INTEL@DRAGOS.COM

DRAGOS

OIL & NATURAL GAS CYBER THREAT PERSPECTIVE

MARCH 2022

SUMMARY

The oil and natural gas (ONG) industrial sector is a crucial foundation for other industrial sectors and for civil society in providing critical resources that enable operations in other industrial sectors. The risk to the ONG sector is high due to the increasing number of adversaries targeting the ONG sector. The ONG industry is a valuable target for adversaries seeking to exploit industrial control systems (ICS) environments for espionage or disruptive objectives. As the number of attacks against ICS overall increases, adversaries with a specific interest in ONG companies remain active and evolve their behaviors. A disruption event from a cyber-attack at an ONG facility can occur at any point across the three major stages of ONG operations: upstream, midstream, or downstream. This can come from: Activity Groups (AGs) targeting ONG interested in espionage and prepositioning for disruptive effects; ransomware groups looking to disrupt operations for quick, high- value payouts and vulnerabilities; and critical cybersecurity issues impacting Operational Technology (OT) networks.

Dragos has not identified any disruptive or destructive cyber operations targeting industrial processes against the ONG sector, or its OT networks in 2020 or 2021. Ransomware caused indirect disruptive effects on OT operations in the ONG sector, even though it only targeted the Information Technology (IT) systems. Certain adversary groups have developed and deployed ICS-specific capabilities such as XENOTIME, ELECTRUM, and DYMALLOY, while other adversaries most likely have created but not yet deployed ICS-specific capabilities such as VANADINITE, TALONITE, and KAMACITE. Certain adversaries actively seek to develop or obtain ICS-specific capabilities such as CHRYSENE, HEXANE, PARISITE, and MAGNALLIUM based upon the ICS Kill Chain.

ANALYST NOTE: Assessments on adversary intent or interest in developing ICS capabilities are produced from a combination of analyzing adversary victimology, previous intrusion data, capabilities, and potential objectives.

KEY FINDINGS

1 The cyber risk to ONG organizations in North America, Europe, South America, and the Asia-Pacific is increasing. At the same time, risk to the Middle East and North Africa remain at high level as before.

2 Dragos tracks seven Activity Groups targeting ONG in different regions, some sharing multiple regional targeting of ONG entities.

3 Between 2018 and 2021, the number of ransomware attacks on ICS entities increased over 500 percent, according to Dragos research, with five percent of attacks impacting ONG entities.

4 Oil and gas adversaries target and can exploit internet-exposed assets, remote access, and insecure vendor or third-party access and introduce serious risk to the operations environment. ONG.

ACTIVITY GROUPS

Dragos tracks seven Activity Groups (AGs) and various ransomware groups targeting ONG. Dragos does not speculate on the identity of AGs, and none should be implied.

PARISITE

PARISITE targets ONG, electric utilities, aerospace, and governmental and non-governmental organizations. Its geographic targeting includes North America, Europe, and the Middle East. PARISITE uses open-source tools to compromise infrastructure and leverages known Virtual Private Network (VPN) vulnerabilities for initial access. A recent shift by PARISITE included incorporating ransomware into its capabilities, known as Pay2Key. Adopting ransomware is a concerning change by this adversary as it provides additional opportunities to cause disruptive attacks that would have unknown effects when deployed in an OT environment.

Associated Groups: **FoxKitten, Pioneer Kitten, RUBIDIUM**

XENOTIME

XENOTIME targets include LNG companies in Europe and United States; ONG companies in Europe, United States, Australia, and the Middle East; electric utilities in North America and the Asia-Pacific (APAC) region. XENOTIME disrupted an ONG facility in Saudi Arabia in August 2017 using the destructive TRISIS framework, specially tailored to interact with Triconex safety instrumented system (SIS) controllers. The TRISIS attack escalated ICS attacks due to its potential catastrophic capabilities and consequences. XENOTIME t argets devices beyond Triconex controllers for manipulation or exploitation. This group also compromised several ICS vendors and manufacturers, providing a potential supply chain threat.

Associated Groups: **Temp.Veles**

DYMALLOY

DYMALLOY's victims include ONG, Electric, Nuclear, and industrial entities in Turkey, Europe, and North America. DYMALLOY is a highly aggressive and capable activity that can achieve long-term and persistent access to IT and operational technology environments for intelligence collection and possible future disruption events.

Associated Groups: **Dragonfly 2.0, Berserk Bear, Temp.Isotope, BROMINE**

CHRYSENE

CHRYSENE's victims include petrochemical, ONG, and electric generation sectors. CHRYSENE was developed from an espionage campaign that first gained attention after the destructive Shamoon cyber-attack in 2012 that impacted 20,000 computers at Saudi Aramco. CHRYSENE targeting shifted to Lebanon, with operations consistently targeting Lebanese government organizations.

