We assess that it is very unlikely that a state-sponsored cyber actor would intentionally disrupt or damage the oil and gas infrastructure in Canada outside of hostilities.

- We assess that the most likely targets for cyber threat actors intending to disrupt the supply of oil and gas in Canada are bottlenecks in the oil transmission and processing stages. Potential targets include the business and OT networks of large-diameter pipelines, transfer terminals, and major refining facilities.

- Russia has repeatedly demonstrated intent to project power by deploying destructive cyber attacks against strategic CI targets of their adversaries as geopolitical crises escalate. The Cyber Centre is aware of efforts by Russian state-sponsored threat actors to compromise and establish persistence (i.e. pre-positioning) on the networks of Canadian and US CI providers, including organizations in the oil and gas sector. We assess that Russian espionage, with the goal of pre-positioning on OT networks, will very likely continue.

- We assess that state-sponsored cyber threat actors are almost certainly continually improving their capability to conduct destructive or debilitating cyber activity against CI. State-sponsored cyber threat actors also sometimes work with non-state cyber groups as a force multiplier to enhance their capabilities, and to avoid direct attribution. The Cyber Centre is aware that Russia's long-standing practice has been to coordinate with non-state actors to conduct cyber threat activity against Ukrainian and allies' CI.

- We assess that there is an even chance that Canada's oil and gas infrastructure would be affected by cyber activity against US assets due to cross-border integration.

The cyber threat to Canada's oil and gas sector

Introduction

The oil and gas sector is a critical contributor to both Canada's economy, and the security and well-being of Canadians. As a result, the cyber security of the oil and gas sector is important to Canada's national security. The oil and gas sector employs about 600,000 Canadians and adds $120 billion dollars to Canada's economy, or about 5% of the gross domestic product (GDP).[1] In Canada, oil and gas is used for energy to heat buildings, move people and goods, seed fields and harvest crops, generate electricity, and also serves as raw materials for many other manufactured products.

It is difficult to overstate the importance of the oil and gas sector to national security because much of our critical infrastructure depends on oil and gas products to operate. At the same time, critical infrastructure, and especially the energy sector, is increasingly at risk from cyber threat activity.[2] In the United States, for example, Colonial Pipeline garnered international attention in May 2021 when it was forced to shut down the operation of one of the largest gasoline, diesel, and jet fuel pipelines in the US, due to a ransomware incident. Although the pipeline was restarted a few days later, the disruption in the fuel supply resulted in shortages that caused the re-routing of flights, panic buying, and short-term price spikes. It was estimated that, at the time that the pipeline was restarted, the Eastern US was only a few days away from experiencing food and other shortages from the disruption of fuel to other sectors such as truck transportation.[3]

Oil and gas sector primer

The organizations that participate directly in the oil and gas sector can be divided into three broad categories:

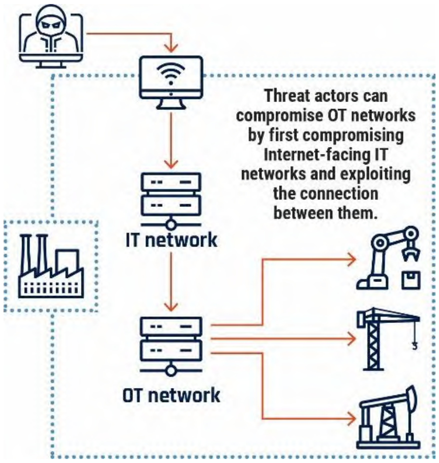
1. Upstream: the organizations involved in exploration, extraction, and production
2. Midstream: pipelines, transportation, and storage
3. Downstream: refining, distribution, and sales

The upstream oil and gas sector organizations are involved in the discovery and extraction of crude oil and natural gas from natural deposits. Activities start with environmental and geological research and planning, leading to extraction including drilling and operating oil and gas wells, and mining oil sands.

