



2019

YEAR IN REVIEW

**THE ICS LANDSCAPE
AND THREAT ACTIVITY
GROUPS**

CONTENT

EXECUTIVE SUMMARY	4
.....	
2019 KEY FINDINGS	5
.....	
INTRODUCTION	6
.....	
RECOMMENDATIONS	6
UNDERSTAND AND ANTICIPATE THREAT PROLIFERATION	6
EFFECTIVELY OPERATIONALIZE THREAT INTELLIGENCE	7
CONDUCT OSINT ASSESSMENTS	7
PRIORITIZE DEFENSE TO “CROWN JEWELS”	7
DEPLOY ICS-SPECIFIC MONITORING AND THREAT DETECTION	7
.....	
THE HUMAN AND SAFETY COMPONENT	8
.....	
THREATS IN DETAIL	9
PROLIFERATION OF THREATS	10
DISRUPTIVE MALWARE, RANSOMWARE, AND SABOTAGE	12
THIRD-PARTY AND SUPPLY CHAIN TARGETING	14
VULNERABILITIES IN REMOTE ACCESS SERVICES	15
COMMON TACTICS REMAIN EFFECTIVE	18
ICS-SPECIFIC TACTICS GROWING	20

CONTENT

THREAT ACTIVITY GROUPS	21
HEXANE	22
PARISITE	24
MAGNALLIUM	26
WASSONITE	28
XENOTIME	30
DYMALLOY	32
ALLANITE	34
CHRYSENE	36
RASPITE	38
ELECTRUM	40
COVELLITE	43
.....	
CONCLUSION	44
.....	
APPENDIX	45
.....	

EXECUTIVE

SUMMARY

THE AMOUNT OF ACTIVITY TARGETING INDUSTRIAL CONTROL SYSTEMS (ICS) INCREASED SIGNIFICANTLY IN 2019.

Despite no publicly reported destructive attacks, ICS network intrusion and disruption persists, and the associated cyber risk continues to grow and remains at a high level.

DRAGOS IDENTIFIED THREE NEW TARGETED ACTIVITY GROUPS, BRINGING THE TOTAL NUMBER OF ACTIVITY GROUPS TARGETING ICS ENTITIES TO 11.

The growing threat landscape affirms previous Dragos assessments: as the community achieves greater visibility into the industrial threat landscape through increased visibility, threat hunting, ICS-specific threat detection, and rising industrial cybersecurity investment, we will continue to identify new adversaries and gain a better understanding of the behaviors, tradecraft, and threats to ICS environments.

Dragos identified three new activity groups targeting ICS: HEXANE, PARISITE, and WASSONITE. Dragos also identified an evolution of tracked adversary behavior including MAGNALLIUM expanding its targeting to include North American electric entities and developing

and deploying new wiper malware against Middle East oil and gas operations. Additionally, XENOTIME began targeting electric utilities and expanding targeting to North America and the Asia Pacific region and obtaining access to documentation that could inform disruptive attacks.

Furthermore, ransomware and other malware infections continue to be a major issue across industrial operations. LockerGoga malware disrupted operations at the Norwegian aluminum manufacturer Norsk Hydro, becoming the most high-profile disruptive ICS event of the year. Additionally, Emotet malware, Ryuk ransomware, and related infections caused business disruptions to multiple industrial and related entities. Although not specifically targeted to ICS, such attacks demonstrate how commodity malware, sometimes limited to IT networks only, impacts operations especially when there is interconnectivity on the operations technology (OT) networks that is not fully understood, documented, or hardened.

2019

KEY FINDINGS

- » In 2019, Dragos identified three new activity groups targeting ICS entities globally increasing the total count to 11 activity groups.¹
- » Threat proliferation contributed greatly to increased risk as entities expanded targeting and capabilities. This includes an increased focus on ICS organizations, specifically in critical infrastructure across the United States and APAC.²
- » Third-party and supply chain threats are increasing, including threats to telecommunications, managed service providers, and backbone internet service providers.³
- » Ransomware and commodity malware – like Ryuk and Emotet – remain threats to industrial operations. Such malware can potentially bridge the IT/OT gap to disrupt operations.⁴
- » Common tactics such as phishing, password spraying, and watering holes remain popular and effective as initial access vectors into industrial organizations.
- » Adversaries are increasingly targeting remote connectivity such as virtual private networks (VPNs), vendor and business management integrations, remote desktop connections, and managed service providers.
- » Escalating geopolitical tensions increase the chance that offensive cyber effects operations against ICS will be employed more regularly putting critical infrastructure and human life at higher risk.^{5 6}

RECOMMENDATIONS

Dragos recommends implementing a risk-based and ICS-specific cybersecurity program, which may leverage existing engineering and corporate resources.



Such a program should evaluate the potential impact of an ICS-disruptive cybersecurity incident and include ICS-specific monitoring, threat detection, and response. Traditional, and even modern, information technology (IT) enterprise approaches are insufficient to defend an industrial environment. The following defensive recommendations can help asset owners and operators move beyond basic security best practices and defend against increasingly capable adversaries targeting industrial networks. Such a program should evaluate the potential impact of an ICS-disruptive cybersecurity incident and include ICS-specific monitoring, threat detection, and response. Traditional, and even modern, information technology (IT) enterprise approaches are insufficient to defend an industrial environment.

UNDERSTAND AND ANTICIPATE THREAT PROLIFERATION

Due to the increasing proliferation of threats, asset owners and operators across all industries must be aware of threats to ICS. As evidenced by XENOTIME and MAGNALLIUM, activity groups that historically target one vertical can expand their focus at any time.

ICS-SPECIFIC THREAT INTELLIGENCE CAN PROVIDE COMPREHENSIVE INFORMATION ABOUT ADVERSARY BEHAVIORS AND TARGETING THAT CAN HELP INFORM PROACTIVE DEFENSE.

This can ensure asset owners and operators proactively defend against threats to critical infrastructure before they become a potential target.

EFFECTIVELY OPERATIONALIZE THREAT INTELLIGENCE

Threat intelligence can inform operations beyond cybersecurity. Knowledge about adversaries' tactics, techniques, and procedures (TTPs) can inform business continuity and remediation plans in the event of a cyberattack. Such information can help business and risk decision making – threat intelligence should be delivered to technical practitioners, but also operation and strategic business managers to understand risk tolerance. Effectively operationalizing and communicating threat intelligence⁷ by delivering appropriate messaging about threats to critical infrastructure can ensure a company-wide understanding of an enterprise's position within the threat landscape. The more organizations know about the threat surface, threat landscape, and their internal environments can enable a better understanding how adversaries are going to interact with them.

CONDUCT OSINT ASSESSMENTS

Dragos has observed adversaries including XENOTIME accessing publicly available data that support disruptive attacks. Asset owners and operators are encouraged to conduct regular open source intelligence (OSINT) assessments. Users should identify and limit information available about vendors and partners; documents, schematics, and data sheets; job advertisements; and credentials in public dumps. Security teams should also identify gaps in security architecture such as remote login portals that lack strong passwords and multi-factor authentication. Additionally, users should proactively identify scanning or automated information scraping activity and implement mechanisms to prevent automation such as requiring CAPTCHA or an email address to download public documentation. Ensure all employees limit exposure of sensitive information, such as employment data on LinkedIn, that could facilitate targeting operations.

PRIORITIZE DEFENSE TO “CROWN JEWELS”

An attacker looking to achieve specific objectives will target an organization's crown jewels, or the highest-valued assets that, if compromised, could cause major impact to the organization. Asset owners and operators should identify such assets and implement a risk-based approach that can accurately scope ICS security controls, tailored threat hunting, and regular security assessments. Dragos created the Crown Jewel Analysis Model⁸ to help asset owners and operators effectively understand and implement ICS cybersecurity strategies.

DESPITE OFTEN CONTAINING SIMILAR TECHNOLOGIES, IT AND OT ARE FUNDAMENTALLY DIFFERENT ENVIRONMENTS AND REQUIRE TWO DIFFERENT DEFENSE AND RESPONSE PLANS.

As a result, Dragos advises asset owners and operators implement and invest in ICS-specific threat detection and response.