Associated Groups: **Helix Kitten, GREENBUG, OilRig, APT34**

HEXANE

HEXANE targets ONG and telecommunications in Africa, the Middle East, and Southwest Asia. Dragos identified the group in May of 2019. In 2020 and 2021, HEXANE shifted operations to focus on Israel, Saudi Arabia, Morocco, and Tunisia.

Associated Groups: **Lyceum, Chrono Kitten**

KAMACITE

KAMACITE targets ONG, LNG, Electric, & Mining participated in multiple critical infrastructure intrusion events, including operations enabling the 2015 and 2016 Ukraine power events and the persistent campaign targeting United States (U.S.) energy companies from late 2019 to mid-2020. Dragos assesses KAMACITE as the activity group associated with developing access for other groups like ELECTRUM, which then follows through with the ICS-focused attack, as observed in 2016.

Dragos assess that KAMACITE does not have ICS-specific capabilities; however, it is an adversary group that enables access for other operational teams with ICS capabilities, making KAMACITE an important adversary to follow.

Associated Groups: **ELECTRUM, Sandworm, Voodoo Bear, IRIDIUM**

ANALYST NOTE: Dragos uses the industry classification established by the Cybersecurity and Infrastructure Security Agency (CISA) for industrial vulnerabilities. CISA reports vulnerabilities impacting ONG entities as part of the Energy Sector.

VANADINITE

VANADINITE targets ONG, energy, manufacturing, and government and educational organizations. Its targeting is geographically broad and includes North America, Europe, and possibly Asia and Australia. VANADINITE leveraged remote access vulnerabilities in 2021 to access OT networks and exfiltrate sensitive operations data from an Energy company in North America. VANADINITE activity is limited to Stage 1, initial access, and Dragos has not observed any ICS-specific capabilities for this AG.

Associated Groups: **APT41, Winnti, LEAD, Wicked Panda**

ANALYST NOTE: Dragos uses the industry classification established by the Cybersecurity and Infrastructure Security Agency (CISA) for industrial vulnerabilities. CISA reports vulnerabilities impacting ONG entities as part of the Energy Sector.

THREATS TO ONG INFRASTRUCTURE

Ransomware is the most significant and most prolific ongoing threat to ONG companies for the ONG industrial sector. Between 2018 and 2021, the number of ransomware attacks on ICS entities increased over 500 percent, according to Dragos data, with five percent of attacks impacting oil and gas entities. Additionally, ransomware adversaries are increasingly adopting ICS-specific process kill lists, demonstrating the ability to stop industrial processes in the OT environment. EKANS, Megacortex, and Clop are examples of ransomware that contain this type of code. IT to OT propagation is another ransomware concern in ICS. IT-focused ransomware can impact control system environments if it migrates into control system networks and disrupts operations. The United States (U.S.) Cybersecurity and Infrastructure Security Agency (CISA) reported an example of this on 18 February 2020. A ransomware incident impacted a natural gas compression facility at an unidentified U.S. pipeline operator. The ransomware event affected IT and ICS assets, causing loss of view and loss of control, potentially as far as Layer 2 in the Purdue Enterprise Reference Architecture (PERA) model. Although the ransomware did not target ICS, the operational disruption lasted two days. Operational impacts were likely caused by a combination of insufficient segregation of IT and ICS environments and shared Windows operating system infrastructure. Ransomware can also indirectly disrupt oil and gas operations by compromising enterprise resource planning (ERP), sales, procurement, order fulfillment, logistics, or IT infrastructure-managed shipping services that impact OT services.

Ransomware actors have increasingly threatened to leak data in order to put added pressure on victims to pay the ransom. Leaked data relating to impacted organizations can provide valuable information for adversaries, potentially leveraging third-party or supply chain compromise mechanisms. It can also help with attack targeting and development, as adversaries conduct open-source intelligence gathering to plan their operations.

The DarkSide Ransomware Group disrupted Colonial Pipeline IT network systems in May of 2021, resulting in the company suspending OT operations for an extended period and disrupting the delivery of petroleum products for a significant portion of the United States East Coast. The encryption of a billing and delivery system and concern for threats to OT operations ultimately caused the operational disruption. This incident highlights the risk of improper segmentation and shows how interconnected systems in both IT and OT networks can indirectly impact operations without direct attacks on the OT environment.

The effects of this disruption led to new directives for pipeline owners to report cyber incidents to CISA and submit reviews of current cybersecurity practices. Another directive was later issued that requires owners and operators of Transportation Security Administration (TSA)-designated critical pipelines to implement specific measures against ransomware and other threats to IT and OT networks.

