



AUSTRALIAN CYBER THREAT PERSPECTIVE

DRAGOS, INC.
INTEL@DRAGOS.COM

SEPTEMBER 2022

SUMMARY

There are a few key elements influencing the Australian industrial control systems (ICS) and operational technology (OT) threat landscape and its elevated levels of cyber risk. These include the constant evolution of ICS/OT targeting adversaries, increased ransomware activity, the prevalence of supply chain threats, and the existence of sub-optimal security controls.

On this note, a range of criminal and state-sponsored adversaries have targeted Australian electric organisations. Specifically, at least 6 out of the 19 Dragos-designated threat groups either directly targeted or have the assessed capability to target electric organisations within Australia.

Adversaries targeting ICS/OT continue to seek initial access to electric utility networks to enable future attacks against these organisations. Additionally, numerous adversaries have demonstrated the capability of utilising offensive cyber tactics to disrupt electric operations through the misuse of control systems, employing specialised malware and leveraging a deep knowledge of the target operating environment. One example is the PIPEDREAM malware framework developed by the CHERNOVITE threat group, which poses a significant potential risk to industrial organisations, globally. CHERNOVITE's PIPEDREAM malware could theoretically cause disruption, degradation, or destruction of industrial environments, irrespective of the associated geography or industry vertical.

Furthermore, ransomware remains a continuous threat with the demonstrated potential to impact both information technology (IT) and operational technology (OT) infrastructure. This is especially the case in target environments where both IT and OT networks possess a flat architecture and inadequate segmentation. Additionally, with the existence of strains of ransomware that either target directly or indirectly ICS environments,

the ability to achieve disruption to the electric system is an ever-present threat. Such a disruption would have the potential to lead to significant financial loss, physical damage, reputational decline and potentially loss of life. Concerningly, an increasing number of Australian electric organisations have been targeted by these criminal groups.

The increased level of software/supply chain dependencies paired with the prevalence of vendor remote access within the Australian electric sector also poses a significant threat to electric operators. This operational reliance can introduce a range of third-party security risks into the customer's environment, including the possibility of targeted supply chain attacks. Numerous adversaries, such as the Dragos-tracked threat group XENOTIME, have historically used these techniques in an attempt to gain access to target ICS environments, thus indicating the prevalence of this initial access technique.

Moreover, the lack of adequate security controls in many industrial organisations may increase the risk of adversaries gaining access to OT networks and achieving their intended objectives. Numerous threat groups have historically leveraged the exploitation of vulnerable externally facing infrastructure/applications as part of initial access operations. This exploitation activity presents substantial risks to industrial organisations, as subsequent access obtained may be leveraged to perform internal reconnaissance, pivot from IT to OT, or deploy malicious tooling such as ransomware.

All the above elements come together to increase the overall risk of an intrusion-facilitated power disruption event. Such an event could occur at various points in electric system operations, including control centres, dispatch centres, or within the actual generation, transmission, or distribution environments. It is possible that in the future, the subsequent disruption could be an intended objective of a cybercriminal operation in

order to incentivise ransom payment. However, state-sponsored entities could also leverage this same disruption to support larger political goals. However, irrespective of the underlying intent, as adversaries and their sponsors invest more resources into obtaining disruptive capabilities, the risk of a disruptive or destructive attack on the electric industry significantly increases.

This observed threat activity ultimately highlights the critical importance of Australian electric organisations adopting

comprehensive security strategies with associated controls across both IT and OT environments. As part of this, organisations should focus on essential elements such as defensible architecture, monitoring and visibility, ICS incident response plans, remote access authentication, key vulnerability management, and comprehensive security policies.

KEY FINDINGS

Australian electric organisations are experiencing elevated levels of cyber risk. The growth in ransomware incidents, increased supply chain threats, inadequate security controls, and an overall increase in the sophistication of adversaries seeking to disrupt industrial entities all contribute to this risk. Notably, at least 6 out of the 19 Dragos threat groups directly targeted or have the assessed capability to target Australian electric organisations.

CHERNOVITE and the associated PIPEDREAM framework supersedes historical ICS malware limitations, with a highly flexible and adaptable framework that can be leveraged to impact a wide range of industrial organisations, potentially including electric entities in Australia.

Ransomware groups are increasingly targeting electric organisations in Australia. This is driven by a decreased barrier to entry (facilitated by factors such as the ransomware-as-a-service model) paired with a high rate of eventual financial success. These incidents can impact electric operations indirectly via disruption to IT infrastructure, directly in merged environments or through the deployment of ICS-aware ransomware strains.

Supply chain dependencies represent a real threat to industrial organisations with the potential to introduce numerous third-party risks into the environment. Compromised software updates, poorly secured third-party network connections, and abused remote access solutions provide a potential entry vector that could be exploited in a supply chain intrusion.

