
nccgroup
Cyber Threat Intelligence Report
Energy Sector: Threats to Operational Technology

Contents

nccgroup

1. Executive Summary

NCC Group's Operational Threat Intelligence team was requested to identify threats to the Energy sector, with a focus on operational technology (OT) environments and the threat actors targeting them. Overall, the research identified hacktivists and Russian state-sponsored actors as developing their OT capabilities to target critical infrastructure, including Energy. Such developments appear to manifest in response to major geopolitical conflicts, and thus elucidate the conditions under which organisations in the sector may observe attacks to their OT infrastructure. Please note that the report, in line with its objectives, focuses on the threats to OT and the threat actors seeking to target these systems, as such, other threats such as espionage and ransomware are not analysed. These however should not be downplayed, as they pose an important threat to the

1.1 Caveats

The research undertaken for this engagement took place between 06/11/23 and 09/11/23. The findings represent a snapshot in time and do not constitute ongoing monitoring. As such, it is possible that after this date further information might become available.

Please also note that NCC Group are bound by certain legal and ethical commitments with regards the research which it can conduct in criminal spaces such as the Dark Web. NCC Group have not made any attempts to purchase access to data, or subscribe to illegal forums or marketplaces, and as such, these have not been scrutinised as part of this engagement.

2. Open Source Research

2.1 Objectives

The following is NCC Group's understanding of the objectives with regard to this engagement:

- To create a focussed report around the Energy sector highlighting threat actors moving towards targeting OT environments.
- To include information relating to OT targeted malware and attack examples where relevant.

3. General Challenges to the Energy Sector

3.1 Increased Digitalisation

Like many other sectors, Energy has undergone a major digital transformation under Industry 4.0, with the objective of increased efficiency, improved safety and the transition towards a net zero energy market. As a result, the sector holds a greater number of interconnected systems, resulting in a greater level of exposure to organisations. Specifically, the convergence of OT and IT has resulted in operational systems, traditionally air-gapped, to be accessible via the internet. This integration supports OT in its ability to monitor, control, measure and adjust industrial machines, as well as for companies to 'diagnose, maintain, track and optimise the physical industrial equipment that drive the businesses'.

Smarter infrastructure is integral to reaching net-zero ambitions, with infrastructure likely to become increasingly digital into the future as well. It is therefore imperative that devices are sufficiently protected, even more so as developments within the sector continue to move at a rapid pace. Positively, the Energy Cyber Priority 2023 report by the DNV found that 89% of the 601 Energy professionals surveyed believe cybersecurity to be a pre-requisite for digital transformation initiatives. In this respect, there is strong awareness for the vital importance of infrastructure resilience within the sector, as it becomes increasingly connected. This was further evidenced by the 72% of respondents who believe that their organisation is digitally advanced, and who consider themselves to be at greater risk of a cyber-attack than the average organisation (59%). That said, the research suggests more progress is required within the sector to translate this awareness into sufficient action.

3.2 Supply Chain Risk

In addition, the sector is characterised by vast supply chains, opening the door to greater risk if vendor products are not efficiently secured. Whilst 57% of those surveyed by the DNV reported good oversight of their supply chain vulnerabilities, this remains a top-five cybersecurity challenge. Likewise, it is uncertain whether good oversight translates into effective action or remains at the awareness level. Moreover, there is a potential danger that vendors may assume that the code used in their products is secure, meaning that they themselves could be unaware of the risks presented to clients.

To mitigate against this, the DNV cites the Software Bill of Materials (SBOM), which identifies the different components of the software, and can be employed to improve security. This can avoid assumptions around the quality assurance of OT products and support wider efforts to limit a cybercriminals' ability to compromise systems. Like many other sectors, the supply chain risk is emphasised, as it is considered a key threat to organisations across the broader threat landscape. The US Department of Energy stressed that supply chain risks to digital components will continue to evolve and likely increase, as systems are increasingly interconnected and operated remotely. Hence, it remains critical to ensure the security of both the systems operated in the immediate organisation, as well as that of the supply chain for maximum OT security.

Greater interconnectivity and vast supply chains are only a couple of examples that render OT environments more insecure, and provide attack vectors for threat actors both in this sector and more broadly. Additional factors should also be considered such as poor network segmentation, lack of visibility of OT assets, or insecure connections. It is important for those within the sector to remain aware of all of the factors that can make their organisations vulnerable to exploitation, to ensure strong cyber resilience overall, and to prevent threat actors from targeting OT and IT environments.

