Threat Perspective

Nordic Region

info@dragos.com | www.dragos.com

Table of Contents

Executive Summary

- Dragos assesses with high confidence the renewable energy sector of the Nordic Region, encompassing Denmark, Finland, Iceland, Norway and Sweden, the autonomous territories of the Faroe Islands and Greenland, and the autonomous region of Åland, matches the targeting profiles of Russian cyber operations (wind, solar, nuclear, hydroelectric, and biofuels) – based on the 2023 threat assessment by the U.S. Office of the Director of National Intelligence (ODNI), along with the leaked NTC Vulkan Files that detailed the Russian programs for offensive cyber operations on critical infrastructure.
- As of June 2023, Distributed Denial of Service (DDoS) attacks performed by hacktivist groups are ongoing in the Nordic Region with an emphasis on Sweden[1].
- Wiper malware has been deployed against Ukraine, which had cascading impacts on European renewable energy asset owners[2]. Nordic countries were victims of the spread of wiper malware (NotPetya infected systems in Denmark).
- Sweden is hosting approximately 57 percent of the internet-connected ICS/OT assets in the Nordic Region.
- Rapid weaponization of exploits on Virtual Private Networks (VPN) and remote services are a prolific attack vector with a proportionally larger risk to Cisco SSL VPNs. Fifty-four percent of Dragos sampled VPN appliances belonging to renewable energy asset owners in the Nordic Region are Cisco SSL VPNs.
    - Worldwide exploitation of the following Known Exploited Vulnerabilities (KEV)
        - Fortinet – FortiOS and FortiProxy SSL-VPN (CVE-2023-27997)
        - MOVEit Transfer – Progress MOVEit Transfer SQL Injection Vulnerability (CVE-2023-34362)

Dragos engagements on hydroelectric dams, wind farms, and solar farms identified many critical findings that elevated levels of risks for those customers including vendor managed control systems, lack of ICS/OT network segmentation, insecure file transfer protocols, internet-connected OT systems, limited security control for remote access, and use of insecure protocols and credentials.

Regionally Significant Industrial Control Systems

Based on the targeting profile of Russian state actors from the 2023 U.S. Office of the Director of National Intelligence (ODNI) threat assessment and the percentage of energy generation for the Nordic countries, Dragos assesses the following ICS/OT systems are the most regionally significant:

Critical Infrastructure Vertical	System	Reasoning	Country
Telecommunications	Subsea Cable Infrastructure	The 2023 ODNI threat assessment specifically calls out Russia's intention to improve its ability to target critical infrastructure, including underwater cables and industrial control systems.	Entire Nordic Region

[1] SocRadar - dark-web-profile-noname05716/
[2] Sentinelone -Acidrain-a-modem-wiper-rains-down-on-europe

Energy	Shoreside/Offshore Wind Energy	Approximately 57 percent of total energy generation for the country[3]	Denmark
Energy	Hydro Power	Approximately 65 percent of total energy generation for the country[4]	Iceland
Energy	Hydro Power	Approximately 95 percent of total energy generation for the country[5]	Norway
Energy	Nuclear Power	Approximately 32 percent of total energy generation for the country[6]	Finland
Energy	Hydro-Electric/Wind Power	Approximately 34 percent of total energy generation for the country	Finland
Energy	Nuclear Power	Approximately 40 percent of total energy generation for the country[7]	Sweden
Energy	Hydro-Electric Power	Approximately 44 percent of total energy generation for the country	Sweden

TABLE 1 REGIONALLY SIGNIFICANT ICS/OT SYSTEMS IN THE NORDIC REGION

Cable landing sites are aggregation points that service subsea cables for critical infrastructure purposes, such as internet/telecommunications and power cables. The 2023 ODNI threat assessment specifically calls out Russia's intention to improve its ability to target critical infrastructure, including underwater cables and industrial control systems.

