




Report


OIL & NATURAL GAS CYBER THREAT PERSPECTIVE

FOR THE GULF COOPERATIVE COUNCIL REGION

November 2021

DRAGOS, INC.

 intel@dragos.com

 [@DragosInc](https://twitter.com/DragosInc)

Summary

Dragos assesses with high confidence that adversaries pose a high risk of causing small-scale Operational Technology (OT) environment disruptions and with moderate confidence that adversaries could cause large-scale OT disruption within the Gulf Cooperative Council (GCC) region during the next year for the following reasons:

- An increase in the number of attacks against Oil and Natural Gas (ONG), including disruptive events that can occur at any stage within ONG operations (upstream, midstream, and downstream).
- The significant increase in ransomware attacks.
- The increased focus in state-sponsored cyber activity, and
- It's continued significance as a high value target.

Ransomware remains the preeminent threat to Information Technology (IT) and OT environments. Ransomware attacks can disrupt production if OT is not properly segmented from IT systems. These disruptions have led to significant financial loss, damage, and reputational damage in the region.

Dragos assesses that the biggest cybersecurity issues asset owners currently face are a lack of asset visibility into their network and weak network authentication controls. Without asset visibility organizations are unable to properly secure their OT environments because defenders cannot protect what they cannot see.

Industrial Control Systems (ICS) adversary groups (AG) that focus on ONG and the energy sector at large pose the most ICS cyber security risk to the GCC regional ONG industry. Important risks include: intrusions enabling intelligence gathering and data theft; and cyber events that align with the economic interests of hostile states that rely on the ONG vertical.

Key Findings

- The ICS security risk to GCC ONG sectors is high due to increasing, numerous intrusions into ICS networks for reconnaissance, research, and espionage, from nation states, as well as the criminal use of destructive malware or ransomware at ONG facilities in the region.
- ONG remains at the largest risk of any GCC sector for a destructive cyber-attack due to their political impact and highly volatile processes.
- 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 ONG entities.
- Activity Groups targeting original equipment manufacturers and third-party vendors pose a significant threat to ONG supply chains and these effects are possibly already present in GCC ONG facilities.
- GCC ONG entities should understand the behaviors and capabilities of Activity Groups targeting any OT systems, as these groups pursue a wide range of targets to expand their access into additional OT/ICS environments. They actively and specifically target internet-exposed assets, remote access, and insecure vendor or third-party access, introducing serious risk to the operations environment.
- Malicious state actors will increasingly target ONG and related industries to further political, economic, and national security goals, potentially causing disruptive or destructive events.
- The complete energy sector (ONG, electric, supply chains, etc.) and all of the GCC member countries are at risk. Companies and utilities face global adversaries as never before. Adversaries see cyberattacks as an increasing means of projecting power in the energy domain.

Activity Groups

The Activity Groups described here are most active in the ONG sector in the Gulf region.



PARISITE

PARISITE targets utilities, aerospace, and ONG entities. Its geographic target includes the GCC along with North America and Europe. 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.

Relevant Links: FoxKitten, Pioneer Kitten, MAGNALLIUM



XENOTIME

XENOTIME is known for its TRISIS attack which caused disruption at an ONG facility in the Kingdom of Saudi Arabia in August of 2017. It interacts with Triconex safety controllers and represents 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 Asia Pacific region; ONG companies in Europe, the U.S., and Australia; as well as devices beyond the Triconex controllers. In February 2020, Dragos learned of an incident at an ONG facility, outside the GCC, which had overlaps with XENOTIME but there was not enough data to attribute the activity to an Activity Group. This group also compromised several ICS vendors and manufacturers, providing a potential supply chain threat.^{1,2,3}

Relevant Links: Temp.Veles⁴



MAGNALLIUM

MAGNALLIUM initially targeted an aircraft holding company and ONG firms based in Saudi Arabia but expanded its targeting to include entities in Europe and North America. In the fall of 2019, following increasing tensions in the GCC, Dragos identified MAGNALLIUM expanding its targets to include electric utilities in the U.S, likely telegraphing the AG's desired geopolitical effects. MAGNALLIUM appears to lack an ICS-specific capability, and the group remains focused on initial IT intrusions.⁵ That said, Dragos has observed several events where IT focused Activity Groups gain access to OT due to a lack of proper segmentation, network misconfigurations, and open internet connections to OT environments. MAGNALLIUM has targeted energy and aerospace entities since at least 2013.

Relevant Links: APT 33, Elfin⁶

¹XENOTIME-Dragos

²TR-2020-06 Possible Turla Activity in the Oil and Gas Sector - Dragos

³TR-2019-23 TRISIS Malware Technical Report: Inject.bin Technical Report -

Dragos⁴ TEMP.Veles-MITREATT&CK

⁵MAGNALLIUM-Dragos

⁶APT33 - MITREATT&CK

Activity Groups



DYMALLOY

DYMALLOY's victims include electric utilities, ONG, and advanced industry entities in Turkey, Europe, and North America.⁷ It is a highly aggressive and capable activity group that can achieve long-term and persistent access to IT and operational environments for intelligence collection and possible future disruption events. In Q2 of 2021, Dragos identified this Activity Group expanding its targeting to include the APAC region based on newly identified malware samples. Though Dragos has not observed this AG in the GCC, several cross-border oil, gas, and product pipelines present a vector from neighboring countries and regions where Dragos has observed DYMALLOY.