4. Threat Actors Targeting Operational Technology

In the Energy sector, the targeting of OT environments has been most prominent in the context of major geopolitical tensions. OT is often targeted for destructive and/or disruptive purposes, and this has proven all-the more evident where considering the ongoing Russia-Ukraine war, in which several incidents have emphasised the threat posed to Energy. Importantly, Energy professionals in the aforementioned survey reported that present geopolitical uncertainty has made them more aware to the vulnerabilities which reside in their OT environments, with two-thirds of respondents having heightened their cyber resilience as a direct result of the conflict.

Furthermore, the survey reports that standard risk assessments which previously deemed war as an unlikely risk factor to Energy infrastructure have been reviewed, with a classification of ‘very likely’ pushing for greater security efforts and regulatory compliance to protect Energy. Overall, greater awareness of the threats posed to OT under these conditions are evident and are being heard by the sector.

Two types of threat actors in particular are often responsible for the targeting of OT environments, state-sponsored actors and hacktivists. The ability to disable, and or cripple energy infrastructure, can result in limited to no access for its consumers, adding to the instability and chaos that war and conflict bring. Such acts of sabotage play into the all-important power dynamics of international security issues, as those responsible seek to achieve their objectives in their operations. In this respect, it is unlikely that the targeting of OT environments in the Energy sector under such conditions will cease, and those within the sector should enforce strict cybersecurity measures to protect both IT and OT.

4.1 State-Sponsored Activity

The targeting of industrial environments in the Energy sector is not new, with the sector having observed major attacks including Stuxnet 2010, BlackEnergy 2015, Industroyer 2016, and the Triton/TRISIS attacks of 2017. Each of these events had detrimental consequences, whether it be the global spread of the Stuxnet worm beyond the nuclear centrifuges, the crippling of Ukrainian power grids or the disabling of safety critical systems in a Saudi Arabian petrochemical facility. Most recently, the Russian Advanced Persistent Threat actor (APT) Sandworm has demonstrated that state-sponsored actors are still prepared to employ ICS-targeted malware to cripple Energy infrastructure in sabotage operations, in times of geopolitical unrest.

4.1.1 Sandworm: Industroyer2 and CaddyWiper Attacks

Early on in the war, Russia employed a renewed version of the ICS-capable malware Industroyer, dubbed Industroyer2, to target a Ukrainian energy company. These destructive attacks were scheduled for the 08/04/22, and were reported to have been planned for at least two weeks prior. Notably, the malware's close association to Industroyer, exploited by Sandworm in the Ukrainian 2016 attacks, demonstrates how threat actors can develop existing capabilities to new environments and objectives. As such, remaining astute to pre-existing malware exploited to target OT environments in the sector should form a key part of organisational defence measures.

ESET research reports that Sandworm deployed Industroyer2 against high-voltage electrical substations to cut power in a Ukrainian region. Additionally, they distributed the CaddyWiper malware against the Ukrainian provider, likely to erase their presence on the machines. Industroyer2 implements the IEC-104 (IEC 60870-5-104) protocol to communicate with industrial equipment, with components believed to control specific ICS systems to cut power. Alongside Industroyer2, the CaddyWiper destructive malware renders response and recovery more difficult where preventing operators from regaining control of ICS consoles as well as hiding evidence of the malware.

Although the attackers were unsuccessful in cutting power to Ukraine in March 2022, thanks to defence efforts, the events demonstrate the desire to target OT networks in the Energy sector, as well as an evolution in OT targeting capabilities. Critically, had the attack been successful, this would have left over 2 million Ukrainians without power, adding significant levels of disruption. The value of targeting OT systems is emphasised by the effort placed in designing ICS-tailored malware, with discussions at BlackHat 2022 noting the level of planning and technical sophistication. Having understood the potential for widespread damage, sophisticated actors will take the time to understand how OT systems function, and how they can be manipulated. This further demonstrates their recognition of the value of such targets, with the exploitation of OT systems thus unlikely to cease in the context of APTs. Furthermore, Energy, as critical infrastructure, provides a nice target for heightened disruption and thus the identification and targeting of OT within this sector appealing.

4.1.2 Sandworm: Ukrainian Power Outages using Living off the Land Techniques (LoTL)

Further targeting of OT systems in Ukraine was observed in October 2022, resulting in unplanned power outages, and which coincided with missile strikes to critical infrastructure. New research published by Mandiant identified Sandworm as exploiting both LoTL techniques, as well as a newer version of the aforementioned CaddyWiper to target Energy infrastructure.