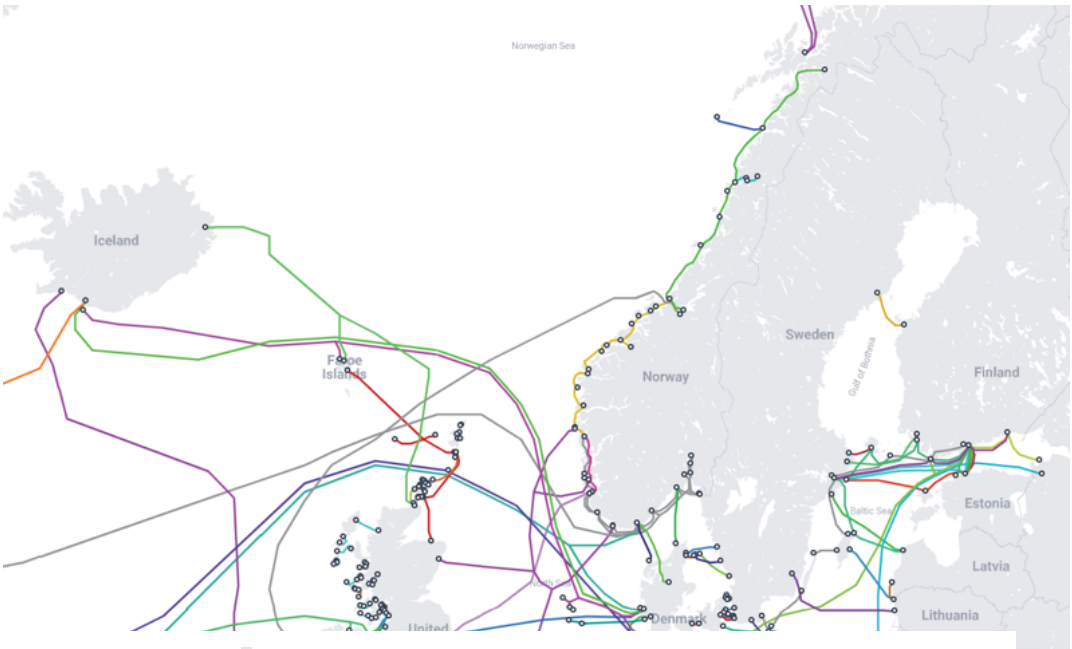


FIGURE 1 SUBSEA CABLE MAP IN THE NORDIC REGION

[3] World Nuclear - Denmark
[4] Our World in Data - Iceland
[5] Statista - Annual Hydro Power in Norway
[6] Trade.gov - Finland Energy
[7] World Nuclear - Sweden

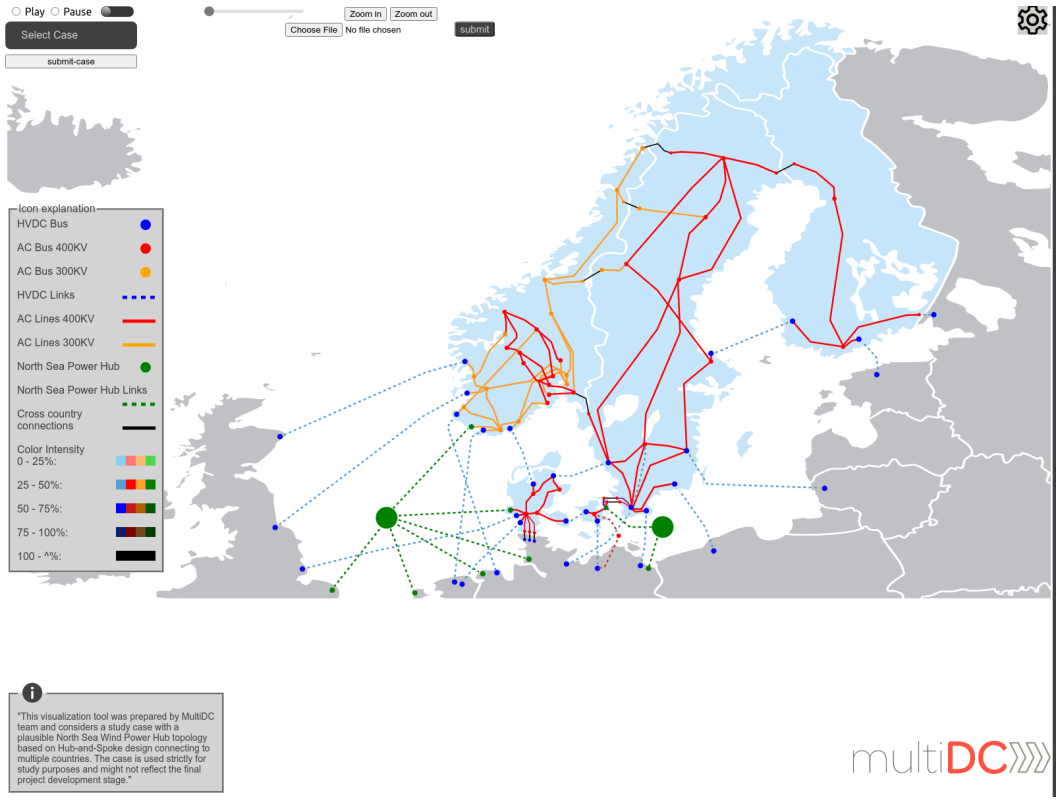


FIGURE 2 NORTH SEA WIND POWER HUB PROPOSALS (NOTE: SOME OF THESE SITES/CABLES ARE PROPOSED TOPOLOGIES)

Threat Environment

Distributed Denial of Service (DDOS)

DDOS via hacktivism is prolific in the Nordic Region. While hacktivism is generally a superficial threat to OT systems, the hacktivists operating in the Nordic Region have some concerning ties to larger threats. Anonymous Sudan is reported to be a sub-group of the pro-Russian threat actor Killnet[8]. This relationship increases the likelihood that the hacktivist groups will receive strategic tasking to aid Russian state objectives or even serve as distraction operations that benefit Russian operations.