Relevant Links: Dragonfly 2.0, Berserk Bear,⁸ Turla



ELECTRUM

Though this group focuses on electric utilities and mostly targets entities in Ukraine, we continue to monitor its activities, should they shift their focus to ONG and other regions. ELECTRUM was responsible for the disruptive CRASHOVERRIDE event in 2016.⁹ This group is capable of developing malware that can modify electric equipment processes, leveraging ICS protocols and communications. Dragos has not observed ELECTRUM in the GCC; however, this AG is included in this threat perspective for background information related to an example of Activity Groups prepositioning for later effects, outlined below.

Relevant Links: SANDWORM¹⁰



ALLANITE

We have not observed ALLANITE in the GCC region; however, it is included in this threat perspective based on the capabilities outlined below. ALLANITE targets business and ICS networks in the United States (U.S.) and UK electric utility sectors. The group performs reconnaissance in operational environments to potentially stage disruptive events. ALLANITE has demonstrated the capability to access and operate within the downstream OT environment. There is no indication that ALLANITE has a disruptive or damaging capability or intent as of late 2021.¹¹

Relevant Links: PALMETTO FUSION, Dragonfly 2.0¹², Berserk Bear

⁷ DYMALLOY – Dragos

⁸ Group: Dragonfly 2.0, Berserk Bear, DYMALLOY Berserk Bear – Dragos

⁹ Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE – Dragos

¹⁰ Sandworm Team - MITRE ATT&CK

¹¹ ALLANITE – Dragos

¹² Alert (TA17-293A) – Cybersecurity and Infrastructure Security Agency

Activity Groups



CHRYSENE

CHRYSENE emerged from an espionage campaign that first gained attention after the destructive Shamoon cyberattack in 2012 that impacted Saudi Aramco. The activity group targets petrochemical, ONG, and electric generation sectors. The Group has shifted its targets beyond its initial focus on the Gulf Region and the group remains active and evolved in more than one area.¹³

Relevant Links: APT34, GREENBUG, OilRig¹⁴



HEXANE

HEXANE targets ONG and telecommunications in the GCC, Africa, and Southwest Asia. Dragos identified this group in May of 2019. HEXANE drops malicious document files containing malware on victim machines, from which it can then proceed to further its goals in the target network.¹⁵

Relevant Links: CHRYSENE, OilRig



WASSONITE

Targets electric generation, nuclear energy, manufacturing, ONG and research entities in the GCC, India, and likely South Korea and Japan.¹⁶ WASSONITE relies on DTrack malware, credential capture tools, and system tools for lateral movement. WASSONITE has operated since at least 2018.

Relevant Links: Lazarus Group, COVELLITE



RASPITE

Targets electric utilities in the U.S. and government entities located in the GCC. Dragos also identified additional victims in Saudi Arabia, Japan, and Western Europe, but has not identified new RASPITE activity since mid-2018.¹⁷

Relevant Links: Leafminer¹⁸

¹³ CHRYSENE – Dragos

¹⁴ OilRig - MITRE ATT&CK

¹⁵ HEXANE – Dragos

¹⁶ TR-2021-07 WASSONITE Targets Oil and Gas, Electric, and Component Manufacturing Industry Entities with Backdoor and WASSONITE

Dragos

¹⁷ RASPITE - Dragos

¹⁸ Leafminer – Dragos

Threat Perspective

Overview of the Electric Sector

The electric system is complex, resilient, and interconnected. This interconnection model enables the safe and reliable flow of power within an interconnection and allows for some flow between interconnections through Direct Current (DC) tie lines. This design allows for power flows to occur through multiple paths within an interconnection and has frequency disturbances within an interconnection. The engineered approach provides redundancy, protection from complete collapse, and provides numerous benefits during emergency operations. However, while the system has been fairly resilient, the complexity has increased significantly and as result such interconnections and dependencies may reduce its resilience, which still remains largely untested in the phase of a determined cyber threat.

Electric utilities have processes in place to provide mutual aid to other entities if one experiences an event such as a storm, fire, or cyberattack that affects their service territories. Regional mutual assistance groups and industry partnerships can share resources and enable stabilization and reliability following disruptive or destructive events. Responding to real-time events, electric utilities have well-defined emergency operations procedures to control and position the electric system during degrading operational conditions that may include public appeals for reducing load, service interruptions, load shedding, and power system restoration actions.