DEPLOY ICS-SPECIFIC MONITORING AND THREAT DETECTION

Every year this becomes more and more evident. If you don't see it, you can't respond to it. If you don't know you have it, you don't know how to protect it. These are the basic axioms of monitoring and detection forming the basis of any defensible environment. ICS environments provide unique assets, configurations, processes, data, protocols, and many other distinctive characteristics that significantly hamper traditional IT enterprise products from performing effectively. It is insufficient to use an “IT” approach to achieve ICS defensibility.

Asset owners and operators should monitor for potentially malicious behaviors within the ICS, such as monitoring for callouts to the internet or internet-routable IP addresses, new account creation, new devices on the network, and configuration changes outside of change windows.

THE HUMAN AND

SAFETY COMPONENT

As geopolitical tensions continue to increase, Dragos anticipates a corresponding increase in cybersecurity activity directed towards critical infrastructure and industrial entities.

Following escalatory messages over the summer between the United States, Saudi Arabia, and Iran, Dragos identified an uptick in malicious activity against ICS.⁹ Indeed, Dragos first identified MAGNALLIUM targeting electric utilities between July and August 2019, coinciding with heightened tensions in the Middle East.

Dragos anticipates ICS-targeting activities will continue, and that such activities can put human life at risk.

ANY ILLICIT ACCESS INTO CIVILIAN
INFRASTRUCTURE, LIKE ELECTRIC
POWER OR MANUFACTURING,
UNACCEPTABLY PLACES INNOCENT
HUMAN LIVES AT RISK.

Policy makers worldwide must establish a red line disallowing all forces, military or otherwise, from operating within civilian industrial networks to ensure civilian safety.



THREATS

IN DETAIL

Threats to ICS are increasing in sophistication and number. In 2019, through intelligence gathering, information sharing, and incident response engagements, Dragos identified a variety of new and ongoing threats to ICS. The following are the most concerning to Dragos.



PROLIFERATION OF THREATS

Cyber threats to ICS are proliferating as adversaries increasingly invest money, time, and talent into the ability to disrupt critical infrastructure. Such targets include oil and gas, electric power, and water.

Disruptive or destructive attacks on critical infrastructure require significant resources, which are increasing across the board as capabilities and targeting expand. The proliferation of cyber threats to ICS can be illustrated by the activity groups XENOTIME and MAGNALLIUM.

In 2019, Dragos identified a change in behavior for XENOTIME, the activity group behind the destructive TRISIS malware. While working with clients across various utilities and regions, Dragos identified a persistent pattern of activity attempting to gather information and enumerate network resources associated with US and Asia-Pacific electric utilities.¹⁰ XENOTIME expanded its probing activity to include electric utilities, using the same techniques previously deployed against oil and gas entities. Additionally, as identified in previous Dragos reporting, XENOTIME has targeted, and in some cases successfully compromised, original equipment

manufacturers (OEMs), potentially impacting the entire industrial supply chain.¹¹

Also this year, Dragos identified MAGNALLIUM beginning to target electric, financial, and government entities in North America. This behavior coincided with an escalation of political and geographic tensions in the Middle East over the summer.¹² The activity demonstrated an expansion of the behavior for the group previously focused on oil and gas entities, largely in or relating to operations in the Middle East.

THE GROUP USED THE SAME INITIAL ACCESS ATTEMPT TECHNIQUES EXHIBITED IN PREVIOUS CAMPAIGNS AGAINST ENERGY COMPANIES, NAMELY PASSWORD-SPRAYING AND PHISHING, IN AN EFFORT TO GAIN A FOOT-HOLD WITHIN COMPANIES.

It is important to note this behavior is not a shift – rather it is an expansion of targeting for two groups historically focused on the oil and gas sector. This means that all ICS entities must be aware of malicious activity and adversary behaviors across industrial sectors as interest and targeting from any group could change.



RECOMMENDED SECURITY IMPROVEMENT

Leverage ICS-specific threat intelligence to become knowledgeable about adversary TTPs across all industrial sectors to prepare for potential shifts in targeting.

DISRUPTIVE MALWARE, RANSOMWARE, AND SABOTAGE

DRAGOS HAS IDENTIFIED AN UPTICK IN MALWARE INFECTIONS, PARTICULARLY RANSOMWARE, AT INDUSTRIAL COMPANIES GLOBALLY. LIKE IN 2018, DISRUPTIVE IT MALWARE WAS AGAIN A THREAT TO ICS ENTITIES IN 2019.

This year the major malware families and events included LockerGoga, Emotet, and Ryuk infections. Additionally, Dragos identified an increase in new IT-based wiper malware activity targeting industrial entities in the Middle East. Dragos has also responded to ransomware events impacting ICS environments, underscoring the potential threat to operations from IT-focused malware if it breaches IT/OT boundaries.

LockerGoga ransomware family first appeared in an incident at French engineering company Altran Technologies in January 2019.¹³ In addition to two US-based chemical manufacturers likely impacted in early March 2019, the most notable impact was to Norway-based Norsk Hydro on 19 March 2019. The crippling event resulted in prolonged and costly operational impacts.¹⁴

The LockerGoga variant likely used at Hydro encrypted all files outside the Windows directory, instead of just files with typical document extensions. The Hydro variant also implemented various changes to make restoration difficult, if not impossible. Thus, Dragos classified LockerGoga as a destructive malware type used for sabotage instead of mere ransomware. Superficially, this is similar to the NotPetya

ransomware event from June 2017, where malware appearing to be ransomware actually resulted in system loss due to the inability to recover files.¹⁵

Emotet first appeared toward the end of 2018, infecting multiple ICS-related entities. Throughout 2019, it continued to affect businesses, with a brief drop-off over the summer.¹⁶ Emotet is a modular trojan commonly observed deploying Trickbot and Ryuk malware. In February 2019, Emotet malware infected a deep draft vessel bound for the Port of New York and New Jersey which impacted their shipboard network (though no essential control systems were impacted) according to the US Coast Guard.¹⁷ Ryuk affected multiple organizations associated with the aviation industry. According to publicly available data and information shared with Dragos, attackers used Ryuk in events involving a US



airport, US airline, Canadian supply chain company, and a Europe-based aviation industry supplier. Additionally, Mitsubishi Canada Aerospace experienced a Ryuk ransomware attack beginning on March 19 and lasting “weeks,” according to local media.¹⁸ Ryuk also impacted an unspecified marine facility, disrupting its camera and physical access control systems, as well as causing a loss of critical process control monitoring systems, according to a December bulletin from the US Coast Guard.¹⁹

In June, UK’s National Cyber Security Centre (NCSC) warned of ongoing Ryuk ransomware campaigns targeting global organizations. Then in October, the Australian Signals Directorate’s Australian Cyber Security Centre (ACSC) released an advisory on a widespread malicious email campaign to spread Emotet malware in Australia. The Australian government received dozens of reports of confirmed Emotet infections in sectors including critical infrastructure providers and government agencies. The ACSC said it was aware of at least 19 Emotet infections in Australia, some of which deployed the Trickbot malware.²⁰

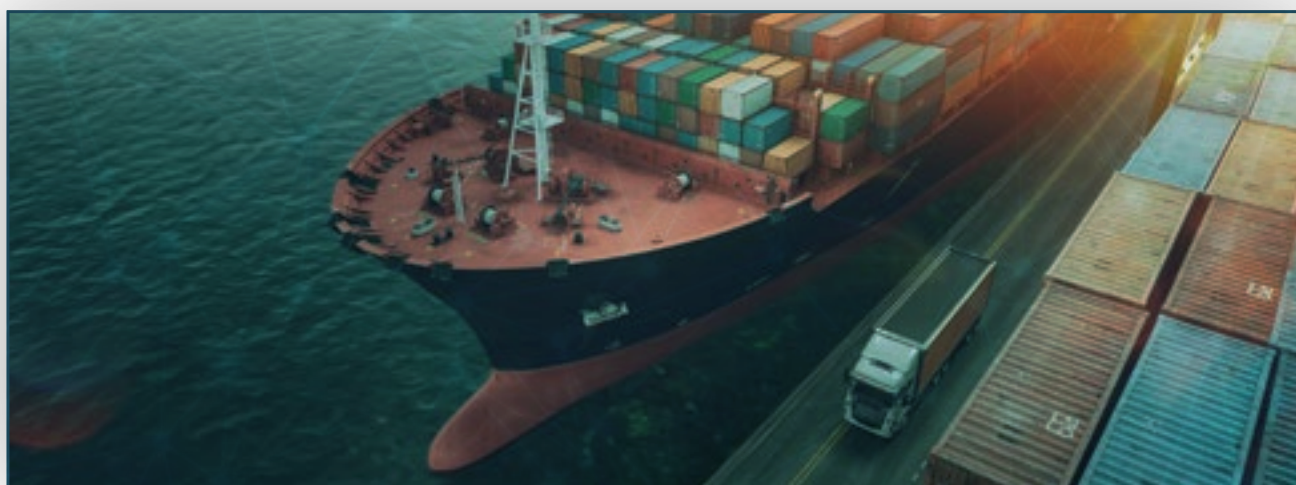
Numerous other malware events disrupted ICS entities in 2019. In July, a ransomware attack on the IT systems at Johannesburg, South Africa’s City Power prevented prepaid electricity purchase via online systems, and prevented customers who had previously bought power to load it to their meter boxes;²¹ in September, Rheinmetall Automotive experienced an unnamed malware attack that disrupted some production processes;²² also that month, a cyber event disrupted production and

