

Global Oil and Gas Cyber Threat Perspective

ASSESSING THE THREATS, RISKS, AND ACTIVITY GROUPS AFFECTING THE GLOBAL OIL AND GAS INDUSTRY

August 2019

Summary

The oil and gas industry is a valuable target for adversaries seeking to exploit industrial control systems (ICS) environments. As the number of attacks against ICS overall is increasing, adversaries with specific interest in oil and gas companies remain active and are evolving their behaviors. Dragos recently discovered a new activity group targeting this space, HEXANE, bringing the total number of ICS-targeting activity groups Dragos tracks to nine, five of which directly target oil and gas. Activity groups are discussed in detail in this report.

A disruption event from a cyberattack at an oil and gas facility can occur at any point across the three major stages of oil and gas operations: upstream, midstream, or downstream. From exploration and production to customer distribution, operational technology (OT) environments are in close proximity to information technology (IT) networks. As adversaries that target ICS environments improve their capabilities, they can more easily execute difficult attacks that cause operational disruptions or environmental damage. Due to the political and economic impact, and direct effect on civilian lives and infrastructure, the oil and gas industry has a high risk for ICS targeted destruction and disruption campaigns originating from a cyberattack.

This report provides a snapshot of the threat landscape as of August 2019 and is expected to change in the near future as adversaries and their behaviors evolve.

Key Findings

- The ICS security risk to global oil and gas is high and increasing, led by numerous intrusions into ICS networks for reconnaissance and research purposes, and adversary use of destructive malware at oil and gas facilities.
- Oil and gas remains at high risk for a destructive loss of life cyberattack due to its political and economic impact and highly volatile processes. Dragos assesses that state-associated actors will increasingly target oil and gas and related industries to further political, economic, and national security goals.
- One significant threat includes active supply chain compromises by activity groups targeting original equipment manufacturers, third-party vendors, and telecommunications providers.
- Oil and gas entities should understand the behaviors and capabilities of activity groups targeting electric utilities as these adversaries may shift or expand targeting to include additional energy sectors.
- Cybersecurity visibility in oil and gas operational environments remains severely lacking allowing intrusions to dwell longer and cyber root cause analysis after an incident to remain elusive.
- The complete "energy infrastructure" (oil and gas, electric, etc) of all countries are at risk and companies and utilities are facing global adversaries. Cyberattacks are an increasing means to project power in the energy domain. Traditional oil, natural gas, electric, and others can no longer be viewed as separate sectors to protect but rather as a single interconnected infrastructure.

Activity Groups Targeting Oil and Gas

Dragos tracks five activity groups¹ targeting oil and gas. There are no Activity Group naming convention standards—some are associated with malware while others refer to those deploying the malware or a specific campaign. Dragos does not speculate on the identity of Activity Groups and none should be implied.



XENOTIME caused the disruption at an oil and gas facility in the Kingdom of Saudi Arabia in August 2017 using the destructive TRISIS framework, specially tailored to interact with Triconex safety controllers. The TRISIS attack represented an escalation of ICS attacks due to its potential catastrophic capabilities and consequences. In 2018 XENOTIME activity expanded to include oil and gas companies in Europe, the US, Australia, and the Middle East; electric utilities in North America and the APAC region; as well as devices beyond the Triconex controllers. This group also compromised several ICS vendors and manufacturers, providing a potential supply chain threat.²

Associated Group: Temp.Veles³



MAGNALLIUM has targeted petrochemical and aerospace manufacturers since at least 2013. The activity group initially targeted an aircraft holding company and energy firms based in Saudi Arabia, but expanded their targeting to include entities in Europe and North America. MAGNALLIUM's capabilities appear to still lack an ICS-specific capability, and the group remains focused on initial IT intrusions.⁴

Associated Groups: APT 33, Elfin⁵



CHRYSENE developed from an espionage campaign that first gained attention after the destructive Shamoon cyberattack in 2012 that impacted Saudi Aramco. The activity group targets petrochemical, oil and gas, and electric generation sectors. Targeting has shifted beyond the group's initial focus on the Gulf Region and the group remains active and evolving in more than one area.⁶

