WWW.DRAGOS.COM

EUROPEAN INDUSTRIAL INFRASTRUCTURE CYBER THREAT PERSPECTIVE

DRAGOS, INC.
INTEL@DRAGOS.COM

APRIL 2022

SUMMARY

Dragos assesses with high confidence that adversaries pose a threat to European Industrial Infrastructure[1] for the following reasons presently and into the next 12 months:

- Increasing regional tensions are likely to result in industrial operations impact from criminal and other adversaries. Particularly of concern are geographically dispersed industrial operations such as renewable electric generation, electric transmission, upstream and midstream oil and gas, water and wastewater management, etc.
- The increase in ransomware attacks, especially those targeting small- to medium-sized manufacturing entities
- The continued development of Activity Group (AG) techniques, tactics, and procedures (TTPs)
- The high interdependence yet independently managed and operated nature of industrial operations across Europe present a unique regional systematic risk where a threat to one European country is a threat to operations in other countries.

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

Dragos assesses with high confidence that the biggest cybersecurity weaknesses European asset owners currently face are a lack of asset visibility into their network and weak network authentication policies. Without asset visibility organizations are unable to properly secure their OT environments as defenders cannot protect what they cannot see. Industrial operators should evaluate and implement the principle of least privilege to limit unauthorized access to OT environments.

Targeted threats (e.g., activity groups) that focus on infiltrating and disrupting industrial control systems pose the most cybersecurity risk to European Industrial Infrastructure. The regionalization of OT equipment use, paired with the dynamic political and economic systems across European countries and European companies create an environment with higher barriers for information sharing and collaboration to defend against regional threats and adversaries.

KEY FINDINGS

Dragos-tracked Activity Groups target European entities with disruptive and destructive attacks. Even if not currently active, Dragos assesses with moderate confidence these groups likely maintain this level of capabilities, should a situation warranting such use reoccur.

While all private and public European industrial entities face a threat from ransomware operators, small- and medium-sized manufacturing firms in Italy, Germany, Austria, and Switzerland are at the highest risk for targeting, specifically by Ransomware-as-a-Service groups, due to lack of IT/OT security and obscured asset visibility.

Oil and Natural Gas assets, including key regasification plants such as those located in Rotterdam, present a target for adversaries looking to disrupt the flow of Oil & Natural Gas (ONG) energy into Europe.

The UK Electric sector is at risk of disruption by adversaries capable of carrying out coordinated attacks against multiple power stations. The Transmission sector is also at risk due to the limited number of controlling parties, though these entities generally demonstrate a greater degree of defense in depth.

Public and private entities will continue to struggle with widely acknowledged threats to OT environments, including those brought by insiders, supply chain threats, intellectual property theft, and digital transformation. These threats may decrease as organizations invest in cybersecurity programs and progress in maturity.

Finally, European organizations face unique risks from political and economic threats in both the near- and far-term abroad. Historic adversary operations against Industrial Infrastructure in Europe have been well documented, including a unique case in which attempted intellectual property theft resulted in extreme operational impact.

ACTIVITY GROUPS

The Activity Groups described below are most active in Europe.

PARISITE

PARISITE targets utilities, aerospace, and ONG entities. Its geographic targets include Europe along with the Middle East and North America.[2] PARISITE uses open-source tools to compromise infrastructure and leverages known virtual private network (VPN) vulnerabilities for initial access. The scope of this group's targeting also includes government and non-governmental organizations. This group has operated since at least 2017, according to Dragos research. Dragos intelligence indicates that PARISITE serves as the initial access group that enables further operations for MAGNALLIUM.