Midstream activities include the storage, processing, and transportation of oil and gas products. Oil and gas can be transported by pipeline, train, truck, and marine tankers. Pipelines are the primary midstream delivery mechanism for moving oil and gas products from producers to consumers in North America. Canada is roughly 7,500 km, from east to west. In that space, there are about 850,000 km of gathering, feeder, transmission, and distribution pipelines for oil and gas products. This includes just under 120,000 km of large-diameter transmission pipelines used to move larger volumes of oil and gas long distances, often across provincial and international borders.[4] Large storage facilities are connected to the pipeline network to counter changes in supply and demand so that pipelines are used efficiently. Natural gas is usually stored underground in large reservoirs. Above ground tanks are used for crude and refined oil, finished oil products, and natural gas.

The downstream part of the oil and gas sector is responsible for the refining of crude oil and raw natural gas into final products, as well as the distribution, and sales of oil and gas products to clients. This includes refineries and chemical plants, and distribution and retail companies.

The cyber threat surface



Threat actors can compromise OT networks by first compromising Internet-facing IT networks and exploiting the connection between them.

Oil and gas organizations tend to have a broad attack surface of connected digital systems. These systems could include business information technology (IT) systems, industrial operational technology (OT) assets, and connected web of suppliers of digital products and services. As we noted in our National Cyber Threat Assessment 2020, the more Internet-connected assets an organization has, the larger the threat surface, which could increase the cyber threat it faces.[5] In 2019, Statistics Canada survey data shows that about 25% of all Canadian organizations classified as oil and gas reported a cyber incident[6] the highest of any critical infrastructure sector.

Like virtually all heavy industry worldwide, the oil and gas sector has embraced digital transformation of their OT in production, transportation, and distribution of their products. The digital transformation of energy sector OT has many management, performance, and productivity benefits. For example, it allows organizations to centrally monitor and manage OT devices that might be spread over a wide geographic area. The Cyber Centre assesses that the digital transformation of OT assets is almost certainly expanding the attack surface of vulnerabilities for cyber actors and exposing oil and gas sector OT assets to cyber threats.[7]

Cyber threats originating in the digital supply chain

We assess that medium- to high-sophistication cyber threat actors are likely to consider targeting organizations indirectly, by first targeting the supply chain.[8] Cyber threat actors target the supply chain for two general purposes: to obtain commercially-valuable intellectual property and information from suppliers about the target organization's networks and OT; and, as an indirect route to access a target organization's networks.[9] Large industrial asset operators, including those in oil and gas, depend on a diverse supply chain of products and services from laboratories, manufacturers, vendors, integrators, and contractors, as well as Internet, cloud, and managed service providers for daily operation, maintenance, modernization, and development of new capacity. Oil and gas OT asset operators' dependence on the supply chain is a critical vulnerability that gives cyber actors inside information on, and opportunities for access to otherwise protected IT and OT systems. We assess that medium- and high-sophistication actors will almost certainly continue to target the supply chain for these purposes for the next 12 months and beyond.

The threat from the proliferation of cyber tools

The Cyber Centre notes that pre-built cyber tools and training in their use are becoming readily available via the Internet and we judge that there is an even chance that low sophistication actors with the intent to disrupt the oil and gas sector could adopt these tools to mount a future successful sabotage attack.

For example, there are OT-specific exploit modules in free cyber tools as well, such as the open source Metasploit framework developed and released by researchers and security professionals for testing OT network defences. These tools are widely available to actors of all sophistication levels and include documentation and tutorials in their use.[10] The Cyber Centre is also aware of high-impact crimeware such as Trickbot, Qakbot, Dridex, etc., using the leaked commercial cyber tool Cobalt Strike to target large organizations and critical infrastructure in Canada. Both Metasploit and Cobalt Strike are in wide use by states and criminal groups to facilitate cyber espionage and ransomware activity.[11] In addition, a large illegal marketplace for cyber tools and services is greatly reducing the start-up time for cybercriminals and potentially other actors by enabling them to conduct more complex and sophisticated campaigns. Many online marketplaces allow vendors to sell specialized cyber tools and services that users can purchase and use to commit cybercrime, including espionage, distributed denial of service (DDoS) attacks, and ransomware attacks, any of which could be used by actors intending to sabotage OT systems.