The events are believed to have started on, or before, June 2022. Initial access was achieved through the IT network, from which threat actors breached the OT environment through a hypervisor hosting a SCADA system for the targets' substation. On October 10th, the attackers leveraged 'an optical disc (ISO) image named "a.iso" to execute a native MicroSCADA binary in a likely attempt to execute malicious control commands to switch off substations'. Researchers believe that, based on a September 23 timestamp, there may be a two-month period between the hackers accessing the SCADA system and creating the OT capability. Mandiant can confirm that the attack resulted in an unscheduled power outage. On October 12th, Sandworm employed the CaddyWiper malware likely to destroy evidence and add to the disruption.

Most notable is the exploitation of LoTL techniques, which demonstrates a clear evolution in Russia's capabilities and how they target OT systems. Attacks on the substation reflect continued interest in critical infrastructure and Energy related systems, with a focus on OT to inflict maximum disruption. Notably, Mandiant report this as posing an immediate threat to critical infrastructure that leverages the MicroSCADA supervisory control system, both in Ukraine and globally. Whilst Ukraine may be the focus of Russia's core efforts at present, the country has clear global interests and may seek to deploy similar capabilities as part of their offensive capabilities. Critically, these capabilities are not limited to MicroSCADA, the attackers are sophisticated enough to target other SCADA systems and programming languages. Organisations should be sure to review the recommendations in the Mandiant report referenced.

4.1.3 Summary

Overall, Russian APTs, notably Sandworm, appear to be evolving their OT capabilities to target Energy infrastructure, and this is evidenced by the revival of Industroyer (Industroyer2), the use of the CaddyWiper malware, as well as exploiting LoTL techniques. As techniques continue to develop, it is evident that Russia sees the value in incorporating OT targets within their broader offensive approach, and are likely to continue developing their capabilities. Importantly, their targeting of OT systems only occur under specific conditions, namely, geopolitical conflict, and this should alert organisations to the circumstances in which they may be most susceptible.

The above said, the targeting of OT in the Energy sector was however on a much smaller scale than anticipated during the Russia-Ukraine war, both in Ukraine and to her allies. In this respect, the Russia-Ukraine war has demonstrated that conventional weapons remain the primary offensive capability in war, with cyber currently adopting a supporting role. For example, in recent weeks, Russia is reported to have targeted energy infrastructure using missiles and drone strikes.

Hence, it can be inferred that whilst Russia is moving towards the targeting of OT systems in Energy and critical infrastructure, attacks only employ such capabilities on a needs basis. Overall, organisations should remain aware of the threat posed by ICS-tailored malware, LoTL techniques, the threat actors responsible, and the circumstances in which such events may occur.

4.2 Hacktivism and Operational Technology

Across 2022, hacktivists demonstrated a growing interest in OT systems, and illustrated how diverse threat actors are increasingly aware of their value as targets. More traditional hacktivist behaviours have taken the form of DDoS attacks, website defacements, and/ or data breaches. Whilst these all remain within their arsenal, a focus on accessing OT devices demonstrates an evolution in objectives and capabilities generally. Again, such activity appears circumstantial and aligned to geopolitical conflicts, but serves to inform organisations in the sector of the conditions in which such attacks are most likely to occur.

4.2.1 Russian-Ukraine Hacktivism

Within the conflict, a number of hacktivists have sought to target Energy amongst other critical infrastructure. For example, Hacken.io, a Ukrainian start-up in cybersecurity and cryptocurrency joined the call to arms in Ukraine's wider cyber-resistance effort. Notably, the group requested the submission of critical vulnerabilities in Russian government and infrastructure, including SCADA systems, Energy, Oil and Gas. As such, even newer hacktivist groups formed in response to the conflict are aware of the value, and seek to leverage ICS/OT environments.

In addition, a joint report by CITALID and Sekoia analysing cyber activity targeting the European Energy sector in 2022, identified several hacktivist attacks to the sector. These include claims by NB65 (part of Anonymous) of having compromised the OT systems of Russian oil distribution company Severnaya, including OpenSCADA devices. Furthermore, Team OneFist, a self-claimed hacktivist group supporting Ukraine, claimed to have compromised several Russian cities electrical control systems and to have removed data on targeted devices. In this respect, a growing interest in OT environments within Energy as part of hacktivists' broader approach is evident where defending Ukraine, with OT considered a valuable target where looking to maximise disruption.