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

XENOTIME

In 2018 XENOTIME activity expanded outside the Middle East to include ONG companies in Europe, the U.S., and Australia. Dragos assesses with moderate confidence, XENOTIME likely possesses capabilities to disrupt oil and natural gas operations in the North Sea.[3] In January 2022, Dragos observed XENOTIME activity focused on research and reconnaissance against Liquefied Natural Gas (LNG) entities in Europe and the United States both in the midstream and downstream verticals. XENOTIME activity currently appears to be the research of LNG entities and reconnaissance of LNG entity infrastructure.[4]

Associated Groups: **Temp.Veles**

MAGNALLIUM

MAGNALLIUM expanded targeting to include entities in Europe and North America after it initially targeted an aircraft holding company and ONG firms based in Saudi Arabia. In 2020, Dragos identified three malicious Hypertext Markup Language (HTML) application samples similar to known MAGNALLIUM behaviors; the samples indicated possible targeting in the United Kingdom and U.S., with a possible emphasis on semiconductor manufacturing and government entities.[5] MAGNALLIUM appears to lack an OT-specific capability, and the group remains focused on initial IT intrusions.[6] Dragos has observed several events where IT focused threats gain access to OT due to a lack of proper segmentation, network misconfigurations, and open internet connections to OT environments. MAGNALLIUM has targeted energy and aerospace entities since at least 2013.

Associated Groups: **APT 33, Elfin**[7]

DYMALLOY

DYMALLOY's victims include electric utilities, ONG, and advanced industry entities in Europe, Turkey, and North America.[8] It is a highly aggressive and capable activity group that can achieve long-term and persistent access to IT and operational technology environments for intelligence collection and possible future disruption events. Dragos assesses with moderate confidence that DYMALLOY repeatedly targeted the Ukrainian energy sector throughout 2019 and 2020; additionally, DYMALLOY has leveraged multiple Ukrainian websites to conduct watering hole attacks.[9] In Q2 of 2021, Dragos identified this AG expanding its targeting to include the Asia Pacific (APAC) region based on newly identified malware samples illustrating their capability to operate globally.

Associated Groups: **Dragonfly 2.0, Berserk Bear**[10]

ELECTRUM

ELECTRUM was responsible for the disruptive CRASHOVERRIDE event in Ukraine in 2016.[11] This group is capable of developing malware that can modify electric equipment processes, leveraging OT protocols and communications. In 2020, Dragos identified a malicious modified Notepad.exe file structurally and behaviorally similar to items associated with ELECTRUM activity seen in the 2016 Ukraine power event.[12] While leveraging multiple publicly available tools for creation, the specific shellcode and other observables within the sample are nearly identical to items ELECTRUM used as part of the CRASHOVERRIDE incident. While Dragos cannot definitively associate the activity with ELECTRUM, given that this activity group is responsible for one of the few known disruptive attacks on industrial infrastructure, Dragos considers this worth monitoring.

Associated Groups: **SANDWORM**[13]

ALLANITE

ALLANITE targets enterprise and OT networks in the UK and U.S. electric utility sectors, as well as German Industrial Infrastructure. The group performs reconnaissance in OT environments to potentially stage disruptive events. ALLANITE has demonstrated the capability to access and operate within the Downstream OT environment. In 2020, a confidential notice from several German government agencies leaked information online related to state-directed intrusions into German critical infrastructure; further Dragos analysis indicates the German technical description overlaps with the ALLANITE activity group.[14] There is no indication ALLANITE has a disruptive or damaging capability or intent as of late 2021.[15]

Associated Groups: **PALMETTO FUSION, Dragonfly 2.0,**[16] **Berserk Bear**

CHRYSENE

CHRYSENE has targeted the IT networks of multiple Industrial Infrastructure organizations since early 2017, with operations focusing mostly on Europe and the Middle East, with some potential indications of operations in North America. The AG targets petrochemical, ONG, and electric generation sectors. Although CHRYSENE itself has yet to demonstrate an OT capability, the group's operations are consistent with initial access and information gathering operations against OT asset owners and operators that can be used to facilitate a future attack.[17]

Associated Groups: **APT 34, GREENBUG, OilRig**[18]

KAMACITE

KAMACITE represents a long-running set of related behaviors targeting critical infrastructure and industrial verticals since at least 2014; the group facilitated OT-specific operations including the BLACKENERGY2 campaign and the 2015 and 2016 Ukraine power events.[19] Dragos assesses with moderate confidence that KAMACITE is an AG that develops access for other groups like ELECTRUM that then follow on with OT-focused attacks. In August 2021, Dragos identified and analyzed a sample of GREYENERGY, a modular malware seen as the successor to BLACKENERGY3, indicating the group remains active and continues to develop its TTPs.