- Commonly Observed Security Issues Contributing to Ransomware Attacks: After analyzing the results of architecture assessment engagements that Dragos has conducted at numerous ONG facilities, Dragos identified the following security issues that could potentially introduce or enable ransomware attacks: Credential reuse, shared credentials, weak credentials, or no passwords at all to access OT systems or workstations, including remote access.
- Weak OT network segmentation or lack of an ICS Network demilitarized zone (DMZ) is among the most observed critical risks uncovered in these assessments.
- Unmonitored vendor and third party-based remote access.

ICS-focused ransomware can disrupt operations and prevent safe and reliable connection, distribution, and management of ONG, and its related support services. Ransomware adversaries may unknowingly impact OT operations even if their intent is only extortion or ransom and not a directed goal designed to affect national security or critical functionality.

OIL AND GAS OPERATIONAL SEGMENTATION THREAT PERSPECTIVE

UPSTREAM

Upstream operations encompass exploration for oil and gas fields, drilling wells, and establishing production infrastructure for both onshore and offshore sites. Offensive cyber activity impacting these operations could disrupt the exploration and extraction of unrefined product or be used for economic espionage, especially around block bidding and exploration.

THREAT LANDSCAPE

The oil and gas upstream segment threat environment is relatively small compared to other oil and gas segments. The most likely ICS/OT target in this segment is the production portion of upstream operations. However, the potential for espionage is a far greater threat in the exploration enterprise network. The technology involved in Exploration and Production (E&P) requires adversaries to develop highly specialized capabilities to operate and interact in this ICS/OT network environment, especially at Purdue Model layers 3 to 0.

Dragos is not aware of any adversaries that have targeted upstream exploration and production operations. XENOTIME, however, has developed the capability to target SIS at an oil and gas facility in Saudi Arabia and upstream oil and gas asset owners and operators across the industrial sector may use this same SIS equipment. The most significant concern for upstream compromise is cellular networks, local telecommunication providers, and satellite connections. This is the adversary's most likely avenue of gaining access to upstream operations, including well sites and drilling operations. HEXANE has demonstrated the ability to utilize Internet Service Provider (ISP) connections, making access to upstream oil and gas operations a possibility.

MAJOR AREAS OF CONCERN FOR UPSTREAM

- Third-Party Equipment That Is Connected To OT Networks Without Restrictions.
- Shared And Unrestricted Vendor Remote Access.
- Limited Logging And Monitoring For ICS Environments.
- Lack Of Multi-Factor Authentication (MFA) For Remote Access.
- Unmanaged And Transient Engineering Systems.
- Insecure File Transfer.
- Configuration File Manipulation From Vendor Or Corporate Networks.
- Weak Or Non-Existent Configuration Change Management.
- Lack Of Network Segmentation Between Facilities.

RECOMMENDATIONS FOR UPSTREAM

- Use MFA where possible. For example, remote access into the OT network from internet-exposed VPNs or access portals should require MFA. Additionally, some file transfer solutions 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 upstream systems.
- Ensure that transient devices used to access wellhead systems and upstream facilities are managed, have appropriate security policies applied, and have anti-virus or Endpoint detection and response (EDR) systems installed.
- Verify the integrity of configuration files imported from the vendor or corporate sources to prevent tampering or manipulation.
- Implement a comprehensive and robust change management policy for upstream operational changes. In the event of adversary manipulation or interaction, track users who implement changes so the "patient zero" can be identified more quickly.

MIDSTREAM

Midstream ICS/OT operations link upstream production and downstream refinement. Midstream assets include field gathering systems, processing plants, pipelines, maritime transportation, rail transportation, and storage. Offensive cyber operations impacting midstream could disrupt the transport of unrefined and refined petroleum products, chemicals, and natural gas by pipeline, rail, or maritime methods, including at terminal points for product transfers to and from transport mediums.

THREAT LANDSCAPE

The oil and gas midstream segment threat landscape is the most prominent emerging attack surface, and that new AGs will target it due to its critical role between production and refining. The most vulnerable OT network target in the midstream segment is the pipeline transportation function of midstream operations. A secondary focus will also involve maritime and rail, although rail threats will likely focus more on transfer processes to cause loss of containment rather than the actual railway tank cars themselves.