The two primary hacktivist groups and their publicly known operations in the Nordic Region include:

- **Anonymous Sudan**
  - Swedish Railways and Scandinavian airlines websites were disrupted via DDoS in February 2023
- **NoName057(16)**
  - NoName057(16) leverages the crowdsourced DDoS tool known as DDosia9
  - NoName057(16) DDoS'd Swedish postal and telecommunication services in 2023

[8] Trustwave - anonymous-Sudan-religious-hacktivists-or-Russian-front-group
[9] Avast - ddosia-project

- SocRadar reports that 18.4 percent of the attacks from NoName057(16) targeted Sweden in January 2023[10]

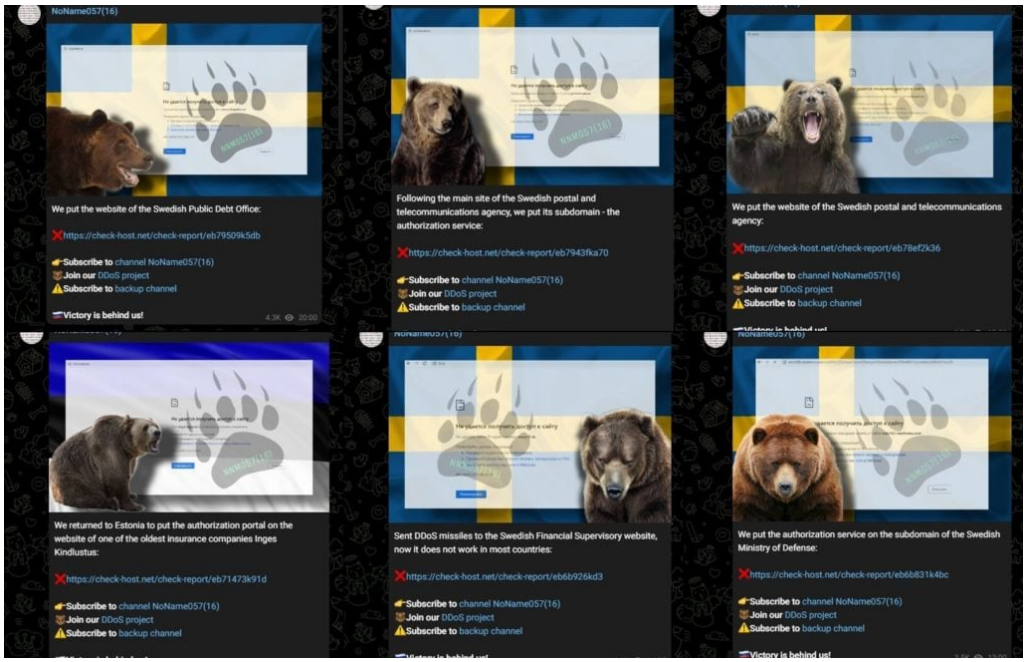


FIGURE 3 SOC RADAR'S COLLECTION ON RECENT CLAIMS OF DDOS ATTACKS IN SWEDEN[11]

Wiper Malware

Wiper malware that aims to destroy the memory contents of a computing device has a demonstrated history of spreading beyond its initial target, especially when paired with a worming capability. Wiper malware has been deployed against satellite communications provider ViaSat, in Ukraine that had impacts spread over into windfarms in Germany[12]. While the wiper malware did not infect the windfarm OT processes, the satellite communications capabilities of the wind turbines were disrupted because of the attack on the satellite communications provider. The AcidRain operators achieved initial access into the target environments through the exploitation of VPN devices. Lateral movement to the trust management segment of the Viasat KA-SAT network facilitated the deployment of the wiper malware. There have been at least 6 wipers deployed in Ukraine since the beginning of the Russian invasion:

- WhisperKill
- WhisperGate
- HermeticWiper
- IsaacWIper
- CaddyWIper
- Double Zero

[10] SocRadar - Dark-web-profile-noname05716
[11] SocRadar - dark-web-profile-noname05716/
[12] Sentinelone -Acidrain-a-modem-wiper-rains-down-on-europe

On January 13, 2023, Microsoft reported on new wiper activity originating in Ukraine from the threat actor dubbed Cadet Blizzard[13]**.** Microsoft reports that the wiper malware appears to target the Master Boot Record (MBR) when the device is powered down. This is a unique wiping mechanism that is not typical of wiper malware. Additionally, there is reported to be a fake ransomware note and has no mechanism for data recovery.