Associated Groups: **Sandworm, ELECTRUM**

COVELLITE

Covellite executes IT compromise with hardened anti-analysis malware against industrial organizations using encoded binaries in documents and evasion techniques.[20] This AG targets electric utilities in Europe, the US, and East Asia. In 2020, Dragos identified potential COVELLITE phishing documents targeting aerospace victims in France; however, Dragos has not identified similar activity targeting Industrial Industry-related entities since COVELLITE operations from 2017-2018.[21]

Associated Groups: **Lazarus Group, Hidden Cobra**

VANADINITE

In 2020, the United States (U.S.) Department of Justice (DOJ) and Federal Bureau of Investigation (FBI) unsealed indictments against several nationals from the People's Republic of China (PRC). Some activity noted in the indictment overlaps with VANADINITE operations targeting external-facing, vulnerable services including various industrial organizations, including victims in Europe.[22] VANADINITE emerged in 2019 as an initial access mechanism targeting various industrial entities. The group uses vulnerabilities in external-facing network appliances, such as VPN gateways, to gain initial access to networks and establish presence.[23]

Associated Groups: **APT41, LEAD, Winnti Group**

THREAT PERSPECTIVE: DEEP DIVES BY INDUSTRY AND REGION

OVERVIEW

Europe is a valuable target for adversaries and criminals exploiting OT environments for geopolitical reasons or financial remuneration. As the number of attacks against Industrial Infrastructure increases globally, adversaries with specific interest in industrial companies remain active and continue to adjust their Tactics, Techniques and Procedures (TTPs). Adversaries will more easily execute attacks against OT environments that cause operational disruptions or damage as state-associated and criminal group capabilities improve. This section provides a summary of Dragos reports, vulnerability assessments, and other indicators affecting European Industrial Infrastructure entities.

- Dragos assesses with moderate confidence Europe is at low risk for widespread Industrial Infrastructure-targeted destruction and disruption campaigns originating from cyberattacks due to the deterrence posed by potential political and economic impact as well as the direct effect on civilian lives and infrastructure.
- Additionally, Dragos assesses with low confidence Europe is at a low risk for localized or small-scale disruption or destruction, as motivated state-executed adversaries may preform low-stakes operations when deemed politically or economically advantageous.

RANSOMWARE IMPACT TO DAS+I COUNTRIES

THREAT LANDSCAPE

The countries of Germany, Austria, Switzerland and Italy (DAS+I) make up a significant portion of manufacturing in Europe; together, Germany and Italy account for 47% of sold production in Europe, according to Eurostat.[24] Dragos analyzed Dark Web resources from June 1 to December 31. Dark Web site victim postings of DAS+I countries accounted for 56 of 79 postings involving European countries, or 71% total European victims. Of these, 45 (80%) were in the manufacturing sector. The highest number of manufacturing subsector victim postings were for metal product manufacturing. Ransomware-as-a-Service (RaaS) families Lockbit 2.0 and Conti were responsible for 34 of the 56 attacks (61%). This trend is reflected globally. Many victim companies were of small- to medium-size with similar technology processes, presenting ripe targets for ransomware adversaries.

ASSESSMENT

Dragos assesses with moderate confidence ransomware operators will continue to target DAS+I countries, and specifically manufacturing firms located in these countries, motivated by profit. While state-affiliated ransomware operations are extremely difficult to prove, Dragos assesses with low confidence this type of attack may occur in DAS+I countries and greater Europe. In-depth ransomware analysis for Europe is available below.

NORTH SEA OIL AND NATURAL GAS ASSETS AND AG ACTIVITY

THREAT LANDSCAPE

Since 2019, Dragos has assessed with low confidence increased targeting of the European oil and gas sector is likely, specifically by groups including DYMALLOY and XENOTIME. Gasification and processing terminals in key areas including the Isle of Grain and Rotterdam demonstrate key dependencies that could have a significant impact on European LNG if successfully disrupted by adversary groups. If these facilities are deemed too impenetrable for adversaries to dedicate time and resources to target, third-party suppliers of critical equipment, including the hydrogen used in the regasification process, may become attractive targets for adversaries due to lower barriers of entry caused by less mature security controls.