Adversaries continue to exploit vulnerable external infrastructure and applications as part of initial access operations. At least three out of the six Dragos-designated threat groups that have targeted Australian organisations have used this technique in previous campaigns.

THREAT GROUPS

Dragos is currently tracking a total of 19 threat groups that target ICS/OT environments or are conducting research on organizations possibly to enable future attacks. Notably, at least 6 out of these threat groups have directly targeted or possess the capability to target Australian electric organisations. These specific threat groups are listed below, along with the names of other threat groups that have shown some overlap in capabilities, targets, or infrastructure.

PARISITE



PARISITE targets utilities, aerospace, and Oil and Natural Gas (ONG) entities. Its geographic targets include Europe, the Middle East, North America and Australia. PARISITE uses open-source tools to compromise infrastructure and leverages known virtual private network (VPN) vulnerabilities for initial access. The scope of this group's targeting also includes government and non-governmental organizations. This group has operated since at least 2017, according to Dragos research. Dragos intelligence indicates that PARISITE serves as the initial access group that enables further operations for MAGNALLIUM.

 Associated Groups: FoxKitten, Pioneer Kitten, MAGNALLIUM

XENOTIME



XENOTIME is known for its TRISIS attack which caused the disruption at an oil and gas facility in the Kingdom of Saudi Arabia in August of 2017. It was specially tailored to interact with Triconex safety controllers and represented an escalation of ICS attacks due to its potential catastrophic capabilities and consequences. In 2018 XENOTIME activity expanded to include electric utilities in North America and the APAC region, oil and gas companies in Europe, the US, Australia, and the Middle East, as well as devices beyond the Triconex controllers. This group also compromised several ICS vendors and manufacturers, exposing them to potential supply chain threats.

 Associated Groups: Temp.Veles

DYMALLOY



DYMALLOY's victims include electric utilities, ONG, and advanced industry entities in Europe, Turkey, and North America. It is a highly aggressive and capable threat group that can achieve long-term and persistent access to IT and operational technology environments for intelligence collection. In Q2 of 2021, Dragos identified this threat group expanding its targeting to include the Asia Pacific (APAC) region based on newly identified malware samples illustrating their capability to operate globally.

 Associated Groups: Dragonfly 2.0, Berserk Bear

VANADINITE




In 2020, the United States (U.S.) Department of Justice (DOJ) and the Federal Bureau of Investigation (FBI) unsealed indictments against several nationals from the People's Republic of China (PRC).¹ Some activity noted in the indictment overlaps with VANADINITE operations targeting external-facing, vulnerable services, including various industrial organizations, including targets in Australia. The group uses vulnerabilities in external-facing network appliances, such as VPN gateways to gain initial access to networks and establish presence.

 Associated Groups: APT41, LEAD, Winnti Group

CHERNOVITE



CHERNOVITE is responsible for the development of PIPEDEREAM, which is a highly capable offensive ICS malware framework with 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 malware, PIPEDEREAM. PIPEDEREAM is the seventh known ICS malware following STUXNET, HAVEX, BLACKENERGY2, CRASHOVERRIDE, and TRISIS. Dragos assesses with high confidence this capability was developed by a state actor with the intention to leverage it in future operations. PIPEDEREAM malware is targeted to equipment in liquefied natural gas (LNG) and electric power environments, but CHERNOVITE could almost certainly easily adapt the capabilities of PIPEDEREAM to compromise and disrupt a broader set of targets.

 Associated Groups: In other publications, PIPEDEREAM has been referred to as INCONTROLLER and no alternative public group names have been assigned to CHERNOVITE at the time of this report.

KOSTOVITE



KOSTOVITE compromised a renewable energy operator in March 2021, achieving Stage 2 of ICS Kill Chain capabilities with confirmed access to the OT networks and devices. KOSTOVITE compromised the perimeter of this ICS/OT network by exploiting a zero-day vulnerability in the popular remote access solution Ivanti Connect Secure, formerly known as Pulse Secure. KOSTOVITE demonstrated a high level of operational discipline and network device knowledge and utilised living-off-the-land techniques by leveraging compromised admin credentials. KOSTOVITE was also able to move laterally to the OT environments of multiple facilities in two continents.

 Associated Groups: UNC2630

OVERVIEW OF THE ELECTRIC SYSTEM

The Electric System is an overarching system encompassing power generation, transmission and distribution – an operational structure that is complex, resilient, and interconnected. Before electricity reaches customers, it goes through multiple steps, including generation, transmission, and distribution. Electric power is generated from energy sources like fossil fuels, nuclear power, or renewables at power generation facilities. The transmission system carries electricity long distances from the plants to distribution substations before finally being distributed to customers. The transmission and distribution systems are comprised of substations containing transformers, which step up or down voltage levels to provide appropriate service delivery to industrial, commercial, and residential customers.