Electric entities registered to perform specific reliability tasks in the U.S., Canada, and parts of Mexico must adhere to the North American Electric Reliability Corporation Critical Infrastructure Protection (NERC-CIP) cyber security standards and regulations. Globally, cybersecurity regulations or guidance vary, but many countries rely on International Electrotechnical Commission (IEC) and International Organization for Standardization (ISO) standards. The ISO and IEC Joint Technical Committee (JTC1) creates cybersecurity standards for Operational Technology (OT) equipment including nuclear power and electric power utilities. GCC electric entities and regulators often rely on NERC-CIP standards, which seem confusing and inconsistent due to the difference in asset owner's needs for products or service capabilities compared to other customer's subject to the same or different sets.¹⁹

The GCC Interconnection Authority (GCCIA) is a joint stock company subscribed to by the six (6) Gulf States and is subject to the same vulnerabilities as other utilities around the world. GCC electricity is a significant part of the future advancement of integrating into the Pan-Arab grid and potentially the synchronous grid of Continental Europe (also known as Continental Synchronous Area).

¹⁹ Standards Reports – NERC

Electric Power Operational Segments Threat Perspective

Fossil fuels, nuclear power, or renewables and other energy sources generate electric power at power generation facilities commonly referred to as power plants. The transmission system carries electricity across long distances from the plants to distribution substations and finally distribute it to customers. The transmission and distribution systems include substations where transformers are used to step-up or step-down voltage levels, to provide appropriate service delivery to industrial, commercial, and residential customers.

Generation

Threat Landscape

Dragos assesses that at least five AGs demonstrate the intent or capability to infiltrate or disrupt electric power generation. XENOTIME demonstrated the capability to access, operate, and conduct attacks in an industrial environment. Dragos assesses this group is capable of retooling and refocusing its disruptive efforts on electric utilities because it has already targeted Safety Instrumented Systems, like the Schneider Electric Triconex system, which is a mainstay in power generation. DYMALLOY demonstrated the ability to access OT networks in generation facilities and obtain screenshots of sensitive ICS data, including screenshots of Human Machine Interfaces (HMIs). ALLANITE is also a threat to generation because it shares some similarities in targeting and capabilities with DYMALLOY. Neither group has demonstrated ICS-disruptive or destructive capabilities as of now, and they continue their targeting for general reconnaissance purposes.

WASSONITE actively targeted critical infrastructure in Asia including nuclear power generation, and successfully deployed malware in the administration systems of at least one nuclear power plant. This is concerning, though no evidence suggests it successfully penetrated operations networks. While the AG is yet to display any ICS-specific capability or disruptive intent, actions to date indicate a sustained and continuing interest in these resources. Finally, STIBNITE was observed specifically targeting wind turbine companies that generate electric power in Azerbaijan. Based on current collection efforts, the activity appears confined exclusively to Azerbaijan. STIBNITE uses PoetrAT remote access malware in its intrusion operations to gather information, take screenshots, transfer files, and execute commands on victim systems. Also in this case, the activity mirrors observations in many of Dragos' AGs, where ICS intentions exist even if ICS-specific capabilities have not yet manifested.

Assessment

ICS-targeting adversaries have not successfully disrupted electric power generation. The observed activities targeting this segment, including obtaining documentation on sensitive operations networks, could be used for espionage purposes or to facilitate a disruptive attack.

Transmission

Threat Landscape

At least two AGs are a threat to transmission operations. ELECTRUM is a well-resourced AG with the capability to disrupt power transmission. Dragos assesses KAMACITE serves as an initial access and facilitation group for ELECTRUM.

ELECTRUM was responsible for the CRASHOVERRIDE malware attack in December 2016 in Kiev, Ukraine.²⁰ The adversaries tailored malware to de-energize a transmission-level substation by opening and closing numerous circuit breakers used in the delivery of power in the electric system and ensuring operator, power line, and equipment safety. The attack demonstrated a deep understanding of the transmission environment and industrial protocols in use, enabling the adversary to customize malware for the specific target.

Assessment

While this attack took place in Europe, it is possible for a similar cyberattack to occur in other parts of the world, with modifications for different industrial protocols, devices, and network topology found in a target environment. For example, the attack targeted breaker operations controlled by ABB devices adhering to the International Electrotechnical Commission (IEC) 61850 ²¹ standard and communicating using the Manufacturing Message Specification (MMS) protocol. However, Dragos assesses with moderate confidence the attack can be leveraged to other equipment that adheres to these standards.

Distribution

Threat Landscape

In the current threat landscape, one adversary group has disrupted electric distribution operations. KAMACITE operations enabled the first widespread cyberattack outage, which took place in Ukraine on 23 December 2015. The adversaries leveraged malware to gain remote access to three electric power distribution companies, performed system operations using the target environments distribution management systems, and disrupted electricity to approximately 230,000 people.²² The utilities fully restored power after a few hours through manual operations.

Assessment

Contrary to ELECTRUM, KAMACITE did not use ICS-specific malware in the 2015 Ukraine incident. It controlled operations remotely via existing tools in the operations environment. Adversaries can deploy KAMACITE and ELECTRUM tools globally depending on the adversary's focus.