distribution at Danish health device manufacturer Demant;²³ BitPaymer ransomware impacted order fulfillment and delivery at the automation firm Pilz in October;²⁴ and oil company Petroleos Mexicanos experienced a ransomware attack in November that disrupted the company’s administration, business, billing, and supply chain operations.²⁵

Government and intelligence organizations frequently publish detailed information on threats to businesses and citizens alike, providing some valuable visibility into threat trends in various countries. However, such releases provide a limited view of malicious activity. Dragos performed incident response cases against a number of IT-focused malware infections at industrial organizations, including a Sodinokibi ransomware infection at an ICS entity that disabled multiple systems required for control of the affected plant. Such events often go unreported in the public sphere, thus Dragos’ incident response capabilities and intelligence collection generate additional insights into threat trends like disruptive ransomware.

2019 also saw two new IT-based wiper malware strains targeting energy entities in the Middle East. Dragos discovered KILLGRAVE malware associated with operations against the oil and gas industry in the UAE in July 2019, with likely links to the MAGNALLIUM activity group. Additionally, in December, IBM released public details on a wiper called ZeroCleave targeting unspecified industrial and energy environments in the Middle East.²⁶ Dragos continues to observe evidence of ZeroCleave use and related variants in the wild.

THE MALWARE AND RANSOMWARE INCIDENTS LARGELY TARGET ENTERPRISE NETWORKS. HOWEVER, LIKE DRAGOS HAS OBSERVED MULTIPLE TIMES, INCIDENTAL INFECTIONS WITHIN THE OT DUE TO POORLY SEGMENTED OR MISCONFIGURED NETWORKS, OR INFECTIONS DISRUPTING IT SOFTWARE OR SERVICES REQUIRED FOR OPERATIONS – LIKE DATA, FLEET, OR PRODUCTION MANAGEMENT SOFTWARE – CAN HAVE OPERATIONALLY DISRUPTIVE EFFECTS.



THIRD-PARTY AND SUPPLY CHAIN TARGETING

AS IN 2018, SUPPLY CHAIN THREATS WERE A KEY ISSUE FOR ICS ENTITIES THIS YEAR. IN 2019, NEW THREATS EMERGED AFFECTING TELECOMMUNICATIONS, MANAGED SERVICE PROVIDERS (MSPS), AND BACKBONE INTERNET SERVICE PROVIDERS.

Dragos identified the new activity group HEX-ANE targeting telecommunications entities in addition to oil and gas in Africa, the Middle East, and Southwest Asia. Additionally, Microsoft²⁷ and security firm Cybereason²⁸ published reports on threat actors targeting telecommunications providers globally.

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, or solar or wind farms – often depend on cellular or satellite communication networks. Dragos observed ICS-specific targeting via

telecommunications networks indicating activity corresponding to initial access attempts, or Stage 1 of the ICS Cyber Kill Chain, trying to bridge to Stage 2 capabilities or access.²⁹

In April, media reporting indicated business process and information technology outsourcing firm Wipro, which provides services for various ICS verticals, allegedly suffered a breach of corporate systems.³⁰ Adversaries then used this access to launch follow-on attacks against Wipro clients. Although not directly involved in industrial operations, Wipro products and services – such as the company's Promax offering – are often tied to industrial processes for data collection, processing, and analysis.³¹ The breach was one of multiple third-party service provider attacks Dragos and other entities have identified since 2017, highlighted in Dragos' 2018 Year in Review reporting.³²

External parties routinely have access to operations, and thus it presents an issue where third-party access bypasses corporate IT. Multiple related services surrounding ICS operations – from managing corporate IT through performing data collection and analysis on industrial processes – rely on trusted third parties deeply integrated into the organization's operations.



RECOMMENDED SECURITY IMPROVEMENT

Manage third-party connections through policy and technical controls including ICS-specific threat detection, visibility, and response to counter both insider and external threats posed by these connections.

In April, Cisco Talos revealed a sophisticated DNS hijacking campaign called Sea Turtle.³³ It targeted 40 organizations in 13 countries, primarily national security organizations in the Middle East and North Africa, and compromised victims included “prominent energy organizations.” The goal of the campaign was to steal credentials to access the primary victims’ networks. The attacks began as early as January 2017 and continued through this year.

DNS hijacking is an attack method that could be used to steal sensitive data and obtain legitimate encryption certificates for a target’s domain names by compromising DNS resolution to funnel traffic to a DNS server generally operated by the

attacker. In this campaign, attackers compromised third-party entities including DNS registries, internet service providers (ISPs), and organizations affiliated with DNS infrastructure support to control the targets’ DNS records. DNS hijacking can be a useful technique to gain initial access to any network, including industrial organizations.

AN ADVERSARY EXPLOITING TECHNOLOGIES FUNDAMENTAL TO INTERNET CONNECTIVITY AND GLOBAL COMMUNICATION IS SIGNIFICANTLY CONCERNING.

VULNERABILITIES IN REMOTE ACCESS SERVICES

VULNERABILITIES PUBLISHED THIS YEAR FOR MICROSOFT'S REMOTE DESKTOP SERVICES AS WELL AS THREE VIRTUAL PRIVATE NETWORK (VPN) PROVIDERS COULD ALLOW AN ATTACKER TO LEVERAGE VULNERABLE REMOTE LOGIN PORTALS FOR INITIAL ACCESS.

Indeed, Dragos has identified at least one ICS-targeting activity group targeting vulnerable VPN appliances, and security researchers identified active exploitation of the Windows vulnerability. In 2019, Dragos also responded to cyber events in which adversaries used RDP connections as a means to obtain initial access.