Wiper malware that has a demonstrated history of spreading to or having cascading impacts into neighboring EU countries. The Shamoon wiper[14] and NotPetya[15] are two examples of wiper malware that have spread into neighboring EU countries. In the case of NotPetya, the wiper malware impacted multiple verticals in critical infrastructure including government, banks, state power utilities, airports, and radiation monitoring systems. In the Nordic Region, DLA piper, Maersk shipping, and Heritage Valley Health Systems all reported system impacts from the wiper malware.

Known Exploited Vulnerabilities

Dragos OT threat groups such as KOSTOVITE, KAMACITE, and BENTONITE have a demonstrated history of rapidly tooling and exploiting "known exploited vulnerabilities" (KEV). KEV's on VPN and remote access devices are a target of choice for threat actors to gain initial access into industrial asset owner networks. Dragos sampled 30 publicly facing VPN devices from Renewable Energy asset owners in the Nordic Region and found that 54 percent of the enterprise VPNs are in use are Cisco SSL VPNs and 27 percent are Citrix remote access solutions.

While Dragos does not assert that one VPN solution is more secure than the other, exploits for Cisco and Citrix remote access solutions regularly appear on CISA KEV list, highlighting that Cisco SSL VPN and Citrix VPN exploits will have a proportionally larger risk in the Nordic Region Renewable Energy space.

[13] Microsoft Digital Security Unit - Destructive Malware Targeting Ukrainian Organizations
[14] https://www.ENISA - Shamoon Campaigns with Disttrack.
[15] CCDCOE -NotPetya

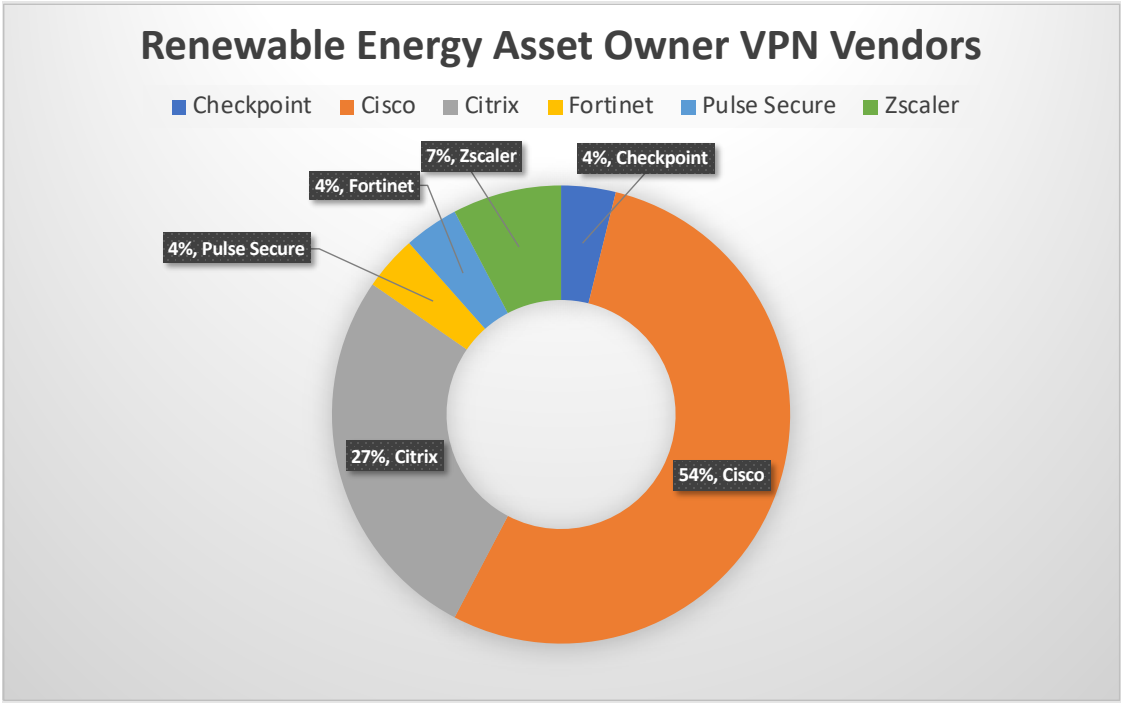


FIGURE 4 RENEWABLE ENERGY ASSET OWNER VPN VENDORS

ICS/OT Internet Exposure

ICS/OT assets that are directly connected to the internet are trivial targets for adversaries intent on impacting OT systems. These ICS/OT assets are at a high risk of disruptions to availability from DDoS and are often targeted by adversaries during the testing and development of offensive OT capabilities. Additionally, publicly connected ICS/OT assets are often targeted by hacktivists due to the high media coverage that ensues after an attack (whether successful or not). Dragos scanned for internet connected ICS/OT devices with data from from the Censys exposure management and threat hunting solution[16]. As of June 22, 2023, Dragos identified a total of 3960 connected ICS/OT assets in the Nordic Region, that is internet connected hosts that are running industrial protocols. A small portion of these may represent active honeypots within the region.