Associated Groups: APT 34, GREENBUG, OilRig⁷

² https://dragos.com/resource/xenotime/

⁶ https://dragos.com/resource/chrysene/

¹ Dragos categorizes ICS-targeting activity into activity groups based on observable elements that include an adversary's methods of operation, infrastructure used to execute actions, and the targets they focus on. The goal, as defined by the Diamond Model of Intrusion Analysis, is to delineate an adversary by their observed actions, capabilities, and demonstrated impact- not implied or assumed intentions. These attributes combine to create a construct around which defensive plans can be built. At this time, two activity groups possess ICS-specific capabilities and tools to cause disruptive events: XENOTIME and ELECTRUM.

³ https://attack.mitre.org/groups/G0088/

⁴ https://dragos.com/resource/magnallium/

⁵ https://attack.mitre.org/groups/G0064/

⁷ https://attack.mitre.org/groups/G0049/



HEXANE targets oil and gas and telecommunications in Africa, the Middle East, and Southwest Asia. Dragos identified the group in May 2019. Dragos can only publicly share limited information about this newly-identified activity group at this time.⁸

Associated Groups: CHRYSENE, OilRig



DYMALLOY is a highly aggressive and capable activity group that has the ability to achieve long-term and persistent access to IT and operational environments for intelligence collection and possible future disruption events. The group's victims include electric utilities, oil and gas, and advanced industry entities in Turkey, Europe, and North America.⁹

Associated Groups: Dragonfly 2.0, Berserk Bear¹⁰

Threats to Energy Infrastructure

Oil and gas entities should realize that a threat to one ICS entity is a threat to all energy infrastructure. No longer are individual threats exclusive to oil and gas, electric, nuclear, or natural gas. As evidenced by XENOTIME's expansion from solely focusing on oil and gas to targeting electric utilities, individual verticals cannot ignore threats to other ICS entities if they are not specifically targeted because an adversary's interests and targeting can be highly variable.¹¹

Dragos observes a trend of threat proliferation among ICS-targeting adversaries. Cyberattacks on critical infrastructure are becoming easier to execute by governments investing in offensive cyber operations, and the tools and capabilities required to achieve a disruptive or destructive impact will become ubiquitous. A parallel can be drawn between traditional weapons proliferation including nuclear capabilities, and cyberattacks and weaponized malware or toolkits in the cyber realm. Additionally, the spread of commodity IT hardware and software into ICS networks increases the attack surface providing ingress opportunities via techniques familiar to the adversary.

Therefore, all energy-related entities should be familiar with malicious activity across the energy sectors.

Activity Groups Targeting Electric

Some of the activity groups Dragos tracks focus on electric utility; these related entities and do not currently demonstrate a specific interest in targeting oil and gas verticals. However, oil and gas and related energy firms should be aware of the below activity groups as their interests and targeting may shift to include not only

⁸ https://dragos.com/resource/hexane/

⁹ https://dragos.com/resource/dymalloy/

¹⁰ https://attack.mitre.org/groups/G0074/

¹¹ https://dragos.com/blog/industry-news/threat-proliferation-in-ics-cybersecurity-xenotime-now-targeting-electric-sector-in-addition-to-oil-and-gas/

organizations within these verticals, but verticals where oil and gas operate, including chemicals and lubricants and maritime.