We assess that the wide availability of free, stolen, commercial and criminal cyber capabilities and services is likely lowering the threshold of sophistication necessary to target and sabotage OT. In the National Cyber Threat Assessment 2020, the Cyber Centre assessed that the development of commercial markets for cyber tools and talent has reduced the time it takes for cyber actors to build cyber capabilities. Some vendors are developing OT-specific capabilities for sale to clients. As more cyber actors gain access to commercial cyber tools, actors that are interested in sabotaging OT, but previously lacked the capability, can now more readily attempt this type of cyber threat activity. The proliferation of commercial tools also makes it more difficult to identify, attribute, and defend against this cyber threat activity. We assess that **although the threat to oil and gas from other actors is likely currently low, the inconsistent level of cyber security in connected OT devices, the global discoverability of devices on the Internet through OT-specific search engines and the availability of free cyber tools will, in combination, likely increase the threat from low sophistication cyber actors in the near future.**

The threat from cybercrime

We assess that cybercriminals motivated by financial gain, particularly criminals attempting business email compromise (BEC) and ransomware, are almost certainly the top cyber threats facing the oil and gas sector. Although BEC is very likely more common and more costly than ransomware to victims**, we assess that ransomware is almost certainly the main threat to the supply of oil and gas to customers.** The underground cybercriminal ecosystem is continuously evolving to maximize profits and increase the payouts extracted from targets.[12] For example, the adaptation of ransomware to a service model (ransomware-as-a-service, or RaaS) and the widespread adoption of stealing and leaking of sensitive data to increase the pressure to pay are two of the main drivers of the recent increase in successful incidents.[13]

The oil and gas sector, like other parts of the energy sector, reportedly attracts more than its share of attention from financially-motivated cyber threat actors due to the high value of the industry's assets and the degree of customer dependence on the industry's products.[14] Other assets of value in the oil and gas sector targeted by cybercriminals include intellectual property and business plans, and stores of client information.

Since oil and gas organizations are part of Canadian critical infrastructure (CI), they are attractive targets for extortion because of the importance of these products and services to Canadians. Cybercriminal activity has the potential to disrupt operations and critical delivery of products by limiting a company's access to essential business data in the IT network, or by preventing safe control of industrial processes in the OT network. The disruption or sabotage of OT systems in Canadian CI poses a costly threat to owner-operators of large OT assets and could conceivably jeopardize national security, public and environmental safety, and the economy.

In early May 2021, for example, Colonial Pipeline suffered an incident attributed to DarkSide, a Russia-based ransomware group. Although the activity was reported to be restricted to the IT systems, the company chose to shut down its operations for business reasons, leading to panic-buying and shortages, and elevating the event to a national security issue. Later, it was reported that the Russia's Federal Security Service (FSB) investigated and arrested members of the group allegedly responsible for the Colonial incident at the request of US officials.[15]

The high profile of the Colonial incident and the resulting attention from law enforcement likely motivated some groups to make public statements about altering their targeting patterns away from some CI, and some criminal forums to ban ransomware completely.[16] However, similar statements about the health sector have not resulted in decreased overall targeting.[17] We assess that these statements and activities are likely largely theatre and do not lower the threat to oil and gas organizations substantially over the long term.

Cybercriminals are opportunistic and will not hesitate to exacerbate a crisis for profit. For example, in late January 2022, incidents at two subsidiaries of the German oil transportation company Marquard & Bahls and an unrelated ransomware incident at Amsterdam-Rotterdam-Antwerp (ARA) caused significant disruption in the delivery of oil products in parts of continental Europe, potentially worsening the existing energy crisis caused by Russia's imminent invasion of Ukraine.[18] **We assess that cybercriminals will almost certainly continue to target high-value organizations in the oil and gas sector in Canada and globally.**

The state-sponsored cyber threat to oil and gas

State-sponsored cyber activity against the oil and gas sector has become a regular feature of global cyber threat activity, especially in times of rising geopolitical tensions.[19] Politically motivated state-sponsored cyber threat actors, including Russia, China, and Iran have targeted the global energy sector for both espionage and disruption/destruction. State-sponsored actors typically conduct espionage on oil and gas targets for foreign intelligence (to obtain oil and gas sector data of economic or foreign relations intelligence value) or for commercial reasons (to obtain business plans or valuable intellectual property to deploy for national competitive advantage). We assess that state-sponsored actors are almost certainly the most sophisticated cyber actors and that some very likely have the capability to launch coordinated effects, and target more than one CI component at a time. In addition, state-sponsored actors use a variety of tactics to work covertly and are often difficult to identify and attribute with confidence.