Figure 1: An Overview Of The Electric System And Its Primary Components

The Australian Energy Market Operator (AEMO) oversees the transmission planning in Australia, whereas transmission network service providers (TNSPs) are responsible for transmission operations in their respective States/Territories.² The TNSPs in Australia include the Northern Territory Electricity System and Market Operator (NTESMO) in Northern Territory, the Wholesale Electricity Market (WEM) in Western Australia, and the National Energy Market (NEM), which covers the rest of the country.

The interconnection of many local electric grids forms these systems. This interconnection model facilitates the safe and reliable flow of power and enables some flow between interconnections through Direct Connection (DC) tie lines. This design allows power flows to occur through multiple paths within an interconnection and contains frequency disturbances. The engineered approach provides redundancy, protections from complete collapse, and numerous benefits during emergency operations. However, while the system has largely been resilient, the complexity has increased considerably. Consequently, such interconnections and dependencies have the potential to reduce the overall levels of resilience, especially in scenarios such as prolonged targeted cyber-attacks.

However, electric utilities have processes to provide mutual aid to other entities if one experiences an event such as a storm, fire, or cyberattack affecting their service territories. Regional mutual assistance groups and industry partnerships can share resources and enable stabilization and reliability following disruptive or destructive events. Electric utilities have well-defined emergency operations procedures to control and position the electric system during degrading operational conditions, including public appeals for reducing load, service interruptions, load shedding, power system restoration actions and financial incentives for generators via Frequency Control Ancillary Services (FCAS).

Additionally, in many parts of the world, the electric sector leads other industrial sectors in security investments. While security investments have historically been focused on enterprise information technology (IT) networks, there is significant advancement in operational technology (OT) security underway. For example, in Australia, the electric sector has been working to address cyber threats through the Australian Energy Sector Cyber Security Framework (AESCSF). However, this is not an enforced regulation.

THREATS TO AUSTRALIAN ELECTRIC ORGANISATIONS

The following section provides a strategic overview of the Australian electric threat landscape and the various elements of the unique risk environment.

ICS/OT TARGETED THREATS

THREAT LANDSCAPE

ICS/OT targeted threats continue to grow in both prominence and sophistication. In the last 18 months alone, Dragos has discovered four threat groups, bringing the total of tracked groups (worldwide, across all verticals) to 19. Concerningly, at least 6 of these have either targeted or have the capability to target Australian electric entities.

Dragos-designated threat groups must demonstrate the intent, opportunity, or capability of impacting industrial operations. Some of these threat groups may be solely focused on initial access development and the enumeration of the victim's internal resources. This subsequent information gathering could support economic or strategic objectives or potentially enable future attacks/operations. VANADINITE's exploitation of vulnerable external network and security devices to facilitate initial access into industrial environments is a prime example of this.³ However, some of these threat groups are possibly more nefarious, with the explicit goal of disrupting or destroying specific industrial infrastructure through targeted ICS/OT cyberattacks. A notable example of this includes the Dragos-designated XENOTIME threat group.



CASE STUDY: XENOTIME

XENOTIME is widely known for the destructive malware targeting Schneider Electric's Triconex safety instrumented system in 2017 – this was a historically significant escalation of attacks targeting ICS systems.⁴ While all assessments of the event indicated that the attack failed, targeting a safety system indicates significant damage and loss of human life were either intentional or acceptable goals of the attack.

Moving forward, in February 2019, while working with clients across various utilities and regions, Dragos identified a persistent pattern of XENOTIME activity attempting to gather information and enumerate network resources associated with U.S. and Asia-Pacific electric utilities.⁵ This behaviour may indicate that the threat group was preparing for a further cyber attack or, at minimum, satisfying the prerequisites for a future ICS-focused intrusion. These activities are consistent with Stage 1 of the ICS Cyber Kill Chain involving reconnaissance and initial access operations. XENOTIME's observed activity also included incidents of attempted authentication with credentials and possible credential stuffing, which may have also involved using stolen usernames and passwords to try and force entry into target accounts.

While none of the electric utility targeting events has resulted in a known, successful intrusion into victim organisations to date, the persistent attempts and expansion in scope are cause for definite concern. Of note is that XENOTIME has historically compromised several oil and gas environments, demonstrating its ability to do so in other verticals. XENOTIME currently remains one of only five threats (along with CHERNOVITE, ELECTRUM, Sandworm, and the entities responsible for Stuxnet) with the demonstrated capabilities to execute a deliberate disruptive or destructive attack against ICS entities.



CASE STUDY: CHERNOVITE

PIPEDREAM is a disruptive and potentially destructive ICS-specific malware framework, which has been developed by the Dragos designated Threat Group, CHERNOVITE.⁶ Dragos identified and analyzed PIPEDREAM's capabilities through normal business operations, independent research, and collaboration with various partners in early 2022.