ELECTRUM currently focuses on electric utilities and mostly targets entities in Ukraine. It is responsible for the disruptive CRASHOVERRIDE event in 2016.¹² Due to the overlap of vendor technologies and relationships in the supply chain with electric utilities, the potential for collateral impact in an electric-targeting event is a risk to oil and gas. Several ICS entities experienced this consequence in the 2017 NotPetya supply chain compromise that impacted companies worldwide. Intelligence firms determined the SANDWORM group was responsible for the NotPetya event, and Dragos assesses ELECTRUM is an offshoot of SANDWORM.¹³

Associated Group: SANDWORM¹⁴



RASPITE targets electric utilities in the US and government entities located in the Middle East. Dragos also identified additional victims in Saudi Arabia, Japan, and Western Europe, but has not identified new RASPITE activity since mid-2018. Although Dragos has not observed direct targeting of oil and gas firms, such entities experienced collateral impact from this group's watering hole activity, thus RASPITE remains a risk to oil and gas.¹⁵

Associated Group: Leafminer¹⁶



ALLANITE targets business and ICS networks in the US and UK electric utility sectors. The group maintains access to victims to understand the operational environment and to stage for potential disruptive events. There is no indication ALLANITE has a disruptive or damaging capability or intent at this time.¹⁷

Associated Groups: PALMETTO FUSION,¹⁸ Dragonfly 2.0, Berserk Bear



COVELLITE compromised networks associated with electric energy, primarily in Europe, East Asia, and North America. The group lacks an ICS-specific capability at this time. While technical activity linked to COVELLITE behaviors exist in the wild, there has been no evidence or indications this group remains active from an ICS-targeting perspective.¹⁹

Associated Group: Lazarus Group²⁰

17 https://dragos.com/resource/allanite/

¹² https://dragos.com/resource/anatomy-of-an-attack-detecting-and-defeating-crashoverride/

¹³ https://dragos.com/resource/electrum/

¹⁴ https://attack.mitre.org/groups/G0034

 ¹⁵ https://dragos.com/resource/raspite/
 ¹⁶ https://attack.mitre.org/groups/G0077/

¹⁸ https://www.us-cert.gov/ncas/alerts/TA17-293A

¹⁹ https://dragos.com/resource/covellite/

²⁰ https://attack.mitre.org/groups/G0032

Oil and Gas Operational Segments Threat Perspective

Upstream

Upstream ICS and process control network (PCN) operations are where exploration for oil and gas fields, drilling wells, and establishing production infrastructure occurs.²¹

THREAT LANDSCAPE

No observed adversary has demonstrated the intent or capability to target upstream exploration and production operations. The greatest concern for upstream compromise is through telecommunications, cellular networks, and satellite connections because it is an adversary's most effective likely avenue of gaining access to upstream operations, including wellheads and drilling operations.

ASSESSMENT

The oil and gas upstream segment threat environment is relatively small compared to other oil and gas segments. The most likely ICS/PCN target in the upstream segment will be focused 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.

Midstream

Midstream ICS/PCN operations provide the link between upstream production and downstream refining. Major midstream assets include field gathering systems, processing plants, pipelines, maritime transportation, rail transportation, and storage.²²

THREAT LANDSCAPE

In the current threat landscape, no adversary has demonstrated the intent, motivation, or capabilities to target midstream ICS/PCN environments. The adversary most likely able to develop these capabilities is XENOTIME. However, adversaries have conducted cyber operations targeting transport and business operations at oil and gas entities to an unknown extent – for instance, in April 2018, attackers targeted electronic data interchanges (EDI) at multiple US energy companies causing disruptions to business operations.²³

ASSESSMENT

The oil and gas midstream segment threat environment is an emerging attack surface. Dragos assesses with high confidence new activity groups will target midstream segments in the future due to its critical role between production and refining. The most likely ICS/PCN target in the midstream segment is the pipeline transportation portion of midstream operations. A secondary focus will also involve maritime and rail, although rail threats

²¹ https://www.investopedia.com/terms/u/upstream.asp

²² https://www.investopedia.com/terms/m/midstream.asp

²³ https://www.eenews.net/stories/1060078327

^{©2019} Dragos, Inc. All rights reserved. [Protected] Non-confidential content. July 29, 2019

will likely focus more on transfer processes to cause loss of containment, rather than the actual railway tanks themselves.