ASSESSMENT

Dragos assesses with moderate confidence that as European oil and gas operations expand and markets become more competitive, the economic interests of states that rely on the oil and gas vertical – for instance, state-owned oil companies – will likely generate more intrusions by groups like XENOTIME and DYMALLOY. All third-party connections should be thoroughly analyzed to ensure an attack on a third-party can be cordoned off from key dependencies.

UNITED KINGDOM ELECTRIC SECTOR THREATS

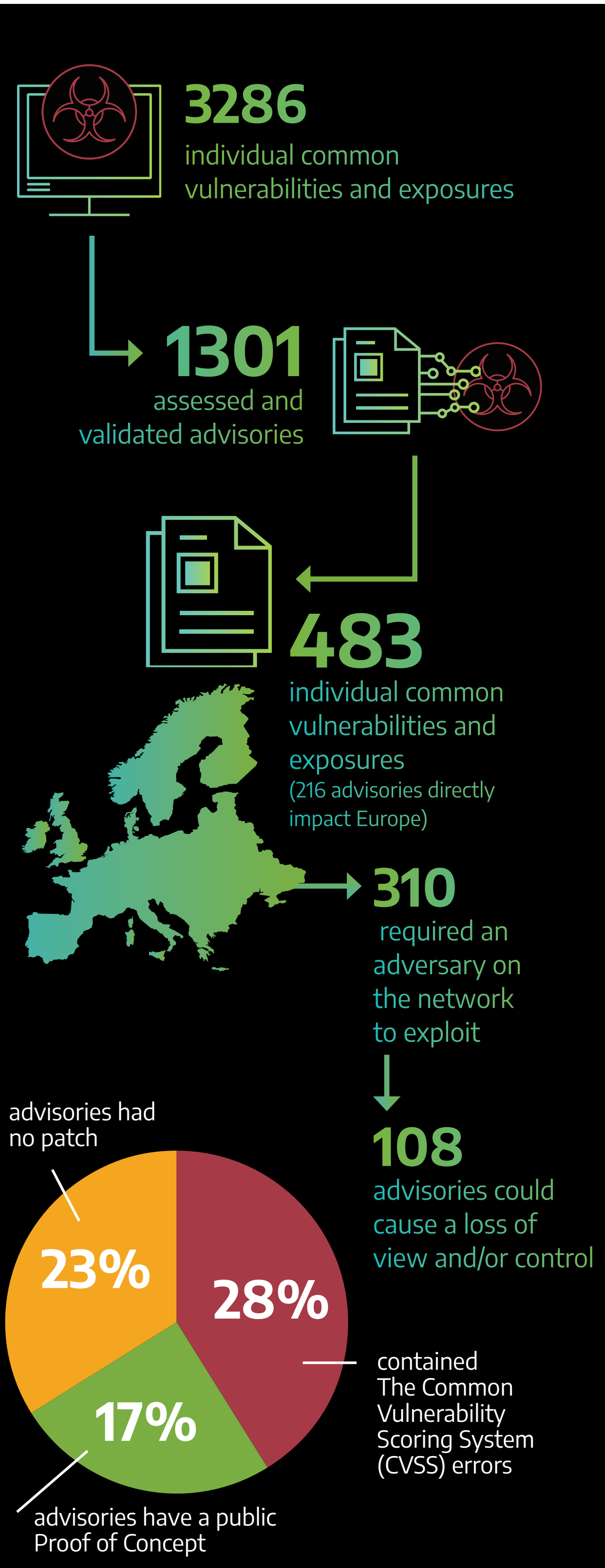
THREAT LANDSCAPE

The unique layout of the UK Energy sector naturally leads to a distinctive threat landscape. While an attack against Transmission assets would be most disruptive (specifically those of National Grid, which controls balancing for the U.K.) these organizations leverage a strong defense in depth at every level of the Purdue model to remain well guarded against adversaries. However, smaller distribution companies are less likely to have dedicated security staff and budgets. Combined with the Dragos 2021 Year in Review report indicating 77% of assets have porous IT/OT boundaries, these distribution companies have a high likelihood of OT devices connected directly to the internet or IT devices connecting into OT systems.[25] This poses significant potential for disruption if just one or two power stations or distribution experience an outage. On August 9, 2019, a simultaneous fire and lightning strike at small power stations on opposite sides of the United Kingdom led to one million customers losing access to electricity; while this event was not cyber-related in nature, it highlights the potential for adversaries with knowledge of OT environments to cause significant disruption through a small and coordinated attack.[26] Additionally, this event had a significant downstream impact on other key industrial Infrastructure verticals including transportation and water.