Commercial espionage

We assess that the oil and gas sector in Canada will very likely continue to be targeted by states for commercial or economic reasons. This could include organizations at any level of the oil and gas value chain. Oil and natural gas digital assets of value to adversarial states include an organization's proprietary trade secrets, research, client data, and business and production plans. Examples of these assets might include oilfield development plans, or research and development on equipment or techniques, which, if stolen, could result in competitive disadvantage from lost investment, lost revenue, and damaged reputations. For example, in 2020 the Norwegian counterintelligence service reported that Russia, China and other countries were using cyber espionage to discover petroleum industry trade secrets and production plans.[20]

Pre-positioning and capability development

The Cyber Centre assesses that critical infrastructure, and especially the network-connected OT in critical infrastructure, is a strategic target for disruption or destruction by state-sponsored cyber actors in times of rising hostilities between states.[21] Energy, water, government, telecommunications, and finance sectors have been targeted over geopolitical disputes. Offensive cyber activity against oil and gas OT to deny essential products to a target country could be used to send intimidating messages about power and capability, delegitimize target governments, demoralize leaders and the public, degrade defences, and threaten a population's health and safety. **We assess that it is very unlikely that a state-sponsored cyber actor would intentionally disrupt or damage the oil and gas infrastructure in Canada outside of hostilities.**

Some large OT asset owner-operators, such as the utilities, pipelines and refineries in the oil and gas sector, are not likely targets for commercial espionage because most of the commercially valuable IP in use and in development resides in the supply chain. We judge that the intent of most state-sponsored cyber activity against oil and gas sector OT asset owners is likely to collect information and pre-position cyber tools as a contingency for possible future sabotage, or as a form of intimidation from a demonstration of state cyber power. These early stages of potential future cyber sabotage tend to resemble commercial espionage.[22] **We assess that it is very likely that state actors are using the information gathered from cyber reconnaissance and espionage to develop access and additional capabilities that would allow them to sabotage the OT used in Canada's CI sectors, including oil and gas.**

The Cyber Centre assesses that **state-sponsored cyber threat actors are almost certainly continually improving their capability to conduct destructive or debilitating cyber activity against CI.** They do this by locating and prioritizing systems of interest, identifying vulnerabilities, developing access to and pre-positioning in those systems, conducting espionage on the OT in use, and developing techniques and tools to disrupt or destroy the OT.[23] In early 2022, Pipedream (aka Incontroller) malware was uncovered, with modules for exploiting OT supervisory workstations and affecting industrial OT automation and safety controllers typically found in liquefied natural gas and electric power facilities.[24] The heightened level of technical sophistication level of PIPEDREAM over earlier malware such as TRITON points to both a state-sponsored author, and the effort that these actors are willing to commit to the development of OT-specific offensive cyber capabilities.[25]

We assess that the state-sponsored actors intending to disrupt the supply of oil and gas in Canada are likely to target supply bottlenecks in the product transmission and processing stages to maximize the effect. Potential targets for this activity could include large-diameter pipelines, marine terminals, and major refining facilities.