Downstream

Downstream ICS/PCN operations focus largely on refining crude oil and raw natural gas, but also includes consumer distribution.²⁴

THREAT LANDSCAPE

In the current threat landscape, several adversaries have demonstrated the intent and capability to target downstream environments, specifically in refining. XENOTIME has demonstrated the capability to access, operate, and conduct attacks in the downstream refining operational area. HEXANE, MAGNALLIUM, and CHRYSENE activity group operations have facilitated initial access in downstream IT network environments. At this time, these groups are not observed to have an ICS-specific disruptive capability but such activity could be a precursor to an attack on ICS operations.

ASSESSMENT

Dragos assesses with high confidence that the oil and gas downstream segment threat environment is currently the largest and most active at this time. The most likely ICS/PCN target in the downstream segment will be refining operations. The nature and role of refining facilities are a high value target for adversaries. This is due in part to centralization of operations and resources, technical complexity, presence of extensive ICS, and the increased possibility for damage or destruction from highly volatile processes.

Regional Assessment²⁵

North America

Of the nine activity groups, five target North American entities, including oil and gas focused groups XENOTIME, MAGNALLIUM, and DYMALLOY. In recent months, Dragos identified an increase in activity targeting North American entities by groups generally focused on oil and gas. Following recent increasing tensions between the US and Iran, Dragos identified MAGNALLIUM activity targeting US government and financial organizations as well as oil and gas companies attempting to gain access to computers at target organizations.²⁶ Dragos expects this activity to continue.

Dragos continues to track XENOTIME activity targeting North American oil and gas. XENOTIME activity enabling potential supply chain compromise could affect entities in this region. Compromising hardware and software ICS vendors poses a threat to all ICS entities regardless of region due to global production and distribution of ICS equipment.

²⁴ https://www.investopedia.com/terms/d/downstream.asp

²⁵ Dragos does not perform attribution on threats. However, when other third-parties perform attribution, especially government entities, we document this for others if it is of interest. It is our position that this style of attribution is not valuable from a network defense perspective and thus Dragos does not spend resources on performing this action internally.

²⁶ https://dragos.com/blog/industry-news/rising-cyber-escalation-between-us-iran-and-russia-ics-threats-and-response/

Trade disputes between the US and China will continue to affect oil markets and potentially disrupt demand for energy, according to the Organization of Petroleum Exporting Countries (OPEC).²⁷ Ongoing trade disputes could lead to an increase in cyber activity between disputing political interests. China continues to use cyber operations to support its strategic development goals and acquire foreign technology, including sensitive trade secrets and proprietary information.²⁸ In addition to territorial disputes over oil and natural gas drilling rights in the South China Sea,²⁹ China's Thirteenth Five-Year Plan³⁰ and Made in 2025³¹ plan both prioritize energy and technology initiatives, making the oil and gas sector a prime target for cyber operations.

It is possible due to upcoming 2020 federal elections in the US, state-backed adversaries who target critical infrastructure such as oil and gas or electric utilities may shift their focus to elections, as observed in previous election years.³²

In Canada, oil imports from Saudi Arabia continue to rise despite political tensions between the two countries that peaked in 2018. According to the CBC, Canada's imports from Saudi Arabia increased by 66% since 2014.³³ Dragos has tracked an increase in targeting focused on organizations based outside of Saudi Arabia that do business in the region. As demonstrated by attacks including SHAMOON3, which targeted Saudi Arabian and associated businesses in 2018, attacks focused on operations or businesses in a specific region can propagate across a company's global operations, producing potentially significant impacts worldwide.³⁴

Europe

Seven tracked activity groups have targeted entities in Europe, including XENOTIME, MAGNALLIUM, CHRYSENE, and DYMALLOY. Dragos recently identified a new MAGNALLIUM password spraying campaign attempting to gain initial network access, with targets including European oil and gas entities.³⁵

XENOTIME survey and reconnaissance activity is ongoing in this region. Additionally, XENOTIME activity enabling potential supply chain compromise could affect entities in this region. Compromised hardware and software ICS vendors poses a threat to all ICS entities regardless of the region due to global production and distribution of ICS equipment.