Several adversaries have demonstrated the intent, motivation, or capability to target midstream OT environments in the current threat landscape. The adversaries most likely to develop and deploy these capabilities are XENOTIME and ELECTRUM, though VANADINITE and TALONITE most likely have the capacity but haven't demonstrated impact to midstream operations. Midstream oil and gas asset owners and operators may use the same technology as in other ONG segments, potentially reducing adversary efforts and resource investment to develop capabilities to target assets in multiple verticals. The Colonial Pipeline incident also shows the potential for disruption in midstream by impacting operationally dependent or connected IT network systems. Ransomware groups are the most likely to disrupt midstream operations at this time. However, their attacks are less likely to be targeted and more likely to be opportunistic criminal operations. The most significant risk from ransomware is the indiscriminate nature of halting processes, which can have unknowable outcomes of disruption or destruction of property due to the complexity of OT environments.

Asset owners and operators should note that an adversary seeking to collect operational information about OT environments is conducting espionage. This information also enables adversaries to develop capabilities to enact disruptive or destructive effects. For example, CISA detailed an operation from a Chinese state adversary against 23 Natural Gas Pipeline Operators between 2011-2013 wherein the adversary focused solely on operational network information in lieu of the typically targeted, high value IT network or economic data.

MAJOR AREAS OF CONCERN FOR MIDSTREAM

- Lack Of ICS/OT Network Visibility.
- Lack Of ICS/OT Network DMZ
- Dual-Homed Assets Between Supervisory Control And Data Acquisition (Scada) Equipment And The IT Network.
- Limited Logging And Monitoring For ICS Systems.
- Lack Of Multi-Factor Authentication For Remote Access.
- End Of Life Operating Systems.
- Lack Of USB Scanning.
- Insufficient Network Segmentation.
- Shared Credentials.
- Reused Local Administrator Password.
- OT Endpoints Exempt From Security Policy Or Antivirus/Edr.
- Overly Permissive Allowlist Or Non-Existent Blocklist.

RECOMMENDATIONS FOR MIDSTREAM

- Place devices such as the following in the OT DMZ:
  - Jump host or server – A jump host or server is a network access system used to access and manage network devices or hosts in a separate network segment. A jump host or server should be hardened, monitored, fully patched, and include separate logons/accounts with multi-factor authentication methods to traverse between an IT and OT network.
  - Historian server mirror – Having a historian mirror in the DMZ offsets the risk of having historians or OT connections in the IT network which can be at risk of disruption and impacting operations.
  - File transfer solution – Place a secure, monitored file transfer system between in the DMZ between IT and OT networks. Conduct regular patch maintenance and review for suspicious activity.
- Force connections or data from the corporate network or ICS/OT network to terminate in the DMZ. For example, remote access from the corporate network should terminate on a jump-host and be required to initiate a session from there using RDP or an application. Push historian data into a historian server or mirror in the DMZ. That mirror server would then push the data into the corporate network to another mirror server where users would then be able to read or retrieve it.
- 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.
- Store servers and data historians hosting services or data that both the OT and IT networks use in the DMZ. Access these resources in the DMZ rather than allowing a direct IT-OT connection.

DOWNSTREAM

Downstream ICS/OT operations focus primarily on refining crude oil and raw natural gas and consumer distribution. Dragos assesses that oil and gas downstream operations are currently the most significant target due to the number of volatile processes, operational environment conditions, and criticality of the operations in downstream facilities. The nature and role of refining facilities make them particularly high-value targets for adversaries. Offensive cyber operations impacting downstream operations could disrupt fuel refining and processing, electricity generation, fuel storage, and the ability to maintain fuel reserves.

THREAT LANDSCAPE

Several adversaries have demonstrated the intent and capability to target downstream environments in the current threat landscape, specifically refinement. XENOTIME has shown the capability to access and conduct attacks in the downstream refinement operational environment. DYMALLOY and ALLANITE have demonstrated the capability to access and operate in the downstream operating environment but have yet to deploy any disruptive or destructive capabilities. Although Dragos has not observed DYMALLOY and ALLANITE deploying destructive attacks, VANADINITE has demonstrated the ability to access OT networks via remote access infrastructure.

MAJOR AREAS OF CONCERN FOR DOWNSTREAM

- Assets with Direct Access to the Internet.
- Dual-homed Asset between SCADA and IT Network.
- Networks lacking an ICS/OT DMZ.
- Networks lacking in ICS/OT Network Visibility.
- Lack of Multi-factor Authentication for Remote Access.
- Third-Party Equipment that is connected to OT Network without Restrictions.
- Shared and Unrestricted Vendor Remote Access.
- Limited Logging and Monitoring for ICS Systems.
- End of Life Operating Systems.
- The ability for a read-only User Able to Write Changes.
- Lack of USB/Removable Media Scanning.