Disrupting electric power at any point throughout generation, transmission, and distribution requires an adversary to have a fundamental understanding of the enterprise and operations environments; equipment used; and how to operate specialized equipment. Adversaries must spend an extended period of dwell time within the target environment learning the control system specifics to successfully deliver an attack that disrupts electric service, defenders have multiple points of opportunity along the potential attack chain to detect and eliminate adversary access.

²⁰ Crashoverride: Analysis of the Threat to Electric Grid Operations – Dragos
²¹ IEC 61850 Communication Protocol Manual - International Electrotechnical Commission

²² Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid – Wired

Interconnection and Power Exchange

The biggest threat to interconnections and power exchange is the potential manipulation of calculated power commitment to the power exchange via network compromise or social engineering attack. An electricity market, also power exchange or PEX, is a system enabling purchases, bids, and offers use supply and demand principles to set the price. Market operators or special-purpose independent entities with that specific function clear and settle wholesale transactions (bids and offers) in electricity. Market operators require knowledge of electricity trades to maintain generation and load balance.

Likewise, cyber adversaries must have a deep understanding of baseline power demands, potential generation, and forecasting procedures to successfully execute an attack; however, much of the information is readily available. Though this part of the energy sector is on the IT environment, attackers could gain access to the power exchange through a web application to manipulate the forecasting of excess electricity to commit to the GCCIA to create an effect within the OT environment.

Combined with careful power price manipulation, actors could create substantial economic effects to individual countries and the region.

Threat Perspective

Overview of the Water Sector

Natural renewable water resources are scarce within the GCC region, making water an especially sensitive resource. Limited rainfall and excessive consumption have depleted groundwater to unsustainable levels and every significant river and watershed within the GCC region is shared among two or more countries. As a result, water desalination is vital to acquiring potable water.

GCC countries host 43 percent of the world's total desalination plants (7,500 of 17,500) and account for about 70 percent of the global total production capacity for desalinated water. In Saudi Arabia, desalination accounts for over 70 percent of the potable water used in cities, and desalinated water has replaced groundwater as the primary source of drinking water throughout the country. The world's largest desalination plant is Ras al-Khair, located on the Persian Gulf coast of Saudi Arabia just north of Jubail.²³

Threat Landscape

Recognizing the criticality of water resources globally, but particularly in the GCC region, adversaries have shifted some of their focus to targeting Water and Wastewater Systems (WWS). Adversaries can use common TTPs to compromise IT and OT networks, systems, and devices at WWS facilities. They commonly use social engineering against WWS because human fallibility is a regular point of vulnerability within any organization. Furthermore, adversaries have consistently demonstrated the ability to bypass email filtering controls to successfully deliver malicious payloads. Adversaries have also taken advantage of systems that did not maintain the proper segmentation between corporate IT and OT networks to enable remote access. The use of remote desktop protocol

²³ Iran's Threat to Saudi Critical Infrastructure- Crisis Briefs

(RDP) to internet exposed services to remotely access WWS networks, including process control equipment is also an effective methodology cyber actors use.

WWS networks are further vulnerable to cyber disruptions or attacks due to the inclusion of unsupported or outdated operating systems, software, and Control System devices with vulnerable firmware versions. Outdated control system devices or firmware versions can expose WWS networks to publicly accessible, remotely executable vulnerabilities. Successful compromise of these devices may lead to loss of system control, denial of service, or loss of sensitive data. Several cyber intrusions from 2019 to early 2021 occurred against WWS facilities and serve as clear indicators of the potential threats to WWS globally. One example was the late April 2020 targeting of Israeli WWS facilities for process disruption. The attack was made possible due to externally exposed Programmable Logic Controller (PLCs) and similar devices, which had no authentication mechanisms in place. Attackers identified these systems, logged in remotely, and attempted changes to the process environment.²⁴

Threat Perspective

Overview of the ONG Sector

The ONG industry is a valuable target for adversaries and criminals exploiting ICS and IT environments for geopolitical reasons or financial remuneration. As the number of attacks against ICS overall increases, adversaries with specific interest in ONG companies remain active and continue to adjust their Tactics, Techniques and Procedures (TTPs). Disruptive cyberattacks against ONG facilities can occur at any point across the three major stages of ONG operations: upstream, midstream, or downstream. Adversaries will more easily execute attacks against ICS environments that cause operational disruptions or damage as Advanced Persistent Threat (APT) and criminal group capabilities improve.

The ONG industry is at considerable risk for ICS targeted destruction and disruption campaigns originating from cyberattacks due to the political and economic impact, and the direct effect on civilian lives and infrastructure, this page provides a summary of Dragos reports, vulnerability assessments, and other indicators affecting ONG entities and related industries globally.