Russia remains the primary antagonist in the European cyber threat landscape. 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.³⁶ Russian cyber campaigns include the compromise of critical infrastructure for disruption and intelligence collection for future operations.

Dragos assesses 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 for economic, political, or military gains. US and European intelligence agencies have linked activity associated with DYMALLOY and ALLANITE to Russian state interests.³⁷ Additionally, third-party

²⁷ https://www.cnbc.com/2019/01/13/opec-secretary-general-worried-about-trade-war-effect-on-china-india.html

²⁸ https://www.dni.gov/files/NCSC/documents/news/20180724-economic-espionage-pub.pdf

²⁹ https://www.cfr.org/interactive/global-conflict-tracker/conflict/territorial-disputes-south-china-sea

³⁰ http://en.ndrc.gov.cn/newsrelease/201612/P020161207645765233498.pdf

³¹ https://www.cfr.org/backgrounder/made-china-2025-threat-global-trade

³² https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf

³³ https://www.cbc.ca/news/business/saudi-oil-imports-rise-canada-diplomacy-1.5096887

³⁴ https://www.symantec.com/blogs/threat-intelligence/shamoon-destructive-threat-re-emerges-new-sting-its-tail

³⁵ https://dragos.com/blog/industry-news/rising-cyber-escalation-between-us-iran-and-russia-ics-threats-and-response/

³⁶ https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf

³⁷ https://www.us-cert.gov/ncas/alerts/TA18-074A

intelligence firms have associated some XENOTIME related infrastructure with Russia.³⁸ At this time, the biggest threat to European oil and gas entities is XENOTIME.

Dragos assesses with moderate confidence activity targeting oil and gas entities in this region will increase. European elections occurred at the end of May. These are often a target of malicious cyber activity. It is possible ICS-targeting attackers temporarily shifted to focus on elections but will likely refocus on other areas of political or financial interest including the oil and gas vertical.

Middle East and North Africa (MENA)

Attackers targeting oil and gas are among the most active and disruptive in the MENA region. The TRISIS attack on an oil and gas facility in Saudi Arabia represented an escalation of attacks due to targeting safety systems designed to protect human life. Previous disruptive events in the region targeted IT including SHAMOON and SHAMOON 2 malware attacks.³⁹ Additionally, military conflict and fraught political relationships contribute to an active cyber threat landscape.

Five activity groups Dragos tracks have targeted this region, specifically focusing on oil and gas and related entities: XENOTIME, CHRYSENE, MAGNALLIUM, RASPITE, and HEXANE.

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. Third-party intelligence has associated some activity from RASPITE, CHRYSENE, and MAGNALLIUM to Iranian interests. Additionally, Iran responded to US reinstatement of sanctions with low-level, regional attacks against Saudi Arabian oil production and refining infrastructure, indicating a reluctance for direct engagement.⁴⁰

In recent months, oil and gas companies doing business in the Middle East with operations outside of the region have become targets of oil and gas adversaries. This trend is exemplified by attacks using variations of SHAMOON malware. The first wave of SHAMOON attacks in 2012 targeted energy companies affiliated with or owned by Saudi Arabia. In 2016, targeting expanded significantly to cover at least 15 Saudi government agencies as well as organizations and joint ventures associated with Saudi Aramco.⁴¹ SHAMOON3 in December 2018 was significantly different in that all publicly-known victims represented foreign oil and gas services or contracting companies, such as Saipem (Italy) and Petrofac (UK).⁴²

HEXANE's activity targeting telecommunications providers in Africa and the greater Middle East is concerning and highlights the increasingly common tactic of attacking third-party service providers in an effort to compromise the target victim from activity groups including XENOTIME. By compromising devices, firmware, or telecommunications networks used by targets within ICS, malicious activity could potentially enter the victim environment through a trusted vendor, bypassing much of the entity's security stack.