Notable state-sponsored cyber activity against the oil and gas sector

- In late 2019 and early 2020, Iranian state-sponsored actors deployed Shamoon variant Zerocleare[26] and Dustman[27] wiper malware onto the networks of unidentified Saudi Arabian energy sector targets and Bapco, Bahrain's national oil company, causing an unreported amount of business disruption.[28]
- In 2018 a variant of Iranian Shamoon malware destroyed about 10 percent of the Italian oil and gas company Saipem's network. Saipem is major Saudi Aramco contractor.[29]

- In 2017, Russian cyber threat actors tested a capability called Triton (aka Trisis) to modify the performance of a Safety Instrumented System (SIS) at a Middle Eastern oil and gas facility. An SIS is a specialized OT device designed to independently detect out-of-range conditions in an industrial process and if needed, initiate a safe shutdown of the equipment. The actors gained remote access for the facility and reprogrammed the SIS controllers, inadvertently causing them to enter a failed state, resulting in an automatic shutdown of the industrial process and subsequent investigation.[30] Later, in 2018 and 2019, the same actors probed the networks of energy sector utilities in the US.[31]
- From 2011 to 2018, Russian state-sponsored cyber actors conducted an extensive cyber espionage campaign against US and European energy sector companies, employing Havex malware to search for OT components and extract OT-related information.[32]
- In 2012, state-sponsored Iranian cyber actors deploy Shamoon wiper malware to IT networks of Saudi Aramco and RasGas in Saudi Arabia and Qatar, deleting data on roughly 30,000 computers and forcing the shutdown of numerous internal networks.[33]
- From 2011 to 2013 Chinese state-sponsored actors conducted a spear phishing and intrusion campaign against US oil and natural gas pipeline companies.[34]

Current geopolitical context: The Russian invasion of Ukraine

In April 2022, the Cyber Centre, along with our partner cyber security agencies in Australia, New Zealand, the UK and the US warned critical infrastructure providers of the potential for activity by both Russian state-sponsored and Russian-aligned, non-state criminal-hacktivist groups in support of the Russian invasion of Ukraine.[35] In July 2023, the Cyber Centre expanded on the role of these actors both within and beyond Ukraine in its “Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine”.[36]

Russia has repeatedly deployed destructive cyber attacks against strategic critical infrastructure (CI) targets to project power when geopolitical crises escalate to armed conflict. In 2022, in support of the invasion of Ukraine, Russia conducted a large-scale cyber campaign targeting Ukrainian CI including government, energy, telecommunications, and financial sectors.[37] This campaign used denial of service and various forms of destructive malware to cause widespread disruption, often coordinated with kinetic attacks. For example, on February 24, Russian state-sponsored hackers conducted destructive cyber threat activity targeting Viasat KA-SAT satellite Internet service in Ukraine as Russian forces invaded Ukraine, rendering CI for Internet and communications inoperable and disrupting Internet access to Viasat customers across Europe.[38]

Threat to Canada: State-sponsored actors

We judge that Russian state-sponsored cyber actors are almost certainly conducting reconnaissance activity against Canadian CI, and that Russian cyber activity with the goal of pre-positioning on industrial OT networks will very likely continue. **We assess that it is very unlikely that Russian state-sponsored actors would choose to conduct a destructive attack against Canadian or allied-state oil and gas infrastructure outside of perceived imminent armed conflict between Canada and Russia.**

Threat to Canada: State-aligned actors

Cyber activity supporting Russia’s invasion of Ukraine by Russian-aligned groups such as Killnet, Xaknet and others has very likely increased substantially over the last 12 months.[39] These groups typically either gain access to networks to deploy ransomware and encrypt data, potentially causing significant disruption to operations, or conduct DDoS attacks (often with extortion) or defacement activity against websites.[40] Targets within a sector are likely chosen opportunistically, based on searches for exposed services with known vulnerabilities, rather than strategically for maximum effect. These attacks often respond to news that the targeted state is providing support to Ukraine.[41]

The Cyber Center is aware of efforts by Russia-aligned threat actors to compromise and establish persistence on the networks of Canadian and US CI providers, including organizations in the oil and gas sector. We assess that the intent of this activity is very likely to disrupt critical services for psychological impact, ultimately to weaken Canadian support for Ukraine. We assess that this activity will almost certainly continue for the duration of the war, and will likely increase as Russia’s invasion efforts falter, or new support for Ukraine is announced. Although Russia-aligned non-state actors almost certainly have a lower overall sophistication and technical capability than Russian state-sponsored actors, we assess there is an even chance of a disruptive incident in the oil and gas sector in Canada caused by Russia-aligned actors, due to their higher tolerance for risk, the increase in their numbers and activity, as well as the number of vulnerable targets in the sector overall.