Dragos assesses with high confidence that CHERNOVITE is a highly motivated and well-funded state sponsored entity, that is skilled in software development methods, well versed in ICS protocols, and experienced in intrusion techniques.⁷ CHERNOVITE has the theoretical capability to operate in both IT and OT networks and possesses a breadth of ICS knowledge beyond any of Dragos' previously discovered threat groups. PIPEDREAM has combined both the specificity and breadth of earlier ICS malware examples into a more modular and flexible platform.

While Dragos assesses with high confidence it has not yet been employed for disruptive or destructive purposes, PIPEDREAM has the potential to impact a wide variety of industrial control PLCs and industrial software, including Omron and Schneider Electric controllers. However, these target devices, while indicative, are not an exhaustive list by which the framework is bound. Rather, it is possible that adversaries could leverage the tool to target a wide range of other devices in the future – including the potential of electric entities in Australia.

ASSESSMENT

Dragos assesses with high confidence that ICS/OT targeting adversaries will continue to target Australian electric organisations for both initial access and potential disruption/destruction activities.

RANSOMWARE

THREAT LANDSCAPE

Dragos analyses and monitors the activities of 37 ransomware groups that have targeted industrial organisations and infrastructure.⁸ While the majority of these groups are financially motivated criminal entities, some state-sponsored adversaries may also leverage ransomware as part of strategic cyber operations (e.g., the Winnti Group).

Moreover, there is a continued prevalence of ransomware activity. In fact, in the last 12 months, there have been at least 23 ransomware incidents involving electric and energy organisations. There have also been at least nine additional attacks against third parties/suppliers related to the electric sector, posing the added risk of a supply chain compromise. Numerous factors have driven this trend, including OT Digital Transformation, suboptimal organisational security hygiene and an increased willingness of ransomware operators to target industrial entities.

Ransomware incidents can impact the operations of electric organisations in a wide variety of scenarios. Firstly, in the case of IT-specific ransomware (e.g., Conti or Lockbit 2.0), initial IT compromise may be followed by lateral movement into OT environments (e.g. in settings with flat architecture) with subsequent ransomware deployment. This can lead to a significant direct operational impact. However, even if an OT foothold is not obtained, direct IT impact can lead to the secondary OT impact via the disruption of business-critical IT systems or the ceasing of all operations as a defined safety precaution.

In addition to the prevalent IT-dominant groups, Dragos is aware of ransomware strains that deliberately target ICS/OT environments. A prime example is the EKANS ransomware, which emerged in mid-December 2019. EKANS featured additional functionality to forcibly stop numerous processes related to ICS operations.⁹ The specificity of processes listed as a static “kill list” demonstrated a level of intentionality previously absent from ransomware targeting the industrial space, acting as yet another reminder of the increasing frequency in which ransomware groups are targeting industrial organisations globally.

Finally, another risk associated with the deployment of destructive malware in an ICS environment is represented by the historian technology, since historian deployment is often architected in a manner that bridges communications from

a read-only historian in an IT network segment and a plant historian within the OT network. Moreover, sensor data is short-lived unless recorded in a historian and a destructive attack on its data could result in unrecoverable losses if not well defended and backed up.

**ANALYST
NOTE:**

Cybercriminal organisations continue to leverage ransomware as part of their operations, owing to the lowered barrier of entry facilitated by the Ransomware-as-a-Service (RaaS) model, paired with the continued profitability and high chance of eventual success. Most ransomware operators are financially motivated organisations, and consequently, they constantly explore new tactics that enhance the probability of being paid. A prime example of this is the increased use of data extortion techniques, whereby compromised victim information is threatened to be released on adversary websites or hacking forums if the associated ransom is not paid. The leaking of this information can create numerous security challenges for an electric organisation, as some of the leaked data may contain internal technical details (e.g., architecture maps or firewall rules) that a separate adversary could leverage to enable future attacks against the victim.

However, this same fixation on incentivisation may also play into targeting decisions made by the adversaries. More specifically, it may contribute to the increasing number of industrial organisations being targeted by these operators. Disruption to these organisations can have crippling impacts on the victim, secondary industries, or society as a whole. All in all, this critical need to ensure operational stability can act to further incentivise ransom payment, thus facilitating a positive feedback loop of increased industrial targeting.

CASE STUDY: CS ENERGY

On 30 November 2021, Australia-based electricity generating company, CS Energy, stated that it was responding to a ransomware incident that occurred there.¹⁰ Thankfully, the incident occurred on the corporate network and did not impact electricity generation at Callide and Kogan Creek power stations. However, notwithstanding this lack of ICS impact, this case study highlights that Australian electric organisations are not exempt from being targeted by ransomware operations. Moreover, should a similar incident occur at another electric organisation with merged environments or a flat architecture, the possibility remains that the impact could carry over to the OT environment.