[16] Censys - Label Descriptions

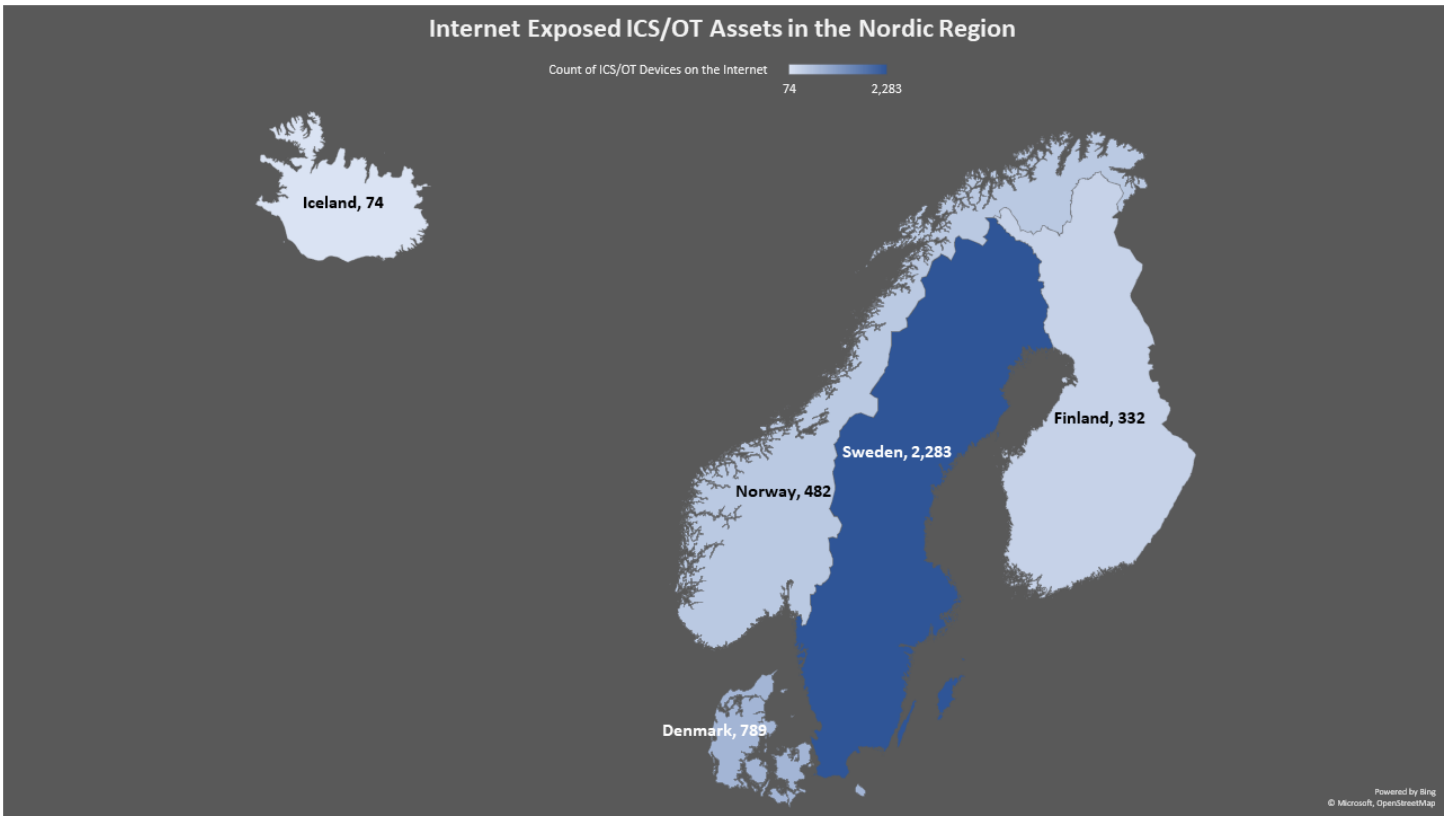


FIGURE 5 INTERNET EXPOSED ICS/OT ASSETS IN THE NORDIC REGION

Of the 3960 publicly connected ICS/OT assets in the Nordic Region, Sweden has the most ICS/OT assets hosted in its country.