Upstream

Threat Landscape

In the current threat landscape, Dragos has not observed an adversary demonstrating the intent or motivation to target upstream Exploration and Production operations. The most likely adversary with motivations to target GCC upstream and Production operations is XENOTIME. Of note, the greatest concern for upstream is cellular networks as this is an adversary's most effective and likely avenue to gain access to upstream operations, including the wellheads. HEXANE has demonstrated the capability to use Internet Service Provider (ISP) connections to access upstream ONG operations.

²⁴ AA-2021-22 Multiple U.S. Agencies Release a Joint Alert on Malicious Cyber Activity Targeting U.S. Water and Wastewater Systems - Dragos

Assessment

Dragos assesses with medium confidence that the ONG upstream segment threat environment is relatively small compared to other ONG segments. The most likely ICS/ Process Control Network (PCN) target in the upstream segment would focus on the production portion of upstream operations, though the potential for economic espionage is a far greater threat in the exploration enterprise network. The technology involved in Exploration and Production (E&P) would require adversaries to develop highly specialized capabilities to operate and interact in this ICS/PCN network environment, especially at Purdue Model levels 3 to 0.

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 ICSSystems
- Lack of Multi-factor Authentication for Remote Access

Midstream

Threat Landscape

In the current threat landscape, no adversary has demonstrated the intent, motivation, or capabilities to target midstream ICS/PCN environments. XENOTIME is the Adversary Group most likely to develop these capabilities.

Assessment

Dragos assesses with high confidence that the ONG midstream segment threat environment is an emerging threat landscape that will likely generate new activity groups into the future due to the critical role it plays between production and refinement. This assessment is partially based on the increased activity in state-sponsored espionage; however, the biggest threat indicator against the midstream segment is the significant increase in ransomware activity paired with the criticality of the midstream segment. Targeting against ICS/PCN in the midstream segment will likely focus on the transportation portion of midstream operations.

Major Areas of Concern for midstream:

- Lack of ICS/OT Network Visibility
- Dual-homed Assets between Supervisory Control and Data Acquisition (SCADA) and IT Network – Do not allow
- Limited Logging and Monitoring for ICSSystems
- Lack of Multi-factor Authentication for Remote Access
- End of Life Operating Systems
- Lack of Universal Serial Bus (USB) Scanning
- Insufficient Network Segmentation
- Shared Credentials
- Reused Local Administrator Password
- OT Endpoint Exempt from Security Policy

Downstream

Threat Landscape

In the current threat landscape, there are several adversaries that demonstrate the intent and motivation to target downstream environments, specifically in refinement. XENOTIME has demonstrated the capability to access,

operate, and conduct attacks in the downstream refinement operational area. DYMALLOY and ALLANITE have demonstrated the capability to access and operate in the downstream operational environment but have yet to deploy any attack capabilities. It should be noted that, although DYMALLOY and ALLANITE have yet to deploy attack capabilities, it is likely within these Adversary Groups' arsenals to deploy such capabilities.

Assessment

Dragos assesses with high confidence that the ONG downstream segment threat environment is the largest target currently for ONG. The most likely ICS/PCN target in the downstream segment will focus on refinement operations. The nature and role of refinement facilities make them high value targets for adversaries.

Major Areas of Concern for Downstream:

- SCADA-Assets with Direct Access to the internet
- Dual-homed Assets between SCADA and IT Network
- Lack of ICS/OT Network Visibility

Vulnerabilities to ONG Infrastructure

Adversary Groups 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 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 September 2021, Dragos researchers assessed and validated 3640 vulnerabilities impacting industrial equipment found in energy environments.

Dragos found that 1004 of these vulnerabilities could cause a loss of view and/or control within a compromised environment. Only 281 of these vulnerabilities that impact industrial equipment found in the energy sector required an adversary to be on the network to exploit them, and 71 required an adversary to be on the local host to exploit them. Dragos recommends asset owners and operators be aware of the threats these vulnerabilities pose to operations. A loss of view or control, for instance, may cause safety concerns and potentially put workers' lives or the environment at risk.

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

In late May 2019, Dragos identified multiple malicious document files all appearing to feature ONG-related themes with a potential emphasis on the GCC. Most of the documents were non-functional or referred to external resources no longer available. Reviewing the attack methodology and coding behind the attacks, Dragos is not certain at this time if the malicious documents recovered represent true adversary activity or penetration testing behavior.

Irrespective of this, Dragos provides the following analysis to both inform asset owners of the underlying behaviors found in these documents, and to provide an early warning in case these items represent initial access mechanisms for an unknown activity group.

Ransomware

Ransomware remains a preeminent threat to IT and OT environments. As mentioned previously, 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. Attacks that can disrupt production if OT is improperly segmented from the targeted IT systems. This can also lead to financial loss and reputational damage. 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. When OT is running on or connected to enterprise IT, ransomware can also interrupt operations.²⁵

On 07 May 2021 operations were temporarily halted at the Colonial Pipeline Company, as a precaution, due to a ransomware compromise incident that occurred on the IT side of Colonial Pipeline's network. The DarkSide ransomware group claimed responsibility for the compromise.^{26,27}

Intellectual Property Theft

Intellectual Property (IP) theft against global organizations facilitates economic espionage and poses a strategic threat to the global economy and sector stability. Industries and technologies associated with the energy sector, environmental protection, and advanced manufacturing are at greatest risk.²⁸ In addition to the data transfer associated with foreign direct investment and joint ventures, two primary methods of IP theft include cyberattacks and insider threats. Stolen data and the theft of intellectual property provides insights on how to impact or disrupt industrial operations.