ASSESSMENT

Dragos assesses with high confidence that financially motivated ransomware groups will continue to target Australian electric organisations.

SUPPLY CHAIN AND THIRD-PARTY RISKS**THREAT LANDSCAPE**

The increased dependency of Australian electric organisations on a range of suppliers, vendors and other third parties has ultimately acted to increase the levels of supply chain and third-party risks.¹¹ Historically, there have been numerous examples of supply chain compromises that leveraged exploited software updates and routine patching, a notable example being the SolarWinds incident. However, Original Equipment Manufacturer (OEM) and vendor remote access solutions also act to add to this risk. Remote access solutions are a vital component of modern OT equipment

solutions. This was especially the case during the Covid-19 pandemic owing to the increase in remote workforces. These solutions are critical in providing access to vendors, troubleshooting issues, and ensuring that optimal functioning of the underlying equipment is maintained. However, remote access solutions can also potentially provide an ingress into ICS/OT environments via compromised or poorly secured connections. One of the most notable examples is XENOTIME's targeting and subsequent compromise of numerous ICS vendors, hardware manufacturers, software suppliers, and integrators, which provided potential supply chain threat opportunities via vendor-enabled access to target ICS networks.¹²



CASE STUDY: KOSTOVITE

In March of 2021, the Dragos Threat Group KOSTOVITE compromised a renewable energy operator.¹³ Dragos deployed a team of investigators to analyze the intrusion and determined that the organization was not an opportunistic target. Initial access was obtained via the exploitation of vulnerable Pulse Connect Secure (PCS) Virtual Private Network (VPN) remote access devices. KOSTOVITE used dedicated operational relay infrastructure against this target to obfuscate the origin of its activities and then stole and used legitimate account credentials for its intrusion. KOSTOVITE then used the stolen account information to move laterally and gain access to the OT environments of multiple facilities on two continents from the one single ingress location. Once past the perimeter ingress, KOSTOVITE relied on Living Off The Land techniques to facilitate the lateral movement. KOSTOVITE then accessed servers used by the target for monitoring and control. In the course of the investigation, the Dragos analysts determined the adversary had been undetected and active in the OT networks for at least a month. The KOSTOVITE intrusion highlights the risks of interconnectivity between organizations.

ASSESSMENT

Dragos assesses with moderate confidence that adversaries will continue to leverage supply chain attacks to facilitate access into the target customer environment or to collect technical information that could enable a later offensive operation against the customers. Exploitation of Vulnerable Infrastructure.

Adversaries have frequently exploited vulnerable public-facing infrastructure and applications as part of initial access operations. In fact, at least 3 out of the Dragos-designated threat groups that have targeted Australian organisations have utilised this technique as part of their historical operations. These include VANADINITE, PARISITE and KOSTOVITE.^{14, 15, 16} The exploitation of vulnerable IT infrastructure poses numerous challenges for industrial organisations. In some cases, these externally accessible vulnerable technologies are also deployed in OT contexts, with successful exploitation yielding direct access to these environments. However, even if this isn't the case, access obtained may be used to perform internal reconnaissance and info collection operations within the IT environment or deploy ransomware and other malware – depending on adversary objectives.



CASE STUDY: VANADINITE

VANADINITE conducted extensive initial access campaigns in 2019 focusing on a range of industrial sectors, including electric utilities. As part of these operations, VANADINITE exploited vulnerable external-facing network devices and utilised publicly available exploits to achieve initial access.¹⁷ From here, VANADINITE likely relied on access to compromised equipment to gather valid credentials to obtain lateral movement within a compromised environment. VANADINITE could then use these credentials for remote logon and process execution to move throughout the victim network. Such access could enable reconnaissance activities in an ICS environment and establish a foothold for future ICS disruptive events. While Dragos identified widespread VANADINITE targeting of industrial entity Information IT environments, Dragos does not assess that the group possesses an ICS capability, but rather is limited to Stage 1 of the ICS Cyber Kill Chain.

ASSESSMENT

Dragos assesses with high confidence that adversaries will continue to utilize the exploitation of vulnerable externally facing infrastructure and applications to gain initial access into the target environment.

DEFENSIVE RECOMMENDATIONS

Suboptimal security controls can enable adversary access into a target environment and facilitate the intended actions on objectives. In many parts of the world, the electric sector leads other industrial sectors in security investments. While the security investments have historically been focused on enterprise IT networks, there is significant advancement in OT security underway. It is crucial that this momentum is maintained – thus ensuring that organisations are adapting their security posture to the modern-day threat landscape. The following section highlights the key defensive recommendations associated with the findings outlined in this report.