Country	Count of ICS/OT Devices on the Internet
Sweden	2,283
Denmark	789
Norway	482
Finland	332
Iceland	74

TABLE 2 COUNT OF ICS/OT ASSETS PER COUNTRY

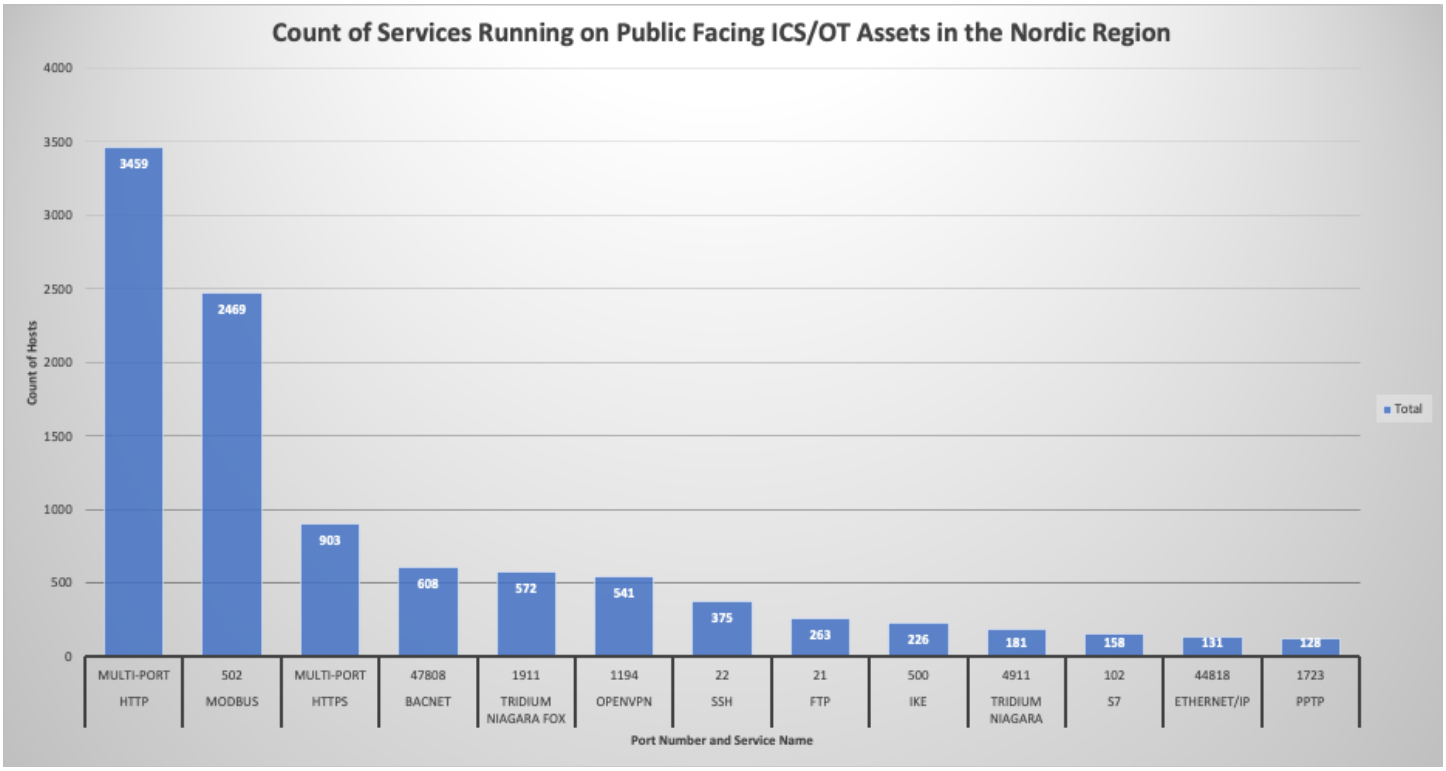


FIGURE 6 COUNT OF SERVICES RUNNING ON PUBLIC FACING ICS/OT ASSETS IN THE NORDIC REGION

Approximately 87 percent of the publicly connected ICS/OT assets in the Nordic Region are running an exposed HTTP service and 62 percent are running an exposed MODBUS service.

Risk of exposed MODBUS: The operational risk of an exposed MODBUS service largely depends on the implemented architecture of the control systems process. But at a minimum, an exposed MODBUS protocol is susceptible to a denial of availability and a lack of confidentially due to the plaintext nature of the protocol. The KAMACITE threat group has been observed leveraging the MODBUS protocol in the modular malware system dubbed "VPNFilter"[17]. KAMACITE's VPNFilter malware contains modules to enable downstream traffic manipulation, destruction of the infected host device, and likely enabled downstream devices to be exploited[18]. VPNFilter included a module specifically to monitor and track MODBUS TCP/IP packets. While the VPNFilter malware from KAMACITE was superseded by the CYCLOPSBLINK (which was also disrupted by NCSC, CISA, FBI, and the NSA), it highlights how OT threat groups can tool the MODBUS protocol for malicious purposes.