Non-governmental organizations affiliated with the oil and gas sector are also a target for ICS-focused adversaries. For instance, OPEC has a major influence on global oil prices, international relations, and

³⁸ https://www.cyberscoop.com/trisis-russia-fireeye/

³⁹ https://unit42.paloaltonetworks.com/unit42-shamoon-2-return-disttrack-wiper/

⁴⁰https://www.reuters.com/article/us-usa-iran-zarif/iran-dismisses-possibility-of-conflict-says-does-not-want-war-idUSKCN1S009C

⁴¹ https://www.reuters.com/article/us-cyber-saudi-shamoon-targets/shamoon-virus-returns-in-saudi-computer-attacks-after-four-year-hiatusidUSKBN13Q4AX

⁴² https://www.upstreamonline.com/live/1658948/petrofac-suffers-it-breach ; https://www.eenews.net/stories/1060109525

information sharing between the world's largest oil and gas producers, thus making it a valuable target for reconnaissance operations.

Dragos assesses with moderate confidence ICS-targeting activity in this region will continue information gathering activities targeting oil and gas, potentially establishing access for ICS attack development and execution.

Asia-Pacific

At this time, Dragos has identified XENOTIME and HEXANE targeting the Asia-Pacific region. Dragos assesses with moderate confidence oil and gas targeting will increase in this region.

Significant oil and gas industry growth is expected across the APAC region. According to reports, Australia's liquified natural gas (LNG) industry is worth \$50 billion. LNG exports from the APAC region increased 21% in the 2019 fiscal year and the area is the world's second-largest exporter of the product.⁴³ An October 2018 report from research firm Wood Mackenzie suggests the APAC oil and gas sector overall is rebounding, led by increased demand, new projects in the region, and more mergers and acquisitions.⁴⁴ This growth opens up new areas of opportunity for attackers both in terms of attack surface as well as information gathering for business and government intelligence purposes. At this time Dragos has not identified activity leveraging a disruptive ICS capability in the region, but it is likely information gathering targeting ICS entities will continue to occur.

Latin America

Dragos does not track any adversaries targeting Latin America at this time. The Latin American region heavily relies on oil and gas production and exportation to as a significant portion of its GDP, especially in Venezuela, Brazil, and Colombia.⁴⁵ The reliance on one industry for economic sustainability makes it an interesting target for adversaries interested in destabilizing the region. However, at this time cybercrime is the biggest threat facing this region and it is generally not relevant to ICS. It is possible that political hacktivists will target and attempt to disrupt oil and gas organizations as political unrest continues in the region; but, physical and traditional activism means remain a more cost effective means of disruption in these environments and cyber should be considered only a low confidence possibility.

Top 5 Attack Scenarios for Global Oil and Gas

1. Destructive Event Causing Loss of Life

It is now demonstrable that an adversary can compromise a safety system via cyber means producing a loss of safety. In the TRISIS attack, XENOTIME made an error that caused the Schneider Electric Triconex Safety Instrumented System (SIS) to fail. The system failed safe as expected, but due to the adversary not achieving their goal. If TRISIS succeeded, the attack could have resulted in severe operator injury or likely

⁴³ https://www.australianmining.com.au/news/australias-Ing-industry-now-a-50-billion-earner/

⁴⁴ https://www.woodmac.com/press-releases/new-wave-of-growth-on-the-horizon-for-asia-pacifics-oil-and-gas-sector/

⁴⁵ https://www.opec.org/opec_web/en/about_us/171.htm

^{©2019} Dragos, Inc. All rights reserved. [Protected] Non-confidential content. July 29, 2019

loss of life. Dragos anticipates activity groups will continue to target safety systems for disruptive or destructive purposes.

2. Third-Party and Original Equipment Manufacturer (OEM) Compromises

Vendors and third-party contractors provide essential services in performing upstream, midstream, and downstream operations, but with these critical functions comes unintended security risks that adversaries are more than willing to exploit to achieve their objectives.