ICS INCIDENT RESPONSE PLANS

Dragos recommends that asset owners and operators establish, practice, and continuously improve ICS incident response plans for when an incident occurs. It is essential to practice these response plans and incorporate them into tabletop exercises (TTXs) to identify any potential issues associated with the response plan before an actual incident eventuates. Incident response plan documentation should define processes and procedures that assign specific roles for remediation along with thresholds for entering the remediation phase of incident response. A recovery playbook should be included in documentation detailing remediation steps within each business unit. A continuous effort to identify and document affected systems should be organized once an event alert or notification has occurred. This allows recovery operations to account for resource requirements and equipment acquisition if necessary.

DEFENSIBLE ARCHITECTURE RECOMMENDATIONS

Every OT environment requires a defensible architecture, reducing cyber risks from an architectural perspective and enabling the human defender.

Dragos recommends the following actions to develop a defensible network architecture.

- ▶ Install anti-virus/anti-malware solutions on ICS workstations.
- ▶ Audit or scan systems, permissions, insecure software, and insecure configurations to identify potential weaknesses and remediate, as necessary.
- ▶ Limit access to resources such as file shares, remote access to systems, and unnecessary services over a network.
- ▶ Ensure an understanding of network interdependencies and conduct crown jewel analysis to identify potential weaknesses that could disrupt business continuity.
- ▶ Leverage industrial-specific threat detection mechanisms to identify malware within OT and reinforce defence in-depth strategies at the network level, leading to defenders' and analysts' more robust investigation ability.
- ▶ Conduct architecture reviews to identify all assets, connections, and communications between IT and OT networks. Identify Demilitarized Zones (DMZ) to restrict traffic between enclaves. Critically examine and limit connections between corporate and ICS networks to only known, required traffic.

- ▶ Identify security zones and conduits based on security or process requirements. ISA 62443 Part 3-2 provides guidance on this process. The Purdue Model is an example of segmenting based on how close to a process a system is and is a good baseline.
- ▶ Store IT network, OT servers, and data historians that host services or data lakes in the DMZ. These resources should be accessed in the DMZ rather than allowing a straight IT-OT connection.

VISIBILITY AND MONITORING RECOMMENDATIONS

Monitoring a network is crucial to identifying and defending against cyber threats. The focus of the associated controls is on improving – or, in many cases obtaining – visibility. This includes long-term logging to investigate potential compromises as new intelligence-derived information about incidents comes to light. The absence of such visibility significantly impairs an organisation's ability to identify malicious activity and threats, including control manipulation, ransomware and even safety manipulation.

Dragos recommends the following actions to develop a defensible network architecture:

- ▶ Configure all capable devices and network components in the ICS/OT environment to send logging and monitoring data to a centralised system.
- ▶ Configure network components to provide an increased level of logging and monitoring for those systems that do not have the native capability of providing logging and monitoring data to a centralised server.
- ▶ Utilise a supplemental ICS/OT-aware logging and monitoring system where possible to supplement the existing capabilities.
- ▶ Coordinate the ICS/OT-aware logging and monitoring system with a Security Operations Center (SOC) to allow for greater visibility and quicker response.
- ▶ Passively identify and monitor ICS network assets to identify critical assets, chokepoints, and external communications in the network.
- ▶ Leverage industrial-specific threat detection mechanisms to identify malware within OT and reinforce defence in-depth strategies at the network level, leading to defenders' and analysts' more robust investigation ability.
- ▶ Orchestrate the direction of connections so that system-to-system connections go from higher-security zones to lower-security zones, i.e., OT to DMZ and DMZ to IT.
- ▶ Implement a default "deny" access policy across the IT/DMZ/OT trust boundaries. This approach is akin to a firewall policy where everything is denied unless specifically allowed. This type of policy can be labour-intensive and requires more administration, working with vendors, operators, and application management to define the minimal set of allowed protocols and ports.

REMOTE ACCESS AUTHENTICATION

Remote access is a leading attack vector, whether internal to the company (IT remoting into OT) or external (OEM/ Integrator remoting into the OT). The most effective control to mitigate this risk is Multi-factor Authentication (MFA), and Dragos recommends that MFA be implemented whenever possible. Understandably, configuring MFA is not always possible; however, defensible architecture can compensate if MFA cannot be implemented. Below are Dragos' recommendations related to a remote access authentication:

- ▶ Establish remote connections that are made on request instead of always being accessible and monitor its usage to identify misuse or exploitation.
- ▶ Require MFA for any remote access into the OT network from internet-exposed VPNs or access portals. Additionally, any file transfer solutions should require MFA.
- ▶ Log and monitor access to remote sites from internet-exposed VPN or remote connectivity solutions. Use a "trust, but verify" approach to third-party and vendor access, as adversaries could utilize this trust relationship to access the OT network.