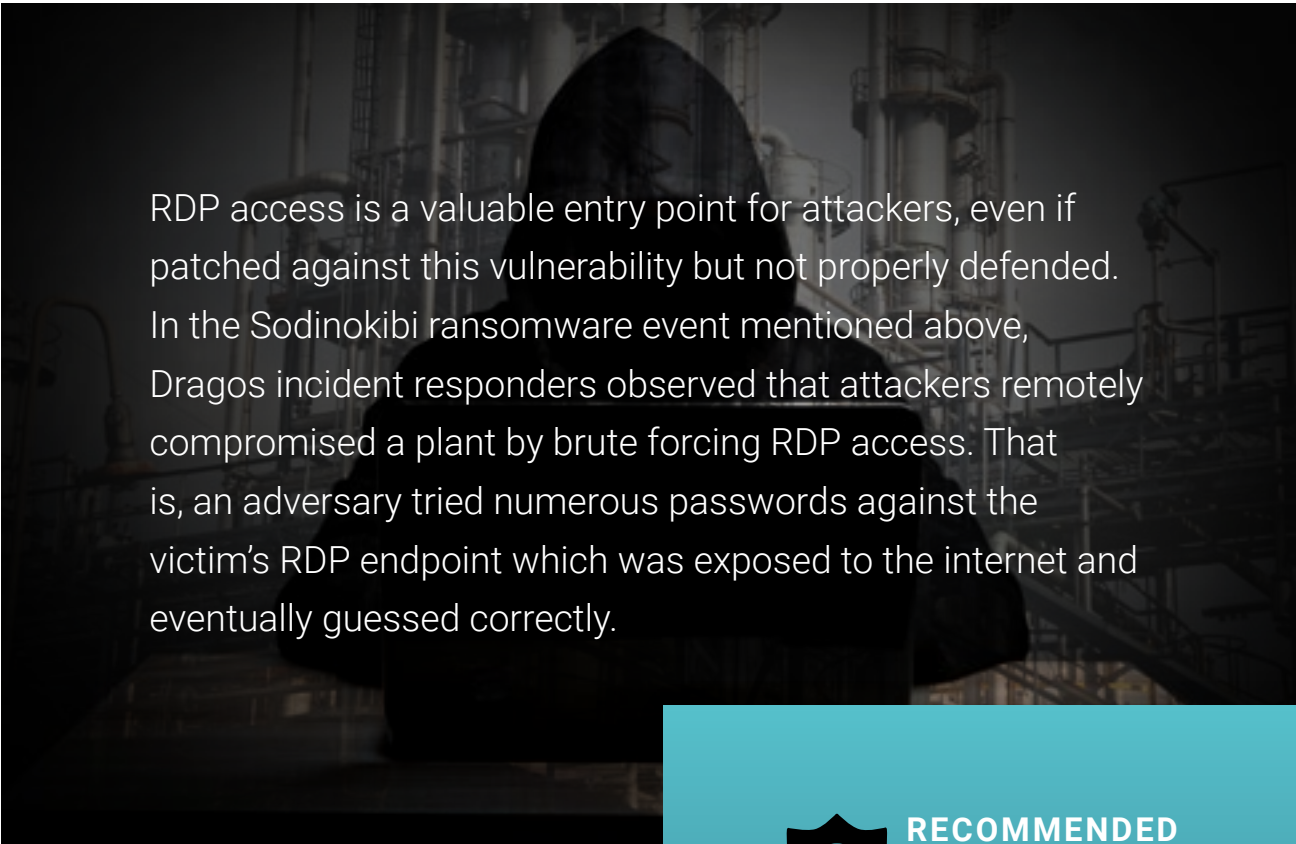
In May, Microsoft published an advisory detailing a critical vulnerability in Remote Desktop Services which could allow an attacker to send a specially crafted packet to a target system via RDP and achieve control of the system.³⁴ The vulnerability is known as "BlueKeep" or CVE-2019-0708 and affects Windows 7, Windows Server 2008 R2, Windows Server 2008, Windows 2003 and Windows XP. If an attacker utilizes

the flaw to deliver malware to a target workstation, it is possible for the malware to propagate throughout the target network in a wormable fashion. Microsoft said in its initial advisory the vulnerability could enable a malware outbreak similar to the WannaCry attacks in 2017.

In November, researchers revealed attackers actively exploiting vulnerability to

install cryptocurrency mining malware on victim machines.³⁵ This is a relatively low impact exploitation of the vulnerability considering the scale and scope of potential consequences. It is likely attackers will continue to exploit this vulnerability, with potentially more disruptive effects. The RDP vulnerability is concerning to ICS asset owners and operators. ICS environments often contain older versions of Windows operating systems on devices including human machine interfaces (HMIs), data historians, and OPC servers. It is especially concerning for DMZ jump hosts, which may have exposure to corporate networks and would be the initial ICS entry point for any future worm which uses this vulnerability.





RDP access is a valuable entry point for attackers, even if patched against this vulnerability but not properly defended. In the Sodinokibi ransomware event mentioned above, Dragos incident responders observed that attackers remotely compromised a plant by brute forcing RDP access. That is, an adversary tried numerous passwords against the victim's RDP endpoint which was exposed to the internet and eventually guessed correctly.

Adversaries are also targeting vulnerable VPN appliances for initial access to target networks. Dragos identified PARISITE targeting known vulnerabilities in Pulse Secure Pulse Connect Secure (CVE-2019-11510),³⁶ Palo Alto Networks GlobalProtect Portal (CVE-2019-1579),³⁷ and Fortinet FortiOS (CVE-2018-13379)³⁸ VPN applications. Dragos identified that the identified activity began as early as April 2019. The exploited vulnerabilities could allow remote attackers to take control of a vulnerable system. Details of the vulnerabilities were published earlier this year, and government intelligence agencies previously said multiple adversaries are actively exploiting the vulnerabilities worldwide.³⁹

VPN gateways are common targets for adversaries as they can provide outside access to internal networks and may lack some security protection mechanisms prevalent inside a perimeter. Third-party services often use VPNs to connect with customers for things like business or maintenance purposes thus making them a valuable target for adversaries aiming to take advantage of trusted relationships.



RECOMMENDED SECURITY IMPROVEMENT

If possible, do not allow direct access from the internet. Exposing RDP could allow for attackers to bypass a network's security stack. Enforce multifactor authentication on all remote services.

Enterprise VPN clients are often used for remote access from IT to OT environments. Dragos has previously reported on adversaries that have shown interest in VPN services, including XENOTIME. Additionally, a September 2019 report described a series of cyberattacks that targeted Airbus via VPN connections between the company and its suppliers reportedly with the intention to steal commercial information and intellectual property.⁴⁰ Dragos observes that similar techniques can be used for other disruptive or destructive ICS-specific cyber incidents.

COMMON TACTICS REMAIN EFFECTIVE

ICS-TARGETING ADVERSARIES CONTINUE TO USE COMMON AND POPULAR TACTICS TO ACHIEVE INITIAL ACCESS.

In June, Dragos identified MAGNALLIUM using brute force password spraying techniques against oil and gas entities in the US, Europe, and the Asia-Pacific region, a new method of initial access for this group. The group implemented the same technique against additional energy companies including electric utilities in the following months. Password spraying refers to adversaries targeting large numbers of accounts using common passwords to perform large-scale authentication attempts.



RECOMMENDED SECURITY IMPROVEMENT

Ensure password complexity is enforced and two-factor authentication is enabled if possible. Identify attempts at password spraying through monitoring both network traffic and application information from webmail, remote services, etc.

Although password spraying is a relatively common technique attackers use to gain access to enterprise resources, organizations are often vulnerable to these types of attacks because of poor account management and authentication policies for external resources.

MAGNALLIUM also remained faithful to its often-observed phishing behavior. MAGNALLIUM frequently uses job-themed phishing lures, largely focused in the Middle East. However, in June and

November, Dragos identified MAGNALLIUM phishing campaigns using North American job-themed phishing lures; this change in phishing behavior aligned with shifts in targeting for other MAGNALLIUM activity, including password spraying as mentioned above.

Throughout the year, Dragos observed watering hole activity associated with DYMALLOY and ALLANITE. Watering holes, also known as strategic web compromises, refer to an adversary infecting a third-

party website frequented by the target with malware in order to compromise the actual targets. The groups' activity this year largely focused on Ukraine, however in

September, Dragos observed DYMALLOY establishing watering holes to compromise targets in Europe, North America, and the Asia-Pacific region.

In the latter part of 2019, Dragos observed a LinkedIn phishing campaign targeting ICS entities. Adversaries used LinkedIn direct messaging to

send “project proposal”-themed lures. LinkedIn can be a useful phishing route for an adversary as it can bypass email security filters and attackers can leverage users’ network connections to appear as a legitimate contact.

Finally, in July and August, Dragos observed a phishing campaign by an unknown adversary that utilized traditional email phishing messages mimicking engineering entities to deliver “LookBack” malware to electric utilities. Dragos collaborated with our intelligence sharing partners to learn more about the campaign’s targeting, and Dragos identified adversary infrastructure, including domains spoofing major engineering standards bodies and a utility regulator. The messages specifically targeted electric utilities in the US. Security firm Proofpoint published public details on the campaign.⁴¹



ICS-SPECIFIC TACTICS GROWING

AS ICS-TARGETING ADVERSARIES BECOME INCREASINGLY SOPHISTICATED AND ADOPT BEHAVIORS SPECIFIC TO ICS ENVIRONMENTS, DEFENDERS MUST BE ARMED WITH TOOLS AND RESOURCES FOR IDENTIFYING AND COMBATING SUCH ACTIVITY.

Although common enterprise tactics remain effective, adversaries are moving towards ICS specific capabilities. Environmental context is key to threat detection; for instance, the difference between lateral movement in a DMZ or lateral movement from an engineering workstation to a safety instrumented system can make all the difference in detection and response.