Adversaries are increasingly utilizing third-party and original equipment manufacturer (OEM) compromise as a method for compromising intended targets. The adversary utilizes this attack vector to prey upon the implicit trust between companies and suppliers or supporting entities. Organizations in energy, oil and gas, manufacturing, and logistics are especially at risk because of the variety of security zones and trust relationships. The information gained from OEM compromises gives the adversary valuable insight into crafting OEM-specific capabilities.

Another attack vector exploited by adversaries is managed service provider (MSP) compromise. Similar to but more extensive than vendor or contractor access, MSPs will typically be embedded within and maintain extensive remote access to client networks. Thus, a breach at an MSP entity can lead to near-direct access to multiple victim networks if undetected. The most extensive operation publicly disclosed was the series of intrusions into MSPs conducted by state-sponsored adversaries, linked in other resources to APT10, announced by the US-CERT in 2018.⁴⁶

3. IT Malware Bridges OT Gap, Disrupting Operations

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 is wormable ransomware attacks that take advantage of Windows vulnerabilities to propagate throughout a network. WannaCry ransomware leveraged this method in 2017 which affected various ICS operations, and in a recent security advisory, Microsoft warned a newly-disclosed remote desktop services vulnerability could be used for a similar attack.⁴⁷ Commodity malware making the leap into operations can affect a variety of operational elements from enterprise business management logistics disruptions to potential plant shutdowns.

4. Electric-Targeting Operational Disruption Enablement

Due to the oil and gas industry's reliance on the electric transmission and distribution across upstream, downstream, and midstream operations, an attacker may compromise a source of electric power generation or distribution used to target an oil and gas entity. An attacker could launch a cyberattack against the electric entity which could disrupt oil and gas production. The symbiotic relationship between the two verticals means all energy sector companies need to be aware of energy-focused threats and activity groups even if the specific industry is not a current target.

⁴⁶ https://www.us-cert.gov/ncas/alerts/TA18-276B

©2019 Dragos, Inc. All rights reserved. [Protected] Non-confidential content. July 29, 2019

⁴⁷https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/

5. Adversary Access Through Cellular or Satellite Connections

As demonstrated by HEXANE activity, telecommunications networks are valuable targets for ICS-targeting attackers. Gaining access to a mobile or satellite network could allow an adversary to interact with upstream and midstream operations that utilize cellular devices or satellite connections for communication, monitoring, and management. Geographically dispersed and remote operations – such as pipeline compressor stations and offshore oil wells – often depend on cellular or satellite communication networks. Cellular and satellite network bridges into OT environments need to be closely monitored.

Defensive Recommendations

Asset owners and operators can implement the following host and network based recommendations to improve detection and defense against ICS-targeting groups.

- <u>VISIBILITY</u> A comprehensive approach for visibility into ICS/OT environments should be taken to ensure that there is not a visibility gap. Asset owners and security personnel should work together to gather network and host-based logs starting from the most critical infrastructure. The ability to identify and correlate suspicious network, host, and operational events can greatly assist in either identifying intrusions as they occur, or facilitate root-cause analysis after a disruptive event. Ensure network monitoring of the ICS through ICS-focused technologies.
- <u>SEGMENT</u> Where possible, segment and isolate networks to limit adversary lateral movement capabilities. While physically difficult in existing environments, modern networking hardware may enable asset owners and operators to virtually segment networks to reduce attack surface and limit adversary mobility.
- <u>ACCESSIBILITY</u> Identify and categorize ingress and egress routes into control system networks. This
 includes engineer and administrator remote access portals, but also covers items such as business
 intelligence and licensing server links that need to access IT resources or the wider internet. Limit these
 types of connections, including firewall rule directionality, to ensure a minimized exposed attack
 surface.
- <u>PUBLIC DATA</u> Assess asset owner hosted, publicly posted information and data that, when aggregated, would generate sensitive information that could be utilized by an adversary. Work with vendors, contractors, and other parties – either informally or through formal requirements in contracts – to minimize or prevent identification of specific sites, capabilities, or equipment in marketing or related material.
- <u>CONFIGURATION</u> Identify and store "known good" configuration information for ICS devices in nonnetwork accessible locations to provide baselines for comparison as well as restore points in the event of disruption. Update these items frequently to ensure such storage mirrors production environments. This action not only assists recovery in the event of IT malware propagating into ICS networks, but also facilitates analysis in TRISIS-like events by providing baselines to compare potentially manipulated configurations against.
- <u>DEFENSE-IN-DEPTH</u> Design and implement defense-in-depth surrounding ICS networks where security controls and enhanced visibility are applied to hosts capable of handling such tasks. Examples include requiring remote access to flow through a jump-host featuring enhanced Windows and network logging to ensure adequate monitoring of remote access to the control system network.