Count	Service Name	Port Number
3,459	HTTP	Multi-Port
2,469	MODBUS	502
903	HTTPS	Multi-Port

[17] Cisco Talos - VPNFilter
[18] NCSC - joint-advisory-shows-new-sandworm-malware-cyclops-blink-replaces-vpnfilter

608	BACnet	47808
572	Tridium Niagara Fox	1911
541	OpenVPN	1194
375	SSH	22
263	FTP	21
226	IKE	500
181	Tridium Niagara	4911
158	S7	102
131	Ethernet/IP	44818
128	PPTP	1723

TABLE 3 COUNT OF SERVICES AND PORT NUMBERS

Dragos Threat Groups

The following Dragos OT threat groups have a demonstrated history of targeting renewable energy systems and traditional energy source systems. While their activity has not been directly observed in the Nordic Region, these OT threat groups have targeted energy/renewable energy systems worldwide. Their TTPs can be used as a framework for OT threat groups that could shift their focus onto the ICS/OT systems in the Nordic Region.

CHERNOVITE

CHERNOVITE has the capability to disrupt, degrade, and potentially destroy industrial environments and physical processes in industrial environments. Through normal business, independent research, and collaboration with various partners in early 2022, Dragos identified and analyzed the capabilities of a new ICS-tailored malware PIPEDREAM. PIPEDREAM is the seventh known ICS-specific malware following STUXNET, HAVEX, BLACKENERGY2, CRASHOVERRIDE, and TRISIS. Based on current knowledge, the highest probability targets include Electric and Oil and Gas, specifically Liquified Natural Gas. These are the primary sectors that would have the biggest impacts and ripple effects from disruptive or destructive attacks. Notwithstanding this, several of the targeted devices also exist in other industrial settings, including but not limited to Backup Power Auxiliary Systems in the Nuclear industry, within Data Centers, and in manufacturing plants[19].

[19] Dragos - TR-2022-12

STIBNITE

STIBNITE targeted wind generation organizations and government entities in Azerbaijan. STIBNITE launched multiple intrusion operations against targets from late 2019 through early 2020, and uses PoetRAT remote access malware in its intrusion operations to gather information, take screenshots, transfer files, and execute commands. STIBNITE does not demonstrate the capability to disrupt ICS operations, although information and access achieved in Stage 1 could facilitate a follow-on Stage 2 event[20].

- Actively targets wind/energy with custom malware.
- They were first observed in 2019 targeting Yashma wind energy farms in Azerbaijan.

KOSTOVITE

KOSTOVITE targets renewable energy in Australia and North America. Its activities focus on initial access operations using perimeter device compromise and living off the land (LOL) using system and network administration tools native to KOSTOVITE's target. KOSTOVITE employs maliciously enlisted third-party Internet of Things (IoT) for relay infrastructure that is exclusive to one target. Dragos began tracking KOSTOVITE in 2021. KOSTOVITE activity appears to consist of information-gathering operations[21].

Rapidly weaponizes known exploited vulnerabilities for VPN and RDP services.

Threat Perspective

Critical Findings in Renewable Energy Systems

These findings are from Dragos Professional Services engagements on hydroelectric dams, wind farms, and solar farms. Dragos professional services has conducted architecture reviews (AR) on renewable energy systems around the world and compiled security findings from the control systems assessments. The following findings have been rated **critical** as their successful exploitation would result in critical impacts to the industrial process:

Dragos Critical Findings on Renewable Energy Control Systems	Threat Activity That Has Exploited the Finding
Vendor Managed Control Systems	Kaseya Supply Chain Ransomware attack: while this software is not control system specific, this event is an example of where vendor managed systems have been impacted through a compromise of the systems vendor/managed service provider[22]
Lack of ICS/OT Network Segmentation	The CRASHOVERRIDE malware leveraged the inherent trust in the OT network architecture to execute an impact on the 2016 Kiev power disruption[23]

[20] Dragos - AG-2020-01
[21] Dragos - AG-2022-04
[22] DNI.gov - Kaseya VSA Supply Chain Ransomware Attack
[23] Dragos - CRASHOVERRIDE

Insecure File transfer protocols	PoetRAT (STIBNITE) has used insecure file transfer protocols for C2 against energy sector targets[24]
OT systems can access the internet	Cl0p ransomware group exfiltrates date from the South Staffordshire water supply company that included screen shots of the control system's human machine interface (HMI)[25]
Vendor Managed Radius Account	Not yet observed
Limited Security Controls for Remote Access	Oldsmar Water Treatment facility incident was accomplished via legitimate remote access tooling (teamviewer) that lacked strict security controls[26]
Use of Insecure Protocols and Credentials transmitted via plaintext	Sandworm's use of interceptor-NG[27]