RECOMMENDATIONS FOR DOWNSTREAM

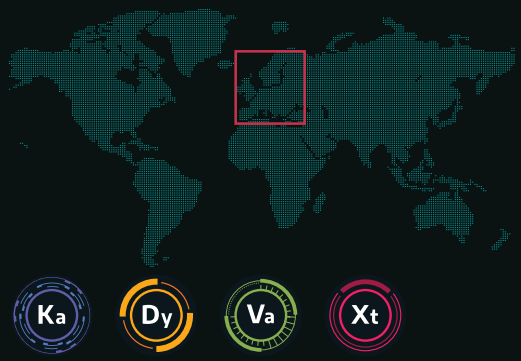
- Identify security zones and conduits based on security or process requirements. ISA 62443 Part 3-2 provides guidance on this process. The Purdue Model is an example of segmenting based on how close to a process a system is and is a good baseline.
- Implement a default “deny” access policy across the IT/DMZ/OT trust boundaries. This approach is like a firewall policy where everything is denied unless specifically allowed. This type of policy can be labor-intensive and requires more administration, working with vendors, operators, and application management to define the minimal set of allowed protocols and ports.
- 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.
- Place servers and data which both OT and corporate users need, in the DMZ. Access these resources in one direction only, rather than allowing a direct IT-OT connection.

REGIONAL ASSESSMENT

NORTH AMERICA

Of the fifteen adversary groups, seven adversaries target North American ONG entities. XENOTIME, KAMACITE, DYMALLOY, VANADINITE, and TALONITE remain the most concerning of adversary groups with CHRYSENE and PARISITE activities shifting to the Middle East and North Africa (MENA) region in 2020 and 2021. The threat landscape remains at a low frequency, high impact level of concern, with most disruptive incidents being derived from ransomware adversaries.

EUROPE



European oil and gas entities and operations represent a lucrative tar get for adversary groups targeting OT environments. The number of adversaries targeting OT environments is increasing; adversaries targeting oil and gas entities remain active and are increasingly evolving their behaviors. Of the fifteen adversary groups, six adversaries target European oil and gas entities. KAMACITE, DYMALLOY, and VANADINITE remain the most active and concerning adversaries for most European oil and gas entities. XENOTIME offensive cyber operations remain a concern for most oil and gas entities in Europe, but little activity has been observed from this adversary group since May 2020.

THE MIDDLE EAST AND NORTH AFRICA (MENA)

Of the fifteen adversary groups, seven adversaries target MENA ONG entities. The MENA threat landscape remains consistently active. There are periods of high activity focused on one geographic area (e.g., Israel, Lebanon, Tunisia, for example) and widespread activity focused mainly on general espionage. The seemingly apparent constant back and forth between Israel and Iran's disruptive cyber activity remains a concern for ONG operations, with possible further impacts on other MENA regions. Dragos recommends that ONG organizations operating in the region assess current local facility remote connections, joint venture connections, and local supply chain as potential avenues of access for regionally focused adversaries. Evidence suggests that CHRYSENE primarily targets Lebanese government entities, with most observed activity showing development in capabilities and specific emphasis on delivery and exfiltration payloads.

ASIA-PACIFIC

Of the fifteen adversary groups, three adversaries target Asia-Pacific ONG entities. The Asia-Pacific threat landscape focuses on adversaries targeting IT networks for espionage. VANADINITE and TALONITE have demonstrated an interest in conducting espionage-oriented offensive cyber operations. They typically target operational information sources. However, their interest could extend to OT environments and the proprietary or sensitive information located there. The Asia-Pacific region threat landscape will likely evolve as more visibility into OT environments grows in this region. It is worth noting that solar and wind generation is at risk in this region from STIBNITE and KAMACITE offensive cyber operations. Although direct ONG wind and solar facilities have not been impacted, they share a threat landscape with Energy Generation. It is worth including when scoping intelligence requirements for this region.

SOUTH AMERICA

Ransomware incidents have significantly impacted the South American threat landscape, and likely include some adversary groups from the North American region. The low visibility in South American oil and gas present multiple issues in assessing the complete South American ONG threat landscape. At higher risk for ONG in South America is most likely from Joint Venture partnerships. Dragos continues to monitor for emerging adversary groups in the South American region.

VULNERABILITIES

Adversaries targeting energy entities are known to quickly weaponize and exploit vulnerabilities in internet-facing services, including Remote Desktop Protocol (RDP), VPN services, and network infrastructure. This includes PARISITE, MAGNALLIUM, ALLANITE, XENOTIME, and VANADINITE. New vulnerabilities revealed throughout 2021 impact critical network infrastructure services, including F5, Palo Alto Networks, Citrix, and Juniper network devices, and are likely targets for adversaries. These vulnerabilities can enable adversaries to gain initial access to enterprise operations or pivot into industrial operational environments.