We assess that both Russian state-sponsored and Russia-aligned cyber threat actors very likely view Ukraine, the US, and leading European NATO members as higher priority targets than Canada. However, **if the US is targeted, we assess that there is an even chance that Canada would be affected**, due to the interconnectedness of US and Canadian oil and gas infrastructure.

Notable Russian cyber activity

- The first state-sponsored cyber activity to sabotage critical infrastructure occurred in 2015 and 2016 against the electricity grid in Ukraine, conducted by Russia's military intelligence agency, the Main Intelligence Directorate of the General Staff (GRU), also known as the Sandworm Team. In 2015, Russia was able to de-energize seven substations from three Ukrainian regional distribution companies for three hours, causing a power outage that affected 225,000 customers. A year later, a cyber incident at Ukraine's national power company, Ukrenergo, caused a one-hour outage in northern Kyiv. These incidents, conducted in the context of the Russian invasion of Ukraine, were a turning point in the history of cyber activity against the energy sector, demonstrating the impact of a cyber attack against critical infrastructure, and its use during international hostilities.[42]
- In June 2017, the NotPetya malware infected tens of thousands of devices, including those on critical infrastructure networks in Ukraine and around the world,[43] likely in an attempt by Russia to disrupt Ukraine's financial systems.
- In 2018, the GRU disabled over 15,000 Georgian government websites and media outlets as part of efforts to destabilize the country.[44]

Other actors

We assess that low-sophistication actors such as terrorists, hacktivists, thrill seekers, and disgruntled individuals, motivated to attract attention by embarrassing or harming the sector through public incidents are currently more likely to engage in noisy, nuisance-level cyber activity, such as website defacement, than to attempt direct OT disruption. Since Russia's full-scale invasion of Ukraine began in February 2022, we assess that the operational tempo and engagement of pro-Russian non-state cyber groups has likely increased.[45] The Cyber Centre is aware that Russia's long-standing practice has been to coordinate with non-state groups, such as cybercriminals and hacktivists, to conduct cyber threat activity against Ukrainian and allies' CI. For example, pro-Russian hacktivist group Killnet has conducted DDoS attacks against critical infrastructure operators' websites, including those of energy sector providers.[46]

Outlook

The cyber security of Canada's critical infrastructure is also national security. The oil and gas sector in Canada has a major role in the economy, both as a contributor to the GDP, and as an energy provider to other parts of the Canadian economy, critical infrastructure, and Canadians. The importance and high profile of the oil and gas sector, along with its expanding threat surface from digital transformation makes it a target for cyber actors intent on maximum disruption.

The Cyber Centre encourages all critical infrastructure network owners, including those in the oil and gas sector, to take appropriate measures to protect your systems against the cyber threats detailed in this assessment, in particular those related to geopolitical events surrounding the Russian invasion of Ukraine.[47] The Cyber Centre joins our partners in the US[48] and the UK[49] in recommending proactive network monitoring and mitigations. The US Cybersecurity & Infrastructure Security Agency's (CISA) advisory "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure" helpfully highlights vulnerabilities known to have been exploited by Russian cyber threat actors, their tactics, techniques and procedures, and potential defence actions.

Useful resources

Threat detection and mitigation

- An introduction to the cyber threat environment
- Cyber security guidance for heightened threat levels
- Ransomware resources
- Baseline cyber security controls for small and medium organizations
- Top 10 IT security actions for Internet connected systems
- IoT security for small and medium organizations
- Cyber Centre’s advice on mobile security
- Cyber security considerations for contracting with managed service providers
- Top 10 IT security action items: No.2 patch operating systems and applications
- Joint report on publicly available hacking tools
- Malicious cyber activity targeting managed service providers

Threat assessment

- Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine
- Cyber threat bulletin: Cyber threat to operational technology
- The cyber threat from supply chains
- National Cyber Threat Assessment 2023-2024
- Cyber threat bulletin: The cyber threat to Canada's electricity sector
- Cyber threat bulletin: The ransomware threat in 2021

Services

- Security review program fact sheet

Endnotes

[1] Natural Resources Canada. “Energy Fact Book 2021–2022.” 23 December 2021.