4.2 Hacktivism and Operational Technology

Across 2022, hacktivists demonstrated a growing interest in OT systems, and illustrated how diverse threat actors are increasingly aware of their value as targets. More traditional hacktivist behaviours have taken the form of DDoS attacks, website defacements, and/ or data breaches. Whilst these all remain within their arsenal, a focus on accessing OT devices demonstrates an evolution in objectives and capabilities generally. Again, such activity appears circumstantial and aligned to geopolitical conflicts, but serves to inform organisations in the sector of the conditions in which such attacks are most likely to occur.

4.2.2 GhostSec as a Key Threat Actor

GhostSec were particularly active in 2022, with attacks on OT infrastructure within and outside of the sector. GhostSec have provided a good example of hacktivists evolving their tactics, where targeting ICS systems and programmable logic controllers (PLCs) specifically. Cybersecurity company Otorio reports that the group is 'polishing their knowledge of open-source tools, different OT protocols, and their capabilities, gaining access to devices such as Human Machine Interfaces (HMIs) and Programmable Logic Controllers (PLCs) with weak security configurations'.

GhostSec are increasingly capable of exploiting ICS misconfigurations, including poor segmentation, default credentials, and OT devices exposed online. Notably, these are some of the key weaknesses discussed by the security community as observed within industrial environments across sectors, stressing the threat. As a hacktivist group, attacks at present have resulted in more of a nuisance than a major threat to its victims. However, Otorio reports that those with more advanced skillsets and nefarious objectives may take note of their activity and seek to do greater damage.

As part of #OpIsreal, in June 2022, Ghostsec shared video evidence of an exposed ELNet interface, an energy meter and electrical power meter at the Scientific Industries Centre (Matam), having been accessed by the group. In July, the group targeted ICS systems at the Gysinoozerskaya Russian hydroelectric power plant, in support of the Ukraine war. A DDoS botnet was used to target ICS systems with the attack resulting in a large explosion, but no casualties. Finally, in September 2022, the group claimed to have compromised 55 Berghof PLCs in Israel (sector unknown), as well as alleging the compromise of water safety systems, having published images of water pH and chlorine levels.

4.2.3 Summary

Both the desire and ability to access OT reflects an understanding of the value of OT by hacktivist groups at present, whether this be the alleged compromise of Russian or Israeli infrastructure..

Whilst some examples crossover with the Utilities sector (water systems), or the sector is not specified (Berghof PLCs), the OT in question, ICS/SCADA, are employed across Energy infrastructure. As such, these examples remain important to understanding the wider risks where these systems are in operation. Furthermore, groups such as GhostSec do not appear to discriminate by sector, rather, they select their targets based on which systems have weak security protocols, such as default credentials. The threat is therefore posed to any sector that may have insufficient security measures protecting their OT, which could include Energy.

It is worth noting that whilst hacktivists may recognise the value of these systems, they may not fully understand what they have accessed or how to engage with it, if possible. For example, the aforementioned water breach concerned pool water rather than drinking water, however, it is assessed that the most likely aim of the breach was to demonstrate the ability to control pH levels regardless. Likewise, GhostSec's breach of Berghof PLCs did not provide direct control over the industrial processes, only some of the PLCs functionality.

In this respect, there is an unfamiliarity with OT environments; however, should hacktivists become more knowledgeable around OT, or more sophisticated actors target these systems, greater damage could be inflicted. What is evident nonetheless is that hacktivists are looking to include the targeting of OT systems as part of their offensive capability, and that sectors who operate ICS/SCADA, notably in critical infrastructure, should be alert to this.

.

5. ICS-Tailored Malware

Across 2022 and 2023, two new types of ICS-tailored malware were identified as posing a potential threat to industrial environments. Although yet to be observed in the wild, it would prove advantageous to the sector to remain informed of their capabilities and to implement mitigations now, prior to any potential future exploitation.

5.1 PIPEDREAM/ INCONTROLLER

Early on in 2022, Dragos identified the seventh known ICS-tailored malware, PIPEDREAM, otherwise dubbed INCONTROLLER by Mandiant. The malware is 'a modular ICS attack framework that an adversary could leverage to cause disruption, degradation, and possibly even destruction depending on targets and the environment'. PIPEDREAM is particularly threatening due to its cross-sector capability, as many industrial environments are likely to use the targeted equipment, and therefore a potential threat to Energy.

Dragos further reports that PIPEDREAM can execute 38% of known ICS attack techniques and 83% of known ICS attack tactics. It can manipulate numerous industrial PLCs and industrial software, including Omron and Schneider Electric controllers. Likewise, it is capable of attacking universally employed industrial technologies including CODESYS, Modbus, and Open Platform Communications Unified Architecture (OPC UA). Additionally, the malware leverages native functionality in Schneider and Omron devices. Given the level of sophistication, the researchers attribute this malware to state-sponsored threat actors, with the assigned name of CHERNOVITE, although no nationality has been officially confirmed.