To that end, Dragos collaborated with MITRE on creating the new ATT&CK for ICS⁴¹ framework. It is designed to help analysts, defenders, and other security practitioners better understand threat behaviors affecting industrial environments and develop defensive strategies. The existing and widely used ATT&CK for Enterprise framework breaks down

common tactics, techniques, and procedures observed by numerous activity groups and buckets them into separate fields like initial access, command and control, and lateral movement. Building on the existing documentation, Dragos and MITRE created a framework specifically for ICS to identify what behaviors and methods we observe targeting operations environments. New categories specific to operations environments within the ATT&CK for ICS framework include inhibiting control or response functions, and the ultimate impact.

Some of the tactics and visibility we have on ICS activity groups are detailed in the following section as mapped to the ATT&CK for ICS framework.*

**Not all of the tactics Dragos has visibility into are shared in this document to avoid threat proliferation. Please contact info@dragos.com to learn more.*

THREAT ACTIVITY GROUPS

Dragos categorizes behavior by activity group,⁴² creating threat analytics that provide comprehensive data around actions, capabilities, and intentions for our Dragos Platform technology.



We report on these threats in our WorldView intelligence reporting. We currently publicly label 11 ICS-focused activity groups and track more unlabeled activity of interest. The following summaries include newly identified activity groups as well as recent activity that Dragos links with high confidence to tracked activity groups.



HEXANE

DRAGOS IDENTIFIED HEXANE IN MAY TARGETING OIL AND GAS COMPANIES IN THE MIDDLE EAST, INCLUDING KUWAIT AS A PRIMARY OPERATING REGION.


Additionally, and unlike other activity groups Dragos tracks, **HEXANE** also targeted telecommunication providers in the greater Middle East, Central Asia, and Africa, potentially as a steppingstone to network-focused man-in-the-middle* and related attacks.

* A "man-in-the-middle" attack describes an adversary surreptitiously compromising communications between two or more parties and can be used to conduct espionage or disrupt or alter communications.

HEXANE intrusion activity includes malicious documents that drop malware to establish footholds for follow-on activity. Although the group appears operational since at least mid-2018, activity accelerated in early- to mid-2019. This timeline, targeting, and increase of operations coincides with an escalation of tensions within Middle East, a current area of political and military conflict.

HEXANE's telecommunications targeting appears to follow a trend demonstrated by other activity groups. ICS adversaries are increasingly targeting third-party organizations along the supply chains of potential targets. For instance, in 2018, Dragos identified the activity group XENOTIME targeting several industrial original equipment manufacturers (OEMs), and hardware and software suppliers.

HEXANE demonstrates similarities to the activity groups **MAGNALLIUM** and **CHRYSENE**, which are discussed below. These activity groups perform ICS-targeting activities focused largely on oil and gas, and share some similar observed tactics, techniques, and procedures (TTPs). Like **HEXANE**, **MAGNALLIUM** also increased its activity in early- to mid-2019. However, the collection of **HEXANE** behaviors, tools, and victimology makes this a unique entity compared to these previously observed activity groups.

	Hexane since 2018
> MODE OF OPERATION IT compromise and information gathering against ICS entities	
> CAPABILITIES Embedded binaries in documents, C2 via DNS and HTTP, evasion techniques	
> VICTIMOLOGY Oil & Gas, Middle East, Central Asia, Africa	
> LINKS None	



ICS ATT&CK MAPPING HIGHLIGHT

HEXANE uses User Interaction (T863) for Execution.

DEFINITION

Adversaries may rely on a targeted organizations' user interaction for the execution of malicious code. User interaction may consist of installing applications, opening email attachments, or granting higher permissions to documents. Adversaries may embed malicious code or visual basic code into files such as Microsoft Word and Excel documents or software installers. Execution of this code requires that the user enable scripting or write access within the document. Embedded code may not always be noticeable to the user especially in cases of trojanized software.

IN CONTEXT

HEXANE used ICS-themed phishing lures targeting industrial entities which required victims to enable macros to execute its malware.



PARISITE

DRAGOS IDENTIFIED PARISITE IN OCTOBER. PARISITE TARGETS VARIOUS INDUSTRIAL VERTICALS INCLUDING AEROSPACE, OIL AND GAS, AND MULTIPLE UTILITIES INCLUDING WATER, ELECTRIC, AND GAS.

PARISITE's broad geographic targeting includes entities in the US, the Middle East, Europe, and Australia. Although **PARISITE** appears focused on industrial organizations with ICS environments and related entities, its targeting activity spans across government and non-governmental organizations.



PARISITE
 since 2017

- MODE OF OPERATION**
 VPN compromise of IT networks to conduct reconnaissance
- CAPABILITIES**
 Exploiting known VPN vulnerabilities; SSH.NET, MASSCAN, and dsniiff hacking tools
- VICTIMOLOGY**
 US, Middle East, Europe, Australia, Electric, Oil & Gas, Aerospace, Government
- LINKS**
 MAGNALLIUM

Dragos identified **PARISITE** activity targeting ICS-related entities using known VPN vulnerabilities.⁴³ **PARISITE**'s current focus of targeting vulnerable VPN appliances indicates an interest in initial access to enterprise networks in order to gain access to industrial networks.

PARISITE infrastructure and capabilities date from at least 2017, indicating operations since at least that time. **PARISITE** uses known open source penetration testing tools for reconnaissance and to establish encrypted communications. This aligns with other activity groups increasingly using publicly available tools and resources as opposed to customized malware once achieving initial access.

At this time, **PARISITE** does not appear to have an ICS-specific disruptive or destructive capability. Dragos intelligence indicates **PARISITE** serves as the initial access group and enables further operations for **MAGNALLIUM**.



ICS ATT&CK MAPPING HIGHLIGHT

PARISITE uses Exploitation of Remote Services (T866) for Lateral Movement.

DEFINITION

Adversaries may exploit a software vulnerability to take advantage of a programming error in a program, service, or within the operating system software or kernel itself to enable remote service abuse. A common goal for post-compromise exploitation of remote services is for lateral movement to enable access to a remote system.

IN CONTEXT

PARISITE exploits known vulnerabilities in VPN appliances for initial access and lateral movement, specifically targeting ICS entities. Such access can enable a foothold for establishing OT network compromise.



MAGNALLIUM

IN 2019, MAGNALLIUM TARGETING EXPANDED TO INCLUDE NORTH AMERICAN ELECTRIC UTILITIES AS WELL AS GOVERNMENT AND FINANCIAL INSTITUTIONS.

Initially focused on oil and gas entities largely operating in the Middle East, **MAGNALLIUM's** expansion to additional industries in 2019 coincides with heightened tensions between multiple countries in the Middle East.

This year Dragos observed **MAGNALLIUM** deploying password spraying campaigns, a new initial access behavior for this group. **MAGNALLIUM** also relies extensively on phishing, frequently using job-themed lures to entice victims.

In July, Dragos identified a new disruptive malware dubbed **KILLGRAVE** associated with **MAGNALLIUM** activity. The malware targeted industrial entities in the Middle East and includes various capabilities to disrupt or potentially destroy infected systems depending on parameters. It represents a new threat to industrial entities either through indirect disruption via IT impacts, or direct disruption if attackers gain access to the ICS environment. Dragos intelligence indicates this malware was likely a coordination between **MAGNALLIUM** and **PARISITE**, with the latter staging the malware via VPN gateway compromise and **MAGNALLIUM** distributing it through the victim network.

Dragos initially identified **MAGNALLIUM** in 2017 and determined that the group targeted petrochemical and aerospace manufacturers since at least 2013. Initially targeting Saudi Arabian energy firms and an aircraft holding company, the group continues to expand targeting across the energy sector and related industries.



MAGNALLIUM
since 2016

- MODE OF OPERATION**
 IT network limited, information gathering against industrial orgs
- CAPABILITIES**
 STONEDRILL wiper, variants of TURNEDUP malware
- VICTIMOLOGY**
 Petrochemical, Aerospace, Oil & Gas, Electric, Saudi Arabia, North America
- LINKS**
 APT33, PARISITE



ICS ATT&CK MAPPING HIGHLIGHT

MAGNALLIUM's Impact causes Loss of View (T829)

DEFINITION

Adversaries may cause a sustained or permanent loss of view where the ICS equipment will require local, hands-on operator intervention; for instance, a restart or manual operation. By causing a sustained reporting or visibility loss, the adversary can effectively hide the present state of operations. This loss of view can occur without affecting the physical processes themselves.