[2] Canadian Centre for Cyber Security. “National Cyber Threat Assessment 2023-24.” 28 October 2022.

[3] Halpern, S. “The Colonial Pipeline Ransomware Attack and the Perils of Privately Owned Infrastructure.” The New Yorker. 19 May, 2021.

[4] Natural Resources Canada. “Pipelines Across Canada.” 14 September 2020.

[5] The Canadian Centre for Cyber Security. “National Cyber Threat Assessment 2020.” 16 November 2020.

[6] Statistics Canada. Table 22-10-0076-01. Types of cyber security incidents that impact enterprises by industry and size of enterprise.

[7] Canadian Centre for Cyber Security. “Cyber Threat Bulletin: The Cyber Threat to Operational Technology.” 16 December 2021.

[8] Canadian Centre for Cyber Security. “The cyber threat from supply chains.” 08 February 2023.

[9] Canadian Centre for Cyber Security. “Cyber Threat Bulletin: The Cyber Threat to Operational Technology.” 16 December 2021.

[10] E.g.: YouTube, https://github.com/miguelob/ICS-Hacking, https://scadahacker.com/resources/msf-scada.html, etc.

[11] Sheridan, K. “Cobalt Strike & Metasploit Tools Were Attacker Favorites in 2020.” *DarkReading*. 7 January 2021.

[12] The Canadian Centre for Cyber Security. “Cyber threat bulletin: The ransomware threat in 2021.” 16 December 2021..

[13] Microsoft 365 Defender Threat Intelligence Team. “Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself.” Microsoft Threat Intelligence Center (MSTIC). 9 May 2022..

[14] Trend Micro Inc. “Cyber-Attacks on Industrial Assets Cost Firms Millions.” Trend Micro News. June 02, 2022.

[15] Tom Balmforth and Maria Tsvetkova. “Russia takes down REvil hacking group at U.S. request – FSB.” Reuters. 14 January, 2022.

[16] ReliaQuest Blog. “Colonial Pipeline Attack Update: Cybercriminal forum XSS, Exploit and RaidForums ban all things ransomware.” ReliaQuest. 14 May 2021.

[17] Statista Research Department. “Malware: most-targeted industries 2020-2021.” Statista. 7 July 2022.

[18] Janofsky, A. “String of cyberattacks on European oil and chemical sectors likely not coordinated, officials say.” Recorded Future. 3 February, 2022. and Klimburg, A., F. Beato, and M. Kolaczkowski. “Why the energy sector's latest cyberattack in Europe matters.” World Economic Forum. 4 February 2022..

[19] The Canadian Centre for Cyber Security. “National Cyber Threat Assessment 2020.” 16 November 2020..

[20] Reuters. “Russian, Chinese intelligence targeting Norwegian oil secrets: report.” December 3, 2020.

[21] Canadian Centre for Cyber Security. “Cyber Threat Bulletin: The Cyber Threat to Operational Technology.” 16 December 2021..

[22] Assante, M.J. and R.M. Lee. “The Industrial Control System Cyber Kill Chain.” SANS Institute. 2015.

[23] Canadian Centre for Cyber Security. “Cyber Threat Bulletin: The Cyber Threat to Canada's Electricity Sector.” 30 November 2020.

[24] Cybersecurity and Infrastructure Security Agency. Alert AA22-103A. “APT Cyber Tools Targeting ICS/SCADA Devices.” 13 April 2022.

[25] Dragos, Inc. “CHERNOVITE’s PIPEDREAM Malware Targeting Industrial Control Systems (ICS).” 13 April 2022, and Brubaker, N., K. Lunden, K. Proska, M. Umair, D. Kapellmann Zafra, C. Hildebrandt, and R. Caldwell. “INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems.” Mandiant. 13 April 2022.