KEY VULNERABILITY MANAGEMENT

Defenders should not assess all vulnerabilities as equal. The priority assigned to each vulnerability should reflect the ease of exploitation, the associated risk, and the overall impact that can be achieved. With defensible architecture and monitoring in place, defenders are in a better position to identify and prioritize addressing vulnerabilities that can have the most impact to reducing threat surface and prevent exploitation by adversaries. Insights from defenders can identify and address the highest priority vulnerabilities from either a patching process or by mitigating security controls.

- ▶ Unsupported Operating systems are a high-risk asset. End of support indicates that these operating systems will no longer be receiving patches of any kind, including security patches. If an attacker was able to attack an unsupported operating system, that asset is at risk of vulnerabilities that came out after the end of support timeframe. Coordinate with applicable vendors to develop a plan to upgrade hosts running operating systems that have reached, or are approaching, end of support. While Microsoft has extended support for Windows 2012R2, asset owners and operators should consider working with vendors to upgrade these systems before reaching the listed support date.
- ▶ Prioritizing vulnerabilities that enable effects that allow adversaries either access to or the ability to interfere or manipulate an ICS process is crucial and should have a higher priority. However, defenders should determine what proximity and the security controls are in place that an adversary would have to defeat to exploit vulnerabilities. Defenders should not use this as an excuse for not addressing the vulnerability, but rather for determining and ordering patching priority.
- ▶ Audit or scan systems, permissions, insecure software, insecure configurations, etc., to identify potential weaknesses and remediate, as necessary.

SECURITY POLICIES

Security policies are a critically important component of an organisation’s security program. It is imperative to give field personnel, engineers, and other OT asset operators ICS/OT-specific cyber security training and to ensure their awareness of security policies and procedures. Organisations must establish and maintain policies and procedures to respond to and recover from an OT-specific cyber event. This will also assist in identifying operational gaps in any processes or procedures.

Below is a list (albiet not exhaustive) list of policies and procedures that should be common across ICS/OT environment security:

Policy Title	Description/Purpose
Asset Management	The process of receiving, tagging, documenting, and eventually disposing of equipment. It is critically important to maintain up-to-date inventory and asset controls to ensure computer/field equipment locations and dispositions are known. Furthermore, when equipment is scheduled to be decommissioned, there should be a documented procedure, thus allowing defenders to ensure their compliance with the associated process.
Change Management	This policy aims to reduce security risks that arise from changing devices, software, or configurations through documentation, approvals, and notifications.
Data Retention	A retention policy sets expectations for how long to keep various logs. This can also expose weaknesses in current retention policies and enable actions to gain visibility and long-term historical data to identify malicious activity.
Decommission/Disposal	Ensuring that old equipment does not contain sensitive information before removing it from possession.
Device Hardening	Reduce security risks that arise from changing devices, software, or configurations through documentation, approvals, and notifications.
Disaster Recovery	This policy establishes lines of communication and the actions necessary to continue operations in the event of a disaster.
Mobile Device Policy	A Mobile Device Policy defines the rules surrounding the use of mobile devices within the corporate and OT networks. Mobile devices, which include laptops, smartphones, external hard drives, and tablets, can unknowingly facilitate the transport of malicious media across network boundaries and security zones. This policy would establish expectations and procedures designed to minimize incidents or risk exposure from mobile devices.
Password Policy	This policy is a set of rules designed to enhance computer security by encouraging users to employ strong passwords and use them properly. OT environments should have strict password requirements and policies that address weak passwords, password age, lockout thresholds, and reuse.
Patch Management	The process of distributing and applying updates to software and operating systems for both routine and emergency or critical updates.

Policy Title	Description/Purpose
Remote Access	This policy is to define the rules and requirements for connecting to ICS/OT networks from any host including requirements for vendors or third parties. These rules and requirements are designed to minimize the potential exposure to ICS/OT networks from damages, which may result from unauthorized use of ICS/OT resources. Damages include unintended catastrophic process failures, unintended exposure (population or environment), loss of control, loss of view, loss of availability, loss of confidence in the system, regulatory fines, sustained process inefficiency, or loss of public confidence.
Third Party Security and Compliance	Establishing a routine security and compliance assessment and checklist to identify any risks associated with third party software or solutions.
Threat Intelligence and Vulnerability Sharing with Engineers and Operators	This policy establishes the importance of threat intelligence in securing the ICS/OT environment and drives efforts to collect and act on it. It also provides engineers and operators awareness of threats and to identify possible suspicious cyber activity.
Unmanaged and Transient Device Policy	This policy establishes procedures and policies around unmanaged devices that are consistently or temporarily but often connected to ICS/OT networks. This includes minimum specifications for device security, device hygiene, and logging to be allowed to access the network and its resources or make changes to connected ICS/OT assets.
Vendor/Transient Device Policy	This policy would establish expectations and treatment of vendor, third-party, or guest devices that can access OT networks.
Vulnerability Management	This policy attempts to ensure personnel are seeking information on network and system vulnerabilities and addressing them in a timely manner. The process also includes identifying, evaluating, treating, and reporting on security vulnerabilities in systems and the software that runs on them.