Vulnerabilities in ICS-specific devices and services can introduce risk to the manufacturing environment. As of December 2021, Dragos researchers assessed and validated 4256 vulnerabilities impacting industrial equipment found in energy environments. Dragos found that 2149 of these vulnerabilities could cause a loss of view and/or control within a compromised environment. Of the Dragos assessed vulnerabilities impacting industrial equipment found in the energy sector, 1447 vulnerabilities required an adversary to be on the network to exploit, and 104 required an adversary to be on the local host to exploit. Dragos recommends that asset owners and operators be aware of the threat these vulnerabilities pose to operations. A loss of view or control, for instance, may cause safety concerns and potentially put workers' lives or the operational environment at risk.

ANALYST NOTE: Dragos uses the industry classification established by the Cybersecurity and Infrastructure Security Agency (CISA) for industrial vulnerabilities. CISA reports vulnerabilities impacting ONG entities as part of the Energy Sector.

Exploiting ICS-specific vulnerabilities to create a specific, desired effect requires an understanding of the operations technology network, the device itself, and the logic or programming required to modify the device. An adversary likely requires less skill to leverage vulnerabilities for unspecific or disruptive purposes. Several adversary groups have demonstrated the ability to quickly implement vulnerabilities into their offensive cyber operations. However, it should be noted that relatively few have used ICS-specific vulnerabilities.

TOP 5 ATTACK SCENARIOS FOR GLOBAL OIL AND GAS

1 OT NETWORK REMOTE ACCESS EXPLOITATION

The COVID-19 pandemic has increased the need to evaluate remote work options, including ONG industrial environments such as processing and transportation operations that may not have previously leveraged widespread remote access options. Third-party vendor access to industrial processes also poses a potential risk for operators due to poor access restrictions, improper segmentation, and improper security controls.

Various ICS-targeting AGs – PARISITE, VANADINITE, TALONITE, DYMALLOY, and XENOTIME – have previously targeted or currently attempted to exploit remote access technology or logon infrastructure.

For example, PARISITE and TALONITE continue to perform password spray activity against remotely accessible logons as an initial access mechanism. This activity enables an adversary to use captured or very common passwords to brute force access. Criminal elements and known ransomware distributors use similar remote access brute force techniques to gain initial network access to complete network compromise. VANADINITE has also leveraged VPN device exploits to gain access to OT networks.

According to Dragos led architecture assessments unmonitored remote access and insecure vendor or third-party access is one of the most common problems at ONG facilities. The following issues were identified during engagements:

- Many third-party contractors and vendors performed logic updates and maintenance of Programmable Logic Controllers (PLCs) using their maintenance and engineering workstations. The contractors connect their laptops to a switch logically or physically shared with the PLC and Human Machine Interface (HMI) in the field location. The entity did not require contractors to verify that their laptops were free of malware before connecting to the OT network.
- Overly permissive configured “egress” Access-Control Lists (ACLs) could allow an adversary to execute code internally, calling home to their external infrastructure.
- Operators did not secure remote access to the SCADA network using MFA. This added layer of protection is essential to prevent an adversary from gaining access by compromising a user’s credentials.
- Vendors had remote access to operations environments via an account shared with multiple users. Additionally, they conducted Remote Terminal Unit (RTU) maintenance via shared accounts. Shared accounts prevent visibility into individual user actions and cannot be sufficiently audited for user accountability and non-repudiation for system actions. Also, using a common or shared password is in combination with shared accounts can allow adversaries to perform lateral movement within the OT environment.
- Operators had managed many connectivity devices were managed using insecure protocols with limited credential management. If critical connectivity nodes are not appropriately secured with access monitoring, critical communication paths providing vital control data could be eliminated and cause a forced shutdown.
- Multiple remote access and third-party compromise security solutions exist. Still, organizations must evaluate solutions and related infrastructure and ensure they are aware of and have mitigations prepared for security weaknesses.

2 DISRUPTIVE OR DESTRUCTIVE RANSOMWARE EVENT

Ransomware represents the second most likely scenario due to its prevalence on the threat landscape, low barrier of entry to implement, and ease of conducting mass targeting campaigns. While there are dedicated ransomware adversaries targeting larger organizations for larger payouts, most ransomware remains opportunistic attacks. However, it should be noted that PARISITE and related activities have incorporated ransomware into their attacks, mainly targeting Israeli facilities, including critical infrastructure.

Dragos does not attribute ransomware activities, per se but will acknowledge already publicly disclosed attribution to any ransomware group acting strategically or tactically on a nation's behalf. Ransomware capabilities are a concerning development as state-sanctioned or state sponsored adversaries implement them into offensive cyber operations as most likely a geopolitical signaling method with operational cover and monetary gain as a secondary intent.