[26] Kessem, L. and the IBM Security X-Force Team. “New Destructive Wiper “ZeroCleare” Targets Energy Sector in the Middle East.” IBM Security Intelligence Blog. 4 December 2019.

[27] Jenna McLaughlin. “Saudis warn of new destructive cyberattack that experts tie to Iran.” Yahoo News. 7 January 2020.

[28] Cimpanu, C., “New Iranian data wiper malware hits Bapco, Bahrain's national oil company.” ZDNet. 8 January 2020.

[29] Cimpanu, C., “Shamoon malware destroys data at Italian oil and gas company.” ZDNet. 13 December 2018.

[30] Johnson, B., D. Cuban, M. Krotofil., D. Scali, N. Brubaker, and C. Glyer. “Threat actors Deploy New ICS Attack Framework “TRITON” and Cause Operational Disruption to Critical Infrastructure.” *FireEye*. 14 December 2017.

[31] Dragos Blog. "Threat Proliferation in ICS Cybersecurity: XENOTIME Now Targeting Electric Sector, in Addition to Oil and Gas." Dragos, Inc. 14 June 2019.

[32] Nelson, N. "The Impact of Dragonfly Malware on Industrial Control Systems." SANS Institute. 18 January, 2016., and Cybersecurity and Infrastructure Security Agency. Alert AA22-083A. "Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector." 24 March 2022.

[33] Finkle, J. "Insiders suspected in Saudi cyber attack." *Reuters*. 7 September 2012.

[34] Cybersecurity and Infrastructure Security Agency. Alert AA21-201A. "Chinese Gas Pipeline Intrusion Campaign, 2011 to 2012." 21 July 2021.

[35] Cybersecurity and Infrastructure Security Agency. Alert AA22-110A. "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure." Revised 09 May 2022.

[36] Canadian Centre for Cyber Security. "Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine." 14 July 2022.

[37] Canadian Centre for Cyber Security. "Cyber threat bulletin: Cyber threat activity related to the Russian invasion of Ukraine." 14 July 2022.

[38] Global Affairs Canada. "Statement on Russia's malicious cyber activity affecting Europe and Ukraine." 10 May 2022..

[39] Zdrok, N. "Cyber War: Hackers' Transformation from Cyber Criminals to Hacktivists." Binary Defense blog. 30 November 2022.

[40] Cybersecurity and Infrastructure Security Agency. Alert Code AA22-110A. "Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure." Revised 09 May 2022.

[41] M. Burgess. "Russian "hacktivists" are causing trouble far beyond Ukraine." Ars Technica. 12 July, 2022.

[42] Canadian Centre for Cyber Security. "Cyber Threat Bulletin: The Cyber Threat to Canada's Electricity Sector." 30 November 2020.

[43] Canadian Centre for Cyber Security. "National Cyber Threat Assessment 2018." 6 December 2018.

[44] Global Affairs Canada. "Canada condemns Russia's malicious cyber-activity targeting Georgia." 20 February 2020.

[45] Zdrok, N. "Cyber War: Hackers' Transformation from Cyber Criminals to Hacktivists." Binary Defense blog. 30 November 2022.

[46] Cybersecurity and Infrastructure Security Agency. Alert AA22-110A. "Cybersecurity Advisory: Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure." 9 May 2022., and Forescout Vedere Labs. "Killnet: Analysis of Attacks from a Prominent Pro-Russian Hacktivist Group." 2 June 2022.

[47] Canadian Centre for Cyber Security. "Cyber threat bulletin: Cyber Centre reminds Canadian critical infrastructure operators to raise awareness and take mitigations against known Russian-backed cyber threat activity." 13 February 2022.

[48] Cybersecurity & Infrastructure Security Agency. "CISA Urges Organizations to Implement Immediate Cybersecurity Measures to Protect Against Potential Threats." 18 January 2022.

[49] National Cyber Security Centre. "NCSC joins US partners to promote understanding and mitigation of Russian state-sponsored cyber threats." 12 January 2022.

CAT. D96-101/2023E-PDF
ISBN 978-0-660-48765-6

Communications Security Establishment
Centre de la sécurité des télécommunications

Canada