CONCLUSION

A range of Dragos-designated threat groups and ransomware operators have increasingly targeted Australian electric entities. Some of these groups perform ICS/OT targeting in support of broader economic, political, or strategic objectives, and others are purely financially motivated. However, irrespective of the underlying intent, this observed increase in adversary activity is cause for concern and may result in the disruption or destruction of electric environments. Additionally, the increased supply chain dependencies paired with a rise in third-party remote access into OT environments adds another element of risk, posing a very real supply chain threat to Australian electric organisations. Finally, the continued exploitation of vulnerable externally facing infrastructure and applications is a prominent initial access technique utilised by multiple threat groups.

The observed threat landscape ultimately highlights the critical importance of Australian electric organisations adopting comprehensive security strategies with the associated controls across both IT and OT environments. As part of this, organisations should focus on critical elements such as defensible architecture, monitoring and visibility, ICS incident response plans, remote access authentication, key vulnerability management and comprehensive security policies.

REFERENCES

- 1 [United States of America v. Jiang Lizhi, Qian Chuan, Fu Qiang – The United States District Court for the District of Columbia](#)
- 2 [About AEMO](#) - AEMO
- 3 [New ICS Threat Activity Group: VANADINITE](#) – Dragos, Inc.
- 4 [XENOTIME](#) – Dragos, Inc.
- 5 [Threat Proliferation in ICS Cybersecurity: XENOTIME Now Targeting Electric Sector, in Addition to Oil and Gas](#) – Dragos, Inc.
- 6 [CHERNOVITE](#) – Dragos, Inc.
- 7 [PIPEDREAM: CHERNOVITE's Emerging Malware Targeting Industrial Control Systems](#) – Dragos, Inc.
- 8 [Dragos ICS/OT Ransomware Analysis: Q1 2022](#) – Dragos, Inc.
- 9 [EKANS Ransomware and ICS Operations](#) – Dragos, Inc.
- 10 [ENERGY RESPONDS TO CYBER SECURITY INCIDENT](#) – CS Energy
- 11 [10 Questions to Ask Suppliers as Part of Third-Party Security Reviews](#) – Dragos, Inc.
- 12 [XENOTIME](#) – Dragos, Inc.
- 13 [KOSTOVITE](#) – Dragos, Inc.
- 14 [VANADINITE](#) – Dragos, Inc.
- 15 [PARISITE](#) – Dragos, Inc.
- 16 [KOSTOVITE](#) – Dragos, Inc.
- 17 [New ICS Threat Activity Group: VANADINITE](#) – Dragos, Inc.

OTHER SOURCES

- ▶ [United States of America v. Jiang Lizhi, Qian Chuan, Fu Qiang](#) – The United States Department of Justice
- ▶ [About AEMO](#) – AEMO
- ▶ [New ICS Threat Activity Group: VANADINITE](#) – Dragos, Inc.
- ▶ [XENOTIME](#) – Dragos, Inc.
- ▶ [Threat Proliferation in ICS Cybersecurity: XENOTIME Now Targeting Electric Sector, in Addition to Oil and Gas](#) – Dragos, Inc.
- ▶ [CHERNOVITE](#) – Dragos, Inc.
- ▶ [PIPEDREAM: CHERNOVITE's Emerging Malware Targeting Industrial Control Systems](#) – Dragos, Inc.
- ▶ [Dragos ICS/OT Ransomware Analysis: Q1 2022](#) – Dragos, Inc.
- ▶ [EKANS Ransomware and ICS Operations](#) – Dragos, Inc.
- ▶ [CS Energy Responds To Cyber Security Incident](#) – CS Energy
- ▶ [10 Questions to Ask Suppliers as Part of Third-Party Security Reviews](#) – Dragos, Inc.
- ▶ [KOSTOVITE](#) – Dragos, Inc.
- ▶ [VANADINITE](#) – Dragos, Inc.
- ▶ [PARISITE](#) – Dragos, Inc.

ABOUT DRAGOS,

Dragos has a global mission: to safeguard civilization from those trying to disrupt the industrial infrastructure we depend on every day. The practitioners who founded Dragos were drawn to this mission through decades of government and private sector experience.

Dragos codifies the knowledge of our cybersecurity experts into an integrated software platform that provides customers critical visibility into ICS and OT networks so that threats and vulnerabilities are identified and can be addressed before they become significant events.

Our solutions protect organizations across a range of industries, including power and water utilities, energy, and manufacturing, and are optimized for emerging applications like the Industrial Internet of Things (IIoT).

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 Dragos and our technology, services, and threat intelligence for the industrial community, please visit www.dragos.com.