IN CONTEXT

MAGNALLIUM activity includes creating and deploying IT-centric wiper malware targeting industrial entities that has the ability to cause loss of view within operations if the malware crosses the IT/OT boundary.



WASSONITE

DRAGOS IDENTIFIED THE WASSONITE ACTIVITY GROUP FOLLOWING A MALWARE INTRUSION AT THE KUDANKULAM NUCLEAR POWER PLANT (KKNPP) NUCLEAR FACILITY IN INDIA.⁴⁴

After further investigation, Dragos observed WASSONITE tools and behaviors targeting multiple industrial control system (ICS) entities including electric generation, nuclear energy, manufacturing, and organizations involved in space-centric research. WASSONITE has been active since at least 2018.

WASSONITE targeting focuses on Asian entities, largely in India, as well as possibly Japan and South Korea. At this time, WASSONITE does not appear to have an ICS-specific disruptive or destructive capability. All the activity represents Stage 1 of the ICS Kill Chain: access operations within IT networks.

WASSONITE operations rely on deploying DTrack malware for remote access to victim machines, capturing credentials via Mimikatz and publicly available tools, and utilizing system tools to transfer files and move laterally within the enterprise system. Researchers first disclosed DTrack in late September 2019,⁴⁵ and identified the tool targeting Indian financial institutions and research centers. DTrack is loosely connected to an earlier observed malware family, ATMDTrack, used for robbing ATM machines.

Third-party security firms associate DTrack and its related malware to the Lazarus Group.⁴⁶ Dragos also associates the activity group COVELLITE to Lazarus Group. However, COVELLITE does not overlap with observed WASSONITE activity despite links to broader Lazarus activity due to substantially different capabilities and infrastructure.



WASSONITE
since 2018

> **MODE OF OPERATION**
IT compromise and information gathering

> **CAPABILITIES**
DTrack RAT, Mimikatz, system tools for file transfer and lateral movement

> **VICTIMOLOGY**
India, South Korea, Japan, Electric, Nuclear, Oil & Gas, Manufacturing, Research

> **LINKS**
COVELLITE



ICS ATT&CK MAPPING HIGHLIGHT

WASSONITE uses Valid Accounts (T859) for Persistence

DEFINITION

Adversaries may steal the credentials of a specific user or service account using credential access techniques. In some cases, default credentials for control system devices may be publicly available. Compromised credentials may be used to bypass access controls placed on various resources on hosts and within the network, and may even be used for persistent access to remote systems. Compromised and default credentials may also grant an adversary increased privilege to specific systems and devices or access to restricted areas of the network. Adversaries may choose not to use malware or tools, in conjunction with the legitimate access those credentials provide, to make it harder to detect their presence or to control devices and send legitimate commands in an unintended way. Adversaries may also create accounts, sometimes using predefined account names and passwords, to provide a means of backup access for persistence.

IN CONTEXT

WASSONITE captures and re-uses legitimate credentials to establish persistence within victim networks. Such behaviors can be deployed to facilitate access to OT environments and control system devices.



XENOTIME

DRAGOS IDENTIFIED MULTIPLE INSTANCES OF XENOTIME PERFORMING RECONNAISSANCE AND POTENTIAL INITIAL ACCESS OPERATIONS ON NORTH AMERICAN AND APAC ELECTRIC UTILITY NETWORKS IN EARLY 2019. THE ACTIVITIES DATE BACK TO APRIL 2018 AT THE EARLIEST.

Available data indicates **XENOTIME** relies on capturing legitimate system credentials to move throughout the target network while deploying a combination of legitimate Windows utilities and custom-developed tools. Evidence suggests that unique tools associated with **XENOTIME** have been in development since 2014.

Dragos has also observed entities associated with **XENOTIME** experimenting with the Cobalt Strike penetration testing framework. This follows the previously-mentioned trend concerning adversaries leveraging legitimate penetration testing frameworks for use in malicious campaigns.

Dragos considers **XENOTIME** to be the most dangerous and capable activity group. It is responsible for the disruptive and nearly life-threatening TRISIS malware attack on an oil and gas facility in the Middle East in 2017.



ICS ATT&CK MAPPING HIGHLIGHT

XENOTIME uses Engineering Workstation Compromise (T818) for Initial Access

DEFINITION

Adversaries may compromise and gain control of an engineering workstation as an Initial Access technique into the control system environment. Access to an engineering workstation may occur as result of remote access or by physical means, such as a person with privileged access or infection by removable media. A dual-homed engineering workstation may allow the adversary access into multiple networks. For example, unsegregated process control, safety system, or information system networks. An Engineering Workstation is designed as a reliable computing platform that configures, maintains, and diagnoses control system equipment and applications. Compromise of an engineering workstation may provide access to and control of other control system applications and equipment.

IN CONTEXT

In the TRISIS event, XENOTIME compromised a workstation capable of communicating with a safety instrumented system (SIS) to act as a staging point for its disruptive malware.



DYMALLOY

IN 2019, DRAGOS IDENTIFIED WATERING HOLE ACTIVITY USING TACTICS, TECHNIQUES, AND PROCEDURES ASSOCIATED WITH THE DYMALLOY AND ALLANITE ACTIVITY GROUPS.

The compromised websites were associated with Ukrainian sports, media, and entertainment entities. In September 2019, Dragos observed new **DYMALLOY**-related activity indicating a return to operations outside of Ukraine – including North America and APAC.

DYMALLOY targeting generally focuses on energy companies and advanced industry entities in Europe, Turkey, and North America. Its attention largely shifted to Ukraine this year, coinciding with Ukrainian parliamentary elections in July 2019. Previously, **DYMALLOY** has demonstrated ability to achieve long-term and persistent access to IT and operational environments for intelligence collection and possible future disruption events.

DYMALLOY has used malware backdoors including Goodor, DorShel, and Karagany. These are commodity malware families, not unique to any particular group, but used together as a toolkit makes this group's behavior unique. Overall, **DYMALLOY** avoids using custom toolkits in its operations, making detection and specific attribution more difficult without recognizing the entirety of adversary actions. Dragos has also found the group leveraged Mimikatz, an open-source software security tool for extracting passwords from memory on Windows systems.

DYMALLOY has operated since at least 2015 and is linked* to the "Dragonfly 2.0" group.⁴⁷



DYMALLOY
 since 2016

- > **MODE OF OPERATION**
Deep ICS environment information gathering, operator credentials, industrial process details
- > **CAPABILITIES**
GOODOR, DORSHEL, KARAGANY, Mimikatz
- > **VICTIMOLOGY**
Turkey, Europe, US
- > **LINKS**
Dragonfly2, Berserker Bear



ICS ATT&CK MAPPING HIGHLIGHT

DYMALLOY uses Screen Capture (T852) for Collection

DEFINITION

Adversaries may attempt to perform screen capture of devices in the control system environment. Screenshots may be taken of workstations, HMIs, or other devices that display environment-relevant process, device, reporting, alarm, or related data. These device displays may reveal information regarding the ICS process, layout, control, and related schematics. In particular, an HMI can provide a lot of important industrial process information. Analysis of screen captures may provide the adversary with an understanding of intended operations and interactions between critical devices.

IN CONTEXT

DYMALLOY successfully obtained HMI screenshots while conducting reconnaissance in target operations networks.

* Links means that there are technical overlaps or assessments made from other entities that provide some connection to the groups; however this is not to imply that there is a one to one relationship to these groups and they should not be considered aliases.



ALLANITE

IN 2019, DRAGOS IDENTIFIED WATERING HOLE ACTIVITY ALIGNING WITH ALLANITE AND DYMALLOY ACTIVITY COMPROMISING WEBSITES ASSOCIATED WITH UKRAINIAN SPORTS, ENTERTAINMENT, AND MEDIA ENTITIES. DRAGOS ASSESSES THE GROUPS' TARGETING SHIFTED DUE TO CURRENT GEOPOLITICAL EVENTS IN UKRAINE.

ALLANITE activity historically focuses on ICS reconnaissance and information gathering against US and UK victims. **ALLANITE** avoids using malware for initial infection and subsequent activity, relying instead on credential capture from authentication attempts and use of native Windows system tools for system discovery and information gathering.