Insider Threats

In 2009 the Night Dragon campaign involved covert cyberattacks on global oil, energy and petrochemical companies and individuals. The attackers used multiple attack methods including social engineering and operating system vulnerabilities to access proprietary operations and financial information.²⁹

In 2013, a former employee of two subsidiaries of General Electric ONG admitted to stealing physical copies of more than 3,700 files containing pictures, diagrams, and other information relating to tools and equipment that the company used in oil field exploration and providing them to a competitor.³⁰ In 2018, the U.S. Department of Justice arrested an employee of a U.S.-based petroleum company for allegedly stealing trade secrets related to a product worth more than \$1 billion to benefit a Chinese company.³¹

²⁵ TR-2021-10: Manufacturing Sector Ransomware Insights June-July - Dragos

²⁶ AA-2021-09 Colonial Pipeline Halts Operations Due to Ransomware - Dragos

²⁷ Ibid.

²⁸ 2018 Foreign Economic Espionage in Cyberspace - The National Counterintelligence and Security Center

²⁹ APT10 - OPERATION CLOUD HOPPER - BAE Systems

³⁰ Branch Man Pleads Guilty to Theft of Intellectual Property - United States Attorney's Office, Western District of Louisiana

³¹ Chinese National Charged With Committing Theft of Trade Secrets - United States Attorney's Office, Northern District of Oklahoma

Beyond IP theft, insider threats can also cause damaging consequences, including operational losses, environmental harm, reputational effects, and even physical destruction.

In 2018, the U.S. Department of Justice indicted two insiders working on behalf of the Chinese Ministry of State Security (MSS) for a decade-long IP theft campaign that included the theft or attempted theft of proprietary information related to ONG exploration, mining, and production technology.³²

Although this behavior can be difficult to detect, there are several steps an organization can take to prevent insider attacks, including ensuring robust segmentation across all levels of the Purdue Model and ensuring employee and contractor access is restricted to only items necessary to perform duties.

Third-Party and Supply Chain Compromises

Increasingly, adversaries target industries using a common and effective method of attack that is difficult to defend against: third-party compromise. This attack vector preys upon implicit trust between companies and suppliers or supporting entities. Organizations in energy, ONG, manufacturing, and logistics are especially at risk because of the variety of security zones and trust relationships.³³ Iranian cyber activity against the IT sector increased more than 3400% in 2021, compared to 2020, mainly targeting Israeli and United Arab Emirates. Though this targeting was against the IT sector, Iranian actors are using techniques to achieve their goals through indirect vectors.³⁴

XENOTIME is one ICS-targeting group that attempts to compromise vendors in the ONG and electric sectors, including original equipment manufacturers (OEMs) involved in electric generation and safety systems, hardware manufacturers, software suppliers, and integrators.³⁵ Additionally, ALLANITE and DYMALLOY operations have compromised vendors and contractors for subsequent phishing campaigns, while multiple AGs compromise websites a target is likely to visit, to enable exploitation.

Asset owners and business units should adopt a “zero trust,” or work toward a “trust and always verify,” mentality with vendors and supply chain managed devices that have direct access to OT environments or credentials to access OT environments from RDP or VPN connections. Zero Trust is a security concept which eliminates the concept of trust from an organization’s network architecture to prevent data breaches. This concept leverages network segmentation, prevents lateral movement, and simplifies user-access control at a frontline level.

Prepositioning for Later Effects

Any disruptive or destructive ICS cyberattack requires an adversary to complete a series of prior steps in the ICS Cyber Kill Chain to achieve their ultimate goal.³⁶

An intrusion into an IT or ICS environment may not immediately cause or indicate an effects portion of a cyberattack. Adversary dwell time – or the time spent within a target environment before executing an attack – can be months or years within ICS. In the case of CRASHOVERRIDE, based on available evidence and intelligence that Dragos gathered, ELECTRUM entered the target environment as early as January 2016, possibly through a phishing campaign.³⁷ The CRASHOVERRIDE attack, which occurred on 17 December 2016, required an intimate knowledge of the target environment to transition from an IT to OT network and a fundamental understanding of ICS communications protocols. Long dwell time can enable an adversary to gather intelligence and assess a victim

³² Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information – Dept. of Justice office of Public Affairs

³³ Supply Chain Threats to Industrial Control: Third-Party Compromise – Dragos

³⁴ Iranian targeting of IT sector on the rise – Microsoft

³⁵ Year in Review 2018 – Dragos

³⁶ The Industrial Control System Cyber Kill Chain – SANS

³⁷ Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE – Dragos

environment to tailor an attack appropriately, while also studying a target's defensive posture and potential for attack obfuscation.