- <u>CONSEQUENCE-DRIVEN</u> Identify and prioritize critical assets and connections, and process consequences of cyberattacks.⁴⁸ Perform threat assessments to scope the most impactful risk of disruptive or destructive attacks and use such data to shape threat hunting and defensive postures.
- <u>THIRD-PARTIES</u> Ensure that third-party connections and ICS interactions are monitored and logged, from a "Trust, but Verify" mindset. Where possible, isolate or create distinct enclaves for such access to ensure that third-party access does not result in complete, unfettered, or unmonitored access to the entire ICS network. Implement features such as jump-hosts, bastions, and secure remote authentication schema wherever possible.
- NETWORK INFRASTRUCTURE ALLANITE and DYMALLOY regularly target routers and switches during compromises, changing configurations to allow for persistent access or delivery of additional malware. Implement router, switch, and firewall configuration review to ensure adversaries do not tamper with configurations and locate security gaps.
- <u>THREAT INTELLIGENCE</u> Use and operationalize ICS-specific threat intelligence. Threat intelligence can
 enable identification of known threat behaviors. The Dragos Platform incorporates intelligence-driven
 threat behavior analytics,⁴⁹ automating identification of known attacker behaviors. Dragos WorldView
 Threat Intelligence provides up-to-date intelligence feeds, reports, analysis, and defensive
 recommendations for new and ongoing threats to oil and gas.
- <u>RESPONSE PLANS</u> Develop, review, and practice cyber attack response plans and integrate cyber investigations into root-cause analysis for all events. Especially consider intelligent adversaries which may also attack plans during remediation and response to increase disruption scale and downtime.

Conclusion

The diverse global oil and gas threat landscape represents a significant concern for asset owners and operators at upstream, midstream, and downstream operations. Oil and gas remains at risk for a destructive cyberattack due to its political and economic impact and highly volatile processes. Additionally, non-OT environment business units that interact with these operations are also at risk for cyberattacks targeting the industry, as seen in the various rounds of SHAMOON disruptive activity in the Middle East.

While the majority of activity groups currently targeting oil and gas do not demonstrate ICS-specific disruptive or destructive capabilities, XENOTIME is a dangerous activity group that has exhibited destructive and damaging behaviors. The enterprise-targeting activity observed by Dragos enables initial intrusion and data gathering, and lays the groundwork for an attacker to pivot to potentially disruptive events. Additionally, the growing threat of supply chain attacks and vendor compromises allows new avenues for activity groups to compromise IT and OT environments alike.

Dragos assesses with moderate confidence that the first major cyber-related ICS event causing major process and equipment destruction or loss of life will occur in the oil and gas sector. It is imperative that private companies, quasi-government organizations, regulatory organizations, and governments work together to strengthen the security and safety of these industrial processes and installations to reduce the harm of such attacks which will undoubtedly occur sometime in the future.

⁴⁸ https://dragos.com/resource/dependency-modeling-for-identifying-cybersecurity-crown-jewels-in-an-ics-environment/

⁴⁹ https://dragos.com/blog/industry-news/threat-analytics-and-activity-groups/

^{©2019} Dragos, Inc. All rights reserved. [Protected] Non-confidential content. July 29, 2019