ALLANITE relies upon insecure environments lacking adequate network traffic control and using single-factor authentication mechanisms for operational techniques. There is no evidence that **ALLANITE** possesses or aims to use any disruptive or destructive capability within target ICS environments. Although superficially similar to other ICS activity groups such as Dragonfly and **DYMALLOY**, **ALLANITE**'s methods, tools, and technology are significantly different from these other entities.

ALLANITE has conducted intrusion and reconnaissance activities within ICS corresponding with Stage 1 of the ICS Cyber Kill Chain and demonstrates some level of intent to move to Stage 2.



ALLANITE
 since 2017

- > **MODE OF OPERATION**
Watering-hole and phishing leading to ICS recon and screenshot collection
- > **CAPABILITIES**
Powershell scripts, THC Hydra, SecretsDump, Inveigh, PSEXec
- > **VICTIMOLOGY**
Electric utilities, US & UK
- > **LINKS**
Palmetto Fusion



ICS ATT&CK MAPPING HIGHLIGHT

ALLANITE uses Point and Tag Identification (T852) for Collection

DEFINITION

Adversaries may collect point and tag values to gain a more comprehensive understanding of the process environment. Points may be values such as inputs, memory locations, outputs or other process specific variables. Tags are the identifiers given to points for operator convenience. Collecting such tags provides valuable context to environmental points and enables an adversary to map inputs, outputs, and other values to their control processes. Understanding the points being collected may inform an adversary on which processes and values to keep track of over the course of an operation.

IN CONTEXT

ALLANITE obtained access to ICS environments, identified point and tag values like device type and control functions. Such information could be combined with exfiltration of plant schematics to develop and conduct tailored operations.



CHRYSENE

CHRYSENE IS RESPONSIBLE FOR INITIAL INTRUSIONS ACROSS SEVERAL CRITICAL INFRASTRUCTURE SECTORS, INCLUDING ELECTRIC UTILITIES AND OIL AND GAS, SINCE AT LEAST MID-2017, WITH AN OPERATIONAL FOCUS ON EUROPE, NORTH AMERICA, AND THE MIDDLE EAST.

Dragos identified phishing activity associated with this group in early 2019 using IT-themed lures and PowerShell for post-exploitation. Dragos identified additional samples of this group's malware indicating they are active and evolving in more than one area.

While observed activity has not revealed an ICS-specific capability, the **CHRYSENE**'s ability and intentions strongly indicate the group is collecting information and achieving initial access in target networks that would be necessary precursors to an attack on ICS operations. **CHRYSENE** has not been observed in further exploitation; they appear to operate as a specialized team in victim acquisition passing the victim to another group for further operations.

This group has some similarities to **HEXANE**. **CHRYSENE**-related activity is known by other names within the security community including Greenbug, APT34, and OilRig.⁴⁸ In April 2019, an unknown entity leaked a slew of hacking tools used by **CHRYSENE**, compromising their known operations and behaviors.⁴⁹ Dragos assesses **CHRYSENE** likely shifted its behavior and retooled following this leak.



CHRYSENE
since 2017

- > **MODE OF OPERATION**
IT compromise, information gathering and recon against industrial orgs
- > **CAPABILITIES**
Watering holes, 64-bit malware, covert C2 via IPv6 DNS, ISMD00R
- > **VICTIMOLOGY**
Oil & Gas, Manufacturing, Europe, MENA, N. America
- > **LINKS**
OilRig, Greenbug




ICS ATT&CK MAPPING HIGHLIGHT

CHRYSENE uses Scripting (T853) for Execution

DEFINITION

Adversaries may use scripting languages to execute arbitrary code in the form of a pre-written script or in the form of user-supplied code to an interpreter. Scripting languages are programming languages that differ from compiled languages, in that scripting languages use an interpreter, instead of a compiler. These interpreters read and compile part of the source code just before it is executed, as opposed to compilers, which compile each and every line of code to an executable file. Scripting allows software developers to run their code on any system where the interpreter exists. This way, they can distribute one package, instead of precompiling executables for many different systems. Scripting languages, such as Python, have their interpreters shipped as a default with many Linux distributions. In addition to being a useful tool for developers and administrators, scripting language interpreters may be abused by the adversary to execute code in the target environment. Due to the nature of scripting languages, this allows for weaponized code to be deployed to a target easily, and leaves open the possibility of on-the-fly scripting to perform a task.

IN CONTEXT

When CHRYSENE gains code execution on a target host, it may deploy encoded malware; the executable is decoded and launched via PowerShell command. PowerShell commands can be deployed by adversaries on Windows hosts within the ICS environment.



RASPITE

DRAGOS FIRST IDENTIFIED RASPITE IN 2018, AND ITS ACTIVITY TO DATE FOCUSES ON INITIAL ACCESS OPERATIONS WITHIN THE ELECTRIC UTILITY SECTOR. ALTHOUGH FOCUSED ON ORGANIZATIONS WITH ICS ENVIRONMENTS, RASPITE HAS NOT DEMONSTRATED AN ICS-SPECIFIC CAPABILITY TO DATE.

In 2019, Dragos identified two new customized applications linked to **RASPITE**. While the two items were not identified until recently, analysis indicates both were developed and likely deployed in 2017, coinciding with the first known activity from **RASPITE**. Further analysis indicates that both applications are tools that **RASPITE**, or another entity, would leverage as part of an intrusion for network enumeration or propagation.

RASPITE leverages custom software and scripts to manipulate victim machines, install malicious services, and enable remote access to victim networks. After almost exclusively focusing on political and strategic targets in the Middle East in 2017, **RASPITE** pivoted to ICS-related organizations in North America in 2018.



RASPITE
 since 2017

- MODE OF OPERATION**
 IT network limited, information gathering on electric utilities with some similarities to CHRYSENE
- CAPABILITIES**
 Service installer malware designed to beacon out to adversary infrastructure
- VICTIMOLOGY**
 Electric Utilities, US, Saudi Arabia, Japan
- LINKS**
 NONE




ICS ATT&CK MAPPING HIGHLIGHT

RASPITE uses Drive-by Compromise (T817) for Initial Access

DEFINITION

Adversaries may gain access to a system during a drive-by compromise, when a user visits a website as part of a regular browsing session. With this technique, the user's web browser is targeted and exploited simply by visiting the compromised website. The adversary may target a specific community, such as trusted third-party suppliers or other industry specific groups, which often visit the target website. This kind of targeted attack relies on a common interest, and is known as a strategic web compromise or watering hole attack.

IN CONTEXT

Dragos observed RASPITE using watering holes for credential capture. Though the compromised websites were not ICS-specific, employees of the targeted ICS entities would be likely to visit them.




ELECTRUM

ELECTRUM IS RESPONSIBLE FOR THE CRASHOVERRIDE MALWARE ATTACK WHICH SUCCESSFULLY BLACKED OUT PORTIONS OF KIEV, UKRAINE IN DECEMBER 2016. IT IS ASSOCIATED WITH THE SANDWORM GROUP.⁵⁰

Dragos identified ELECTRUM and SANDWORM collaborated on CRASHOVERRIDE as part of a two-pronged attack: SANDWORM served as the initial access vector that enabled the ICS-specific entity, ELECTRUM, to conduct a sequenced, ICS-specific attack aimed at physical process destruction.

CRASHOVERRIDE represents the first publicly known application of specialization and division of labor to ensure maximal effectiveness and efficiency in critical infrastructure-targeting cyberattacks.

Dragos did not observe ELECTRUM in 2019. It is possible ELECTRUM has substantially changed behavior and is now identified as another activity group, reduced their activity below detectable levels, or gone away entirely.



ELECTRUM
 since 2016

- > **MODE OF OPERATION**
Electric grid disruption and long-term persistence
- > **CAPABILITIES**
CRASHOVERRIDE
- > **VICTIMOLOGY**
Ukraine, Electric Utilities
- > **LINKS**
Sandworm




ICS ATT&CK MAPPING HIGHLIGHT

ELECTRUM uses Data Destruction (T809) to Inhibit Response Function

DEFINITION

Adversaries may perform data destruction over the course of an operation. The adversary may drop or create malware, tools, or other non-native files on a target system to accomplish this, potentially leaving behind traces of malicious activities. Such non-native files and other data may be removed over the course of an intrusion to maintain a small footprint or as a standard part of the post-intrusion cleanup process.