PIPEDREAMs' capabilities could support CHERNOVITE to 'enumerate an industrial environment, infiltrate engineering workstations, exploit process controllers, cross security and process zones, fundamentally disable controllers, and manipulate executed logic and programming'. It is yet to be observed in disruptive and destructive attacks however, likely to be observed in future operations. Should the malware successfully compromise OT environments, there is real possibility for the loss of safety, availability, and control. An understanding of the threat should be clear to all sectors operating these technologies (such as Energy), and appropriate mitigations put in place. A full list of mitigations can be accessed in the Dragos Whitepaper.

5.2 COSMICENERGY Malware

In May 2023, Mandiant identified an additional OT/ICS focused malware posing a risk to Energy infrastructure. COSMICENERGY is designed to disrupt electric power by interacting with IEC 60870-5-104 (IEC-104) devices like remote terminal units (RTUs), which are often leveraged in electric transmission and distribution operations. Mandiant suggest that the malware is capable of causing cyber physical impacts, and comparable to those employed in previous incidents and malware, such as Industroyer and Industroyer2.

Researchers believe this may have been developed as a tool for simulated power disruption exercises hosted by Rostelecom-Solar, a Russian cyber security company, to recreate attack scenarios against energy grid assets. Attribution however is yet to be confirmed, and researchers note that this may have been created by additional threat actors.

Notably, Dragos conducted an independent analysis of COSMICENERGY and concluded that the malware does not pose an immediate threat to OT. Furthermore, they emphasise that the codebase lacks maturity, and sits behind more notable threats such as Industroyer2/ CRASHOVERRIDE. The ICS-experts agreed that the malware is likely to have been developed in training scenarios rather than for external use. What remains evident in both analyses is that organisations should ensure appropriate mitigations are in place regardless. This is the third identification of an IEC104 targeted tool, as such; organisations should ensure cyber resilience to reduce the risk of future attacks to energy infrastructure.

6. Final Comments

Overall, the Energy sector remains an important target within critical infrastructure as the ability to access, and or cripple systems, can support threat actors to achieve their respective objectives. At present, where considering those threat actors moving towards the targeting of OT environments and posing a potential threat to the sector, research points to hacktivists and Russian state-sponsored activity.

Specifically, hacktivists' have been evolving their tactics to incorporate the targeting of OT systems more generally, moving away from their traditional arsenal. This occurs mostly within wider geopolitical tensions, as threat actors take sides. Activity by groups such as GhostSec as well as broader efforts in the Russia-Ukraine war demonstrate an interest in ICS/SCADA systems, and an understanding of their value as a target. This is evidenced within the Energy sector and others, but should also push organisations operating ICS/SCADA systems more broadly to ensure sufficient mitigations are in place. Whilst hacktivists may in some cases only access such systems rather than manipulate them, should they learn how to target them more aggressively, this could pose a more serious threat. Likewise, more sophisticated actors may take note of the vulnerabilities in systems identified by hacktivists, and exploit such opportunities.

Additionally, Russian APTs, notably Sandworm, pose a threat to OT environments in the Energy sector, as evidenced by the recent use of Industroyer2, CaddyWiper malware and LoTL techniques. Through recent developments and improvements to their capabilities, it appears that Russia are maturing their offensive OT arsenal, with a risk to the Energy sector. Although less targeting of OT systems in the Energy sector has been observed during the war, both to Ukraine and to Western allies, it would be wise for the Energy sector to remain aware of Russian TTPs. Ultimately, conventional weapons continue to inflict greater damage and as such, cyber adopts a secondary role. This does not diminish its importance however, as evidenced by Russia's push to target OT systems, and we are likely to observe continued efforts by Russia to target OT systems in critical infrastructure.

Finally, it is important to remember that a number of other threats exist within the sector that may not concern the direct targeting of OT. Notably, ransomware and cyberespionage should not be ignored, and should be factored into the sectors cyber resilience plan. The direct and deliberate targeting of OT systems is less frequent, and manifests under specific conditions, notably, international conflicts. By contrast, ransomware remains a consistent threat to the sector, likewise, cyberespionage activity, notably by Chinese APTs, depicts intelligence-gathering efforts as alive and well. Organisations should not become complacent to these risks, but ensure a well-rounded approach to defence.

nccgroup

Our experts are here to help you every step of the way. Contact us today to learn more about cyber security.