Asset owners and operators should understand the evolution of adversary tradecraft and behavior. Utilizing ICS-specific threat intelligence can inform and guide proactive decision-making and ensure defense-in-depth methodologies are implemented across IT and OT. Identifying and alerting on threat behavior patterns in addition to indicators of compromise can help identify initial intrusion and reconnaissance activity before a disruptive attack occurs.

Digital Transformation

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 expanded connectivity increases risk and makes the IT environment a potential attack vector into the OT environment.

One example of this is wormable ransomware attacks that take advantage of Windows vulnerabilities to propagate throughout a network. WannaCry ransomware leveraged this method in 2017, and in a recent security advisory, Microsoft warned of a newly disclosed remote desktop services vulnerability that adversaries could use for a similar attack.³⁸

Microsoft has released patches for several critical flaws, but industrial processes like those in oil refining may limit an asset operator's ability to patch large-scale physical process systems quickly and safely. In addition, many ICS environments contain older versions of Windows operating systems on devices like human machine interfaces (HMIs), data historians, Open Platform Communications (OPC) servers, and interconnected hosts. Jump boxes are especially critical, as they may have exposure to corporate networks and could provide an OT entry point for wormable attacks.

In ICS, system reliability is crucial, and taking machines offline to receive patches means experiencing potential downtime and loss of production, and potentially, revenue. This balancing act often favors foregoing necessary security updates to keep operations up and running. But patches for some vulnerabilities, such as Common Vulnerabilities and Exposures (CVE), CVE-2019-0708, or MS17-010,³⁹ and patches for the remote desktop vulnerability and WannaCry, respectively, are all vital to apply.

Asset owners and operators should test vendors' released patches on test devices then patch production devices as soon as practicable.

Political and Economic Threats

Dragos does not attribute activity groups to individuals or states. However, Dragos recognizes the impacts and implications in state-associated operations against ICS entities, including GCC ONG as it relates to greater political or economic goals and events. Some of our activity groups are associated with state interests based on third-party intelligence assessments, which are noted below.

³⁸ Prevent a worm by updating Remote Desktop Services (CVE-2019-0708)–Microsoft

³⁹ Microsoft Security Bulletin MS17-010–Critical–Microsoft

RUSSIA

Russia remains a major antagonist in the European cyber threat landscape and is also interested in the GCC region and assets. Russian cyber operations align closely with Russian goals and sociopolitical events. Russia views its efforts in cyberspace as an ongoing conflict for dominance of the cyber realm.⁴⁰ This motivates Russian groups to be highly aggressive and to tolerate high risk in conducting their cyber operations. Russian cyber campaigns include the compromise of critical infrastructure for disruption and intelligence collection for future operations.

Intelligence Assessment

It is possible, or even likely, that Russia will continue its aggressive utilization of cyberspace as a key component in its national strategy to project its power abroad, gather intelligence, and conduct destructive and/or disruptive operations against ICS/ Supervisory Control and Data Acquisition (SCADA) for economic, political, or military gains. U.S. and European intelligence agencies have linked activity associated with DYMALLOY and ALLANITE to the Russian state.⁴¹ Additionally, third-party intelligence firms have associated some XENOTIME activity with Russia.⁴² It is likely that Russian cyber operations will operate like others and expand to multiple industry verticals including electric, ONG, and beyond.

IRAN

Iran uses increasingly sophisticated cyber techniques to conduct espionage. It is currently capable of causing localized, temporary disruptive effects, such as disrupting a large company's corporate networks for days to weeks. Adversaries associated with the Iranian government conducted data deletion attacks against dozens of Saudi governmental and private-sector networks in late 2016 and early 2017. However, Iran is also attempting to develop cyber capabilities that would enable attacks against critical infrastructure in the U.S. and allied countries.⁴³ Third-party intelligence associates some activity from RASPIITE, CHRYSENE, and MAGNALLIUM to Iranian interests.

Intelligence Assessment

Iran responded to the U.S. reinstatement of sanctions with low-level, regional attacks against Saudi Arabian oil production and refinement infrastructure, indicating a reluctance for direct engagement.⁴⁴ Dragos assesses with moderate confidence that Iran will increase low-level asymmetric information-gathering and disruptive cyber operations against ICS entities in Europe, the U.S., and the GCC.

Defensive Recommendations

Defensible Architecture

- Implement OT network segmentation.
- Conduct architecture reviews to identify all assets, connections, and communications between IT and OT networks. Identify Demilitarized Zones (DMZs) to restrict traffic between enclaves. Critically examine and limit connections between corporate and ICS networks to only known, required traffic.