IN CONTEXT

ELECTRUM deployed a wiper module in the 2016 CRASHOVERRIDE event. The module was designed to impede the target's recovery process and delete configuration files which would inhibit restoration on infected SCADA systems.




COVELLITE

**COVELLITE PREVIOUSLY
COMPROMISED IT NETWORKS
ASSOCIATED WITH ELECTRIC
UTILITIES, PRIMARILY IN EUROPE,
EAST ASIA, AND NORTH AMERICA.**

The group has not shown 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 is continuing to target electric utilities.⁵¹

COVELLITE is linked to the Lazarus Group, which third-parties attribute to North Korean state interests. Due to a lack of recent ICS targeting observed by this group, it is possible COVELLITE evolved into a new activity group with different TTPs and targeting focus. Dragos will continue to monitor COVELLITE and potentially associated groups and behaviors that may be reflected in future operations against ICS targets.



COVELLITE
since 2017

- MODE OF OPERATION**
 IT compromise with hardened anti-analysis malware against industrial orgs
- CAPABILITIES**
 Encoded binaries in documents, evasion techniques
- VICTIMOLOGY**
 Electric Utilities, US
- LINKS**
 Lazarus, Hidden Cobra



ICS ATT&CK MAPPING HIGHLIGHT

COVELLITE uses Spearphishing Attachments (T865) for Initial Access

DEFINITION

Adversaries may use spearphishing attachment, a variant of spearphishing, as a form of social engineering attack against specific targets. Spearphishing attachment is different from other forms of spearphishing in that it employs the use of malware attached to an email. All forms of spearphishing are electronically delivered social engineering targeted at a specific individual, company, or industry. In this scenario, adversaries attach a file to the spearphishing email and usually rely upon User Execution to gain execution and access.

IN CONTEXT

Dragos observed COVELLITE targeting grid operators with phishing attacks attempting to gain initial access to their networks. Such access could establish a foothold for future compromise and potentially help facilitate movement to the OT network.

CONCLUSION

Dragos anticipates activity targeting and affecting ICS to increase into 2020 and further. We expect to see more adversaries expand their focus to additional critical infrastructure and industrial environments, which will likely align with activity associated with military or geopolitical conflict. Although defenders continue to gain insight through OT-specific detection and monitoring platforms, it is imperative we continue to improve visibility into activities and threats impacting critical infrastructure.

Although 2019 did not produce a disruptive or destructive attack with an impact like CRASHOVERRIDE or TRISIS, Dragos expects adversaries to be developing such capabilities and will likely leverage them for disruptive effects in the future.

Despite adversaries continuing to evolve and develop their capabilities, Dragos anticipates continued collaboration with our partners, clients, and the community at large to improve cybersecurity awareness and better secure industrial control systems.

In 2020, we plan to continue embodying our mission to safeguard civilization.

APPENDIX

- 1 <https://dragos.com/adversaries/>
- 2 <https://dragos.com/blog/industry-news/threat-proliferation-in-ics-cybersecurity-xenotime-now-targeting-electric-sector-in-addition-to-oil-and-gas/>
- 3 <https://dragos.com/blog/industry-news/supply-chain-threats-to-industrial-control-third-party-commitment/>
- 4 <https://dragos.com/blog/industry-news/implications-of-it-ransomware-for-ics-environments/>
- 5 <https://dragos.com/blog/industry-news/industrial-cyber-attacks-a-humanitarian-crisis-in-the-making/>
- 6 <https://dragos.com/blog/industry-news/escalating-cyber-tensions-risk-human-life/>
- 7 <https://dragos.com/resource/industrial-control-threat-intelligence-whitepaper/>
- 8 <https://dragos.com/blog/industry-news/combating-cyber-attacks-with-consequence-driven-ics-cybersecurity/>
- 9 <https://dragos.com/blog/industry-news/rising-cyber-escalation-between-us-iran-and-russia-ics-threats-and-response/>
- 10 <https://dragos.com/blog/industry-news/threat-proliferation-in-ics-cybersecurity-xenotime-now-targeting-electric-sector-in-addition-to-oil-and-gas/>
- 11 <https://dragos.com/resource/dragos-oil-and-gas-threat-perspective-summary/>
- 12 <https://www.wired.com/story/iran-hackers-us-phishing-tensions/>
- 13 <https://cyware.com/news/altran-technologies-hit-by-lockergoga-ransomware-attack-e1f90570>
- 14 <https://www.bbc.com/news/business-48661152>
- 15 <https://www.wired.com/story/notpetya-cyberattack-ukraine-russia-code-crashed-the-world/>
- 16 <https://blog.talosintelligence.com/2019/09/emotet-is-back-after-summer-break.html>
- 17 <https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf>
- 18 <https://toronto.citynews.ca/video/2019/04/11/canadian-company-victim-of-apparent-cyber-attack/>
- 19 https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/MSIB/2019/MSIB_10_19.pdf?ver=2019-12-23-134957-667
- 20 <https://www.cyber.gov.au/threats/advisory-2019-131-emotet-malware-campaign>
- 21 <https://www.news24.com/SouthAfrica/News/joburg-prepaid-electricity-users-left-in-the-dark-as-city-power-crippled-by-computer-virus-20190725>
- 22 <https://www.rheinmetall-automotive.com/en/press/press-releases/news-detail/news/regional-disruption-of-production-due-to-malware-at-rheinmetall-automotive/>
- 23 <https://www.computerworld.dk/art/248774/kritisk-it-nedbrud-bliver-dyrt-for-demant-vurderer-it-sikkerhed-sekspert-det-ligner-et-ransomware-angreb>
- 24 <https://www.zdnet.com/article/major-german-manufacturer-still-down-a-week-after-getting-hit-by-ransomware/>
- 25 https://elpais.com/economia/2019/11/17/actualidad/1574027226_840148.html
- 26 <https://www.ibm.com/downloads/cas/OAJ4VZNJ>
- 27 <https://www.microsoft.com/security/blog/2019/12/12/gallium-targeting-global-telecom/>
- 28 <https://www.cybereason.com/blog/operation-soft-cell-a-worldwide-campaign-against-telecommunications-providers>
- 29 <https://www.sans.org/reading-room/whitepapers/ICS/industrial-control-system-cyber-kill-chain-36297>
- 30 <https://krebsonsecurity.com/2019/04/experts-breach-at-it-outsourcing-giant-wipro/>
- 31 <https://www.wipro.com/consumer-packaged-goods/wipro-promax/>
- 32 <https://dragos.com/year-in-review/>
- 33 <https://www.wipro.com/consumer-packaged-goods/wipro-promax/>
- 34 <https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/>
- 35 <https://doublepulsar.com/bluekeep-exploitation-activity-seen-in-the-wild-bd6ee6e599a6>
- 36 CVE-2019-11510
- 37 CVE-2019-1579
- 38 CVE-2018-13379
- 39 <https://www.ncsc.gov.uk/news/alert-vpn-vulnerabilities>
- 40 <https://www.france24.com/en/20190926-airbus-hit-by-series-of-cyber-attacks-on-suppliers>
- 41 https://collaborate.mitre.org/attackics/index.php/Main_Page
- 42 <http://www.diamondmodel.org/>
- 43 <https://www.ncsc.gov.uk/news/alert-vpn-vulnerabilities>
- 44 <https://www.zdnet.com/article/confirmed-north-korean-malware-found-on-indian-nuclear-plants-network/>
- 45 https://usa.kaspersky.com/about/press-releases/2019_dtrack-previously-unknown-spy-tool-hits-financial-institutions-and-research-centers
- 46 <https://securelist.com/my-name-is-dtrack/93338/>
- 47 <https://attack.mitre.org/groups/G0074/>
- 48 <https://attack.mitre.org/groups/G0049/>
- 49 <https://www.zdnet.com/article/source-code-of-iranian-cyber-espionage-tools-leaked-on-telegram/>
- 50 <https://attack.mitre.org/groups/G0034>
- 51 <https://dragos.com/resource/covellite/>
- 53 <https://www.zdnet.com/article/source-code-of-iranian-cyber-espionage-tools-leaked-on-telegram/>
- 54 <https://attack.mitre.org/groups/G0034>
- 55 <https://dragos.com/resource/covellite/>