TABLE 4 DRAGOS PROFESSIONAL SERVICE ENGAGMENT FINDINGS ON RENEWABLE ENERGY CONTROL SYSTEMS

Forward Looking Assessment

Leveraging ODNI Threat Assessment and NTC Vulkan Files

Using information from the 2023 ODNI Threat Assessment and the series of alleged contracts between the Russian company NTC Vulkan and the Russian Ministry of Defense, Dragos assesses with low confidence that Nordic Region ICS/OT asset owners should prepare for the following threat activity:

- "Russia will continue to use energy as a foreign policy tool to try to coerce cooperation and weaken western Ukraine"- 2023 ODNI Threat Assessment[28]
    - Dragos assesses with moderate confidence that the Nordic Renewable Energy systems may be targeted by cyber threat actors, with a favored method of DDoS attacks
- "Russia will target ports as a means to threaten/control exports in the region" – 2023 ODNI Threat Assessment
    - Dragos assesses with low confidence that Nordic port operations may be targeted to threaten/control exports in the region, since many Nordic ports have a public-facing internet presence, there is a possibility of the port networks being targeted for operation disruptions
- Dragos assesses with low confidence that Nordic critical infrastructure entities may be targeted with malware that utilizes "living off the land (LOTL)" techniques. According to the NTC Vulkan Files, the development of malware that utilizes LOTL is favored.[29] LSASS Dumping for privilege escalation and

[24] MITRE ATT&CK - PoetRAT
[25] Dragos - AA-2022-40
[26] MITRE ATT&CK - Olsdmar Treatment Plant Intrusion
[27] welivesecurity - analyzing-disruptive-killdisk-attacks
[28] DNI.gov - 2023 ODNI Threat Assessment
[29] Dragos - TR-2023-10

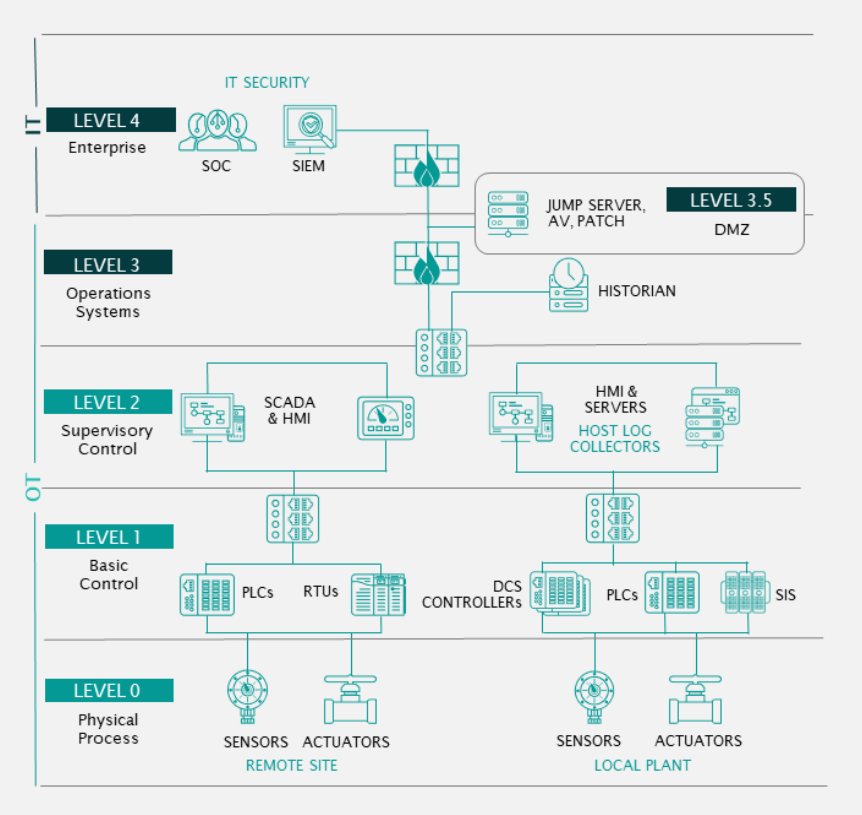
credential harvesting has been a commonly reported technique in a recent threat actor's TTPs from Microsoft (Cadet Blizzard[30]).

CURRENT LEVEL 4 THREATS

- DDOS
- Application Exploitation (MOVEit Transfer)
- VPN Exploitation (Fortinet SSL-VPN)

CURRENT LEVEL 0-3 THREATS

- Vendor Managed Control Systems
- Lack of ICS/OT Network Segmentation
- Insecure File Transfer Protocols
- OT Systems that can access to the internet
- Limited Security Controls for Remote Access
- Use of Insecure Protocols and Credentials transmitted via Plain Text



[30] Microsoft- cadet-blizzard-emerges-as-a-novel-and-distinct-russian-threat-actor/

ABOUT DRAGOS, INC.

Dragos, Inc. has a global mission to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

To learn more about a Dragos Threat Intelligence subscription, contact us for a demonstration.

Request a Demo

info@dragos.com @DragosInc @Dragos, Inc.