3 OT CLOUD COMPROMISE

As more OT systems become internet-connected, the traditional OT focus on ensuring high availability with less regard for confidentiality and integrity has evolved. The digitalization of operational environments and cloud hosting creates an environment that has little visibility and allows adversaries methods of access to obtain data to enable offensive cyber operations without the normal oversight of a security operations center. This places a lot of trust on the cloud provider to either secure the cloud enclave with appropriate safeguards or effective monitoring with oversight from the asset owner and operators. As further cloud integration occurs in OT environments, especially for reliance on the availability of historian data and other critical monitoring systems, it increases the likelihood of an adversary gaining initial access, collect operational information, or manipulate data to generate a specific action or effect.

4 SUPPLY CHAIN

Supply chain compromise remains a significant threat to oil and gas operations. Supply chain compromise enables an adversary to bypass security mechanisms by exploiting trusted connections to a victim. The December 2020 SolarWinds Orion compromise discovery demonstrated the severity of supply chain threats. Dragos observed multiple SolarWinds compromises in North American industrial organizations, to include oil and gas companies.

SolarWinds software is often used in OT environments to monitor and manage site operations across Level 2 and Level 3 of the Purdue Model. This includes Engineering Workstation (EWS), SCADA or Distributed Control System (DCS) servers, and data historian devices and supporting infrastructure, such as Active Directory (AD) Domain Controllers (DC). An adversary could leverage a SolarWinds compromise to gain access to OT networks, elevate credentials on a compromised device, move laterally within the network, and conduct reconnaissance.

The full scope and impact of the SolarWinds compromises are currently unknown. Dragos is not aware of adversary access to an ICS environment. This is not surprising as customers often do not have the ability to see from a visibility or logging perspective if they have had adversary access.

However, previous attacks highlight the broad and often disruptive impacts of supply chain compromise. Examples of supply chain compromise impacting industrial operations include:

- The MeDoc accounting software compromise that led to the NotPetya malware attack. This malware masqueraded as ransomware and caused significant disruptive impacts globally.
- The infiltration of electronic data interchange (EDI) systems linked to oil and gas pipeline operations.
- Intrusions focused on enterprise resource planning providers (ERP) such as SAP and Oracle in 2018.
- REvil in July 2021, conducted a supply chain attack on Kaseya, an enterprise IT and MSP management solutions provider This attack, which leveraged a vulnerability in Kaseya's VSA software to upload a malicious software update, led to the delivery of REvil ransomware and the encryption of the Kaseya MSP's customers.

Additionally, XENOTIME has targeted original equipment manufacturers supporting numerous industrial sectors. Access to equipment vendors could enable additional compromise of customers' operations.

5 JOINT VENTURES

Joint Ventures provide adversaries an opportunity to obtain access to an ONG collaborative network that may have access to main partner networks. Depending on security controls, Joint Venture networks may allow an insider threat from the partner country or an adversary to obtain information or cause disruptions from lightly monitored sources or introduce additional methods to access proprietary information or other OT networks from the business network connection.

Dragos assesses that Joint Ventures are a risk center for organizations that share corporate and OT networks with other Joint Venture entities, especially if the corporate network is flat or does not have proper segmentation between the Joint Venture network and main partner network. Joint Venture network connections represent an avenue of continued access for adversaries to utilize as a trusted connection that may not be scrutinized or have appropriate protective measures due to the trust relationship, asset management, and inconsistent logging in Joint Venture networks. Dragos recommends segmenting Joint Venture networks from the main business network, strict access controls, and monitoring network activity and asset activity in and from Joint Venture Networks, if the host partner allows such security controls. If this is not possible, restrict access from the Joint Venture network to the main business network and monitor all network activity originating to and from the Joint Venture network.

RECOMMENDATIONS

DEFENSIBLE ARCHITECTURE RECOMMENDATIONS

Every OT environment requires a defensible architecture[1]. This reduces cyber risks from an architecture perspective and enables the human defender. A defensible environment is not a defended environment. It takes a human to turn something from defensible to defended but not all environments are defensible. Dragos recommends the following actions to develop a defensible network architecture.

- Install anti-virus/antimalware solutions on ICS workstations.
- Audit or scan systems, permissions, insecure software, insecure configurations, etc., 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 defense 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 DMZs 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 and 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.