⁴⁰ Russia's Approach to Cyber Warfare – CNA Analysis Solutions

⁴¹ Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors – Cybersecurity & Infrastructure Security Agency ⁴²

FireEye links Russia-owned lab to group behind Trisis - FireEye

⁴³ Worldwide Threat Assessment of the U.S. Intelligence Community – Senate Select Committee on Intelligence

⁴⁴ Iran dismisses possibility of conflict, says does not want war – Reuters

Monitoring

- Audit or scan systems, permissions, insecure software, insecure configurations, etc., to identify potential weaknesses and remediate as necessary.
- 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 becomes known from intelligence sources.
- Passively identify and monitor ICS network assets to identify critical assets, chokepoints, and external communications in the network.

Remote Access Authentication

- Limit access to resources such as file shares, remote access to systems, and unnecessary services over a network.

Key Vulnerability Management

- Ensure an understanding of network interdependencies and conduct Crown Jewel Analysis⁴⁵ to identify potential weaknesses that could disrupt business continuity.

ICS Incident Response Plan

- Leverage industrial-specific threat detection mechanisms to identify malware within OT and reinforce defense in-depth strategies at the network level, to provide defenders and analysts with more robust investigation capabilities.

Conclusion

The GCC industrial environment presents unique interdependencies on water, ONG, and power processes.

Industrial environments (OT/ICS networks and SCADA systems), such as gas pipelines, power transmission systems, transportation systems, and water distribution systems, consist of similar components. These components are vulnerable to attack through direct access through insider threats or poor physical security controls, close access through wireless cyber operations, and remote access. Poor design or configuration leaves environments open to cyber exploitation.

Industrial environments remain at risk for a disruptive – or potentially destructive – cyberattacks due to the political and economic impact such an event may cause. Due to the interconnectivity of electric systems that enable robust resilience and redundancy during disruptive events such as storms or earthquakes, the system in most developed areas would likely recover very quickly from a disruptive cyber event. A disruptive attack requires significant effort to achieve, as CRASHOVERRIDE demonstrated.

An adversary's requisite dwell time within a target environment provides defenders with numerous opportunities to identify and remove malicious activity. Dragos observed Enterprise-targeting activity enables the initial intrusion, intelligence collection, and lays the groundwork for an adversary to pivot for disruptive events. The growing threat of supply chain attacks and vendor compromises allows new avenues for AGs to compromise IT and OT environments alike.

Numerous opportunities exist for asset owners and operators to improve cyber defense and implement simple, effective controls, security policies, and procedures to lower their cyber risk. Dragos continues to monitor adversary 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 utilize adversary-based threat intelligence to detect and respond to attacks.

References

- XENOTIME – Dragos
- TR-2020-06 Possible Turla Activity in the Oil and Gas Sector - Dragos
- TR-2019-23 TRISIS Malware Technical Report: Injection Technical Report - Dragos
- Timberley – MITRE ATT&CK
- MAGNALLIUM – Dragos
- APT33 – MITRE ATT&CK
- DYMALLOY – Dragos
- Group: Dragonfly 2.0, Berserk Bear, DYMALLOY Berserk Bear - Dragos
- Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE – Dragos
- Sandworm Team - MITRE ATT&CK
- ALLENITE – Dragos
- Alert (TA17-293A) – Cybersecurity and Infrastructure Security Agency
- CHRYSENE – Dragos
- Oil Rig - MITRE ATT&CK
- HEXANE – Dragos
- TR-2021-07 WASSONITE Targets Oil and Gas, Electric, and Component Manufacturing Industry Entities with Backdoor and WASSONITE – Dragos
- RASPITE – Dragos
- Leaf miner – Dragos
- TR-2021-10: Manufacturing Sector Ransomware Insights June-July – Dragos
- AA-2021-09 Colonial Pipeline Halts Operations Due to Ransomware – Dragos
- 2018 Foreign Economic Espionage In Cyberspace – The National Counterintelligence and Security Center
- APT10 - OPERATION CLOUD HOPPER – BAE Systems
- Branch Man Pleads Guilty to Theft of Intellectual Property – United States Attorney's Office, Western District of Louisiana
- Chinese National Charged with Committing Theft of Trade Secrets – United States Attorney's Office, Northern District of Oklahoma
- Two Chinese Hackers Associated with the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information – Dept. of Justice Office of Public Affairs
- Supply Chain Threats to Industrial Control: Third-Party Compromise – Dragos
- Year in Review 2018 – Dragos
- The Industrial Control System Cyber Kill Chain – SANS
- Anatomy of an Attack: Detecting and Defeating CRASHOVERRIDE – Dragos
- Prevent a worm by updating Remote Desktop Services (CVE-2019-0708) – Microsoft
- Microsoft Security Bulletin MS17-010 – Critical – Microsoft
- Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors – Cybersecurity & Infrastructure Security Agency
- FireEye links Russia-owned lab to group behind Trinis – FireEye
- Worldwide Threat Assessment of the U.S. Intelligence Community – Senate Select Committee on Intelligence
- Iran dismisses possibility of conflict, says does not want war – Reuters
- Crown Jewels Analysis – MITRE