MONITORING AND VISIBILITY RECOMMENDATIONS

Monitoring a network can come in many forms but in the focus of these controls it really is about helping maintain a defensible architecture and enabling a human defender to make it a defended environment. Improving – or, in many cases obtaining – visibility is crucial for identifying and defending against cyber threats. This includes long-term logging to investigate potential compromises as new information about incidents comes to light from intelligence sources. Dragos recommends the following steps to improve monitoring and visibility:

- Configure all capable devices and network components in the ICS/OT environment to send logging and monitoring data to a centralized system that is ICS/OT-aware.
- 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 centralized server.
- Utilize a supplemental ICS/OT-aware logging and monitoring system where possible to supplement the existing capabilities.

1 Dragos CEO on building a robust OT security programme - Dragos

- Coordinate the ICS/OT-aware logging and monitoring system with a 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 defense 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 like a firewall policy where everything is denied unless specifically allowed. This type of policy can be labor-intensive and requires more administration, working with vendors, operators, and application management to define the minimal set of allowed protocols and ports.

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 important to practicing these response plans and incorporate them into Tabletop Exercises (TTXs) to identify chokepoints or problems in the response plan. 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 alert or notification of an event has taken place. This allows recovery operations to account for resource requirements and acquisition of equipment if necessary.

REMOTE ACCESS AUTHENTICATION

Remote access, whether internal to the company (IT remoting into OT) or external (OEM/Integrator remoting into the OT) is a leading attack vector[2]. Currently, the most effective control MFA. Dragos recommends that MFA be implemented whenever possible. It is understandable that MFA is not always possible, however defensible architecture can compensate if MFA cannot be implemented.

- Establish remote connections that are made on request instead of always being accessible and monitor its usage for identifying misuse or exploitation.
- Any remote access into the OT network from internet-exposed VPNs or access portals should require MFA. 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.

2 Recommendations Following the Oldsmar Water Treatment Facility Cyber Attack - Dragos

KEY VULNERABILITY MANAGEMENT

Defenders should not assess all vulnerabilities with the same level of risk and priority for addressing in patch management practices. They should learn the effects that different vulnerabilities have and where adversaries need to be to exploit these vulnerabilities. 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 mitigating security controls.

- Unsupported Operating systems t are a high-risk asset. End of support means 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. This should not be used as an excuse or cause for not addressing the vulnerability, but in determining and ordering patching priority.
- Audit or scan systems, permissions, insecure software, insecure configurations, etc., to identify potential weaknesses and remediate as necessary.
- It is imperative to give field personnel, engineers, and other OT asset operators ICS/OT specific cyber security training, and to include them in security discussions, and awareness of security policies and procedures.
- Establish, document changes, practice and secure policies and procedures to assist in responding to and recovering from an OT-specific cyber event. This will also assist in identifying process or procedure operational gaps. Below is a list recommended, but not an exhaustive list of policies and procedures that should be common across ICS/OT environment security:
  - 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 procedure documented that defenders can follow to ensure consistency and compliance with the process.
  - Decommission/Disposal
    This policy primarily addresses ensuring that old equipment does not contain sensitive information before removing it from possession.
  - Change Management
    This policy aims to reduce security risks that arise from changing devices, software, or configurations through documentation, approvals, and notifications.
  - Device Hardening
    This policy aims to reduce security risks that arise from changing devices, software, or configurations through documentation, approvals, and notifications.

3 Understanding the Challenges of OT Vulnerability Management and How to Tackle Them - Dragos

- 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 would define 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.
- Vendor/Transient Device Policy
  This policy would establish expectations and treatment of vendor, third-party, or guest devices that can access OT networks.
- 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.
- 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.
- Data Retention
  A retention policy sets expectations for how long various logs will be kept. This can also expose weaknesses in current retention policies and enable actions to gain visibility and long-term historical data to identify malicious activity.
- 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.
- 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.

CONCLUSION

The cyber risk to ONG is increasing as the threat landscape continues to expand with the identification of new threat activities, ICS-specific ransomware, and remote and third-party services exploitation. Insufficient security policies and procedures in the operations environment enable adversaries to leverage these tactics on vulnerable ONG entities. However, numerous opportunities exist for asset owners and operators to improve cyber defense and implement simple, effective security policies and procedures to lower their cyber risk. Dragos continues to monitor adversary tactics, techniques and procedures (TTPs) and provides continuous updates to customers in the form of new indicators of compromise, knowledge pack updates, playbooks, and alerts to help owners and operators detect and respond to attacks based on adversary-based threat intelligence.

ABOUT DRAGOS, INC.

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.

TAGS:

Oil & Natural Gas, ONG, PARISITE, XENOTIME, DYMALLOY, ELECTRUM, CHRYSENE, HEXANE, KAMACITE, VANADINITE Upstream, Downstream, Midstream, Ransomware, Vulnerabilities