ASSESSMENT

Dragos assesses with moderate confidence groups that have previously targeted electricity operations in Europe, including XENOTIME and VANADINITE are likely to continue to demonstrate an interest in the United Kingdom energy infrastructure; however, a direct attack is unlikely, barring significantly heightened political tensions. Dragos assesses with low confidence adversaries, whether state-affiliated or cyber-criminals, may target small energy distributors and power stations to cause disruption or demand ransom payments.

OBSERVED RISKS AND IMPACTS



3286 individual common vulnerabilities and exposures

1301 assessed and validated advisories

483 individual common vulnerabilities and exposures (216 advisories directly impact Europe)

310 required an adversary on the network to exploit

108 advisories could cause a loss of view and/or control

advisories had no patch
23%
28%
17%
contained The Common Vulnerability Scoring System (CVSS) errors
advisories have a public Proof of Concept

VULNERABILITIES TO EUROPEAN INDUSTRIAL INFRASTRUCTURE

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

Vulnerabilities in OT-specific devices and services can introduce risk to the operating environment. As of February 2022, Dragos researchers assessed and validated 1301 advisories (3286 individual Common Vulnerabilities and Exposures) impacting industrial equipment worldwide. Of these, 216 advisories (483 individual Common Vulnerabilities and Exposures) directly impact Europe, as they are from vendors that European entities use, according to U.S. Cybersecurity and Infrastructure Security Agency (CISA) advisories analyzed by Dragos vulnerability analysts. Of these Europe-specific vulnerabilities, 310 (64%) required an adversary to be on the network to exploit them. Dragos found that 108 of these advisories could cause a loss of view and/or control within a compromised environment.

Dragos found 28% of all advisories affecting European systems contained Common Vulnerability Scoring System (CVSS) errors; 17% of all advisories have a public Proof of Concept, and 23% of advisories had no patch. Dragos advises asset owners and operators to be aware of the threats these vulnerabilities pose to operations. A loss of view or control, for instance, may cause safety concerns and potentially put workers' lives or the environment at risk. Corrected advisories, with explanations as warranted, can by accessed by customers through the Dragos WorldView Portal.

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

In April of 2018, the U.K.'s National Cyber Security Centre (NCSC) published an advisory titled *Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices;* victims included industrial infrastructure providers and Internet service providers (ISPs) that support them.[27, 28] Affected systems include Generic Routing Encapsulation (GRE) Enabled Devices, Cisco Smart Install (CSI) enabled devices, and Simple Network Management Protocol (SNMP) enabled devices. The report notes the FBI and the NCSC assessed with high confidence Russian state-sponsored cyber actors were using compromised routers to conduct man-in-the-middle attacks to support espionage, extract intellectual property, maintain persistent access to victim networks, and potentially lay a foundation for future offensive operations. Additionally, access to Enterprise assets may lead to adversary access to the DMZ, which may allow adversaries to gain access to the OT network.[29] On 14 March 2022, security researchers from ESET Research Labs disclosed their discovery of a third wiper malware variant called CaddyWiper.

ANALYST NOTE: In January of 2022, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) published an alert regarding Russian state-sponsored cyber threats to US critical infrastructure.[30] While the alert was limited in scope to the US, based on vulnerabilities noted in the report and previous targeting associated with those vulnerabilities, the targeting of these campaigns is likely broader in scope and may include European Industrial Infrastructure providers.

RANSOMWARE

A common misconception suggests ransomware is solely a threat to IT; however, data from 2021 indicates ransomware is having an increasing impact on operational technology as well. Ransomware can cause OT impacts in four ways. First, in the case of Colonial Pipeline, operators preemptively shut down their operations to prevent enterprise IT ransomware from spreading into OT. This strategy, while causing disruption, preserves OT from potential long-term downtime caused by a successful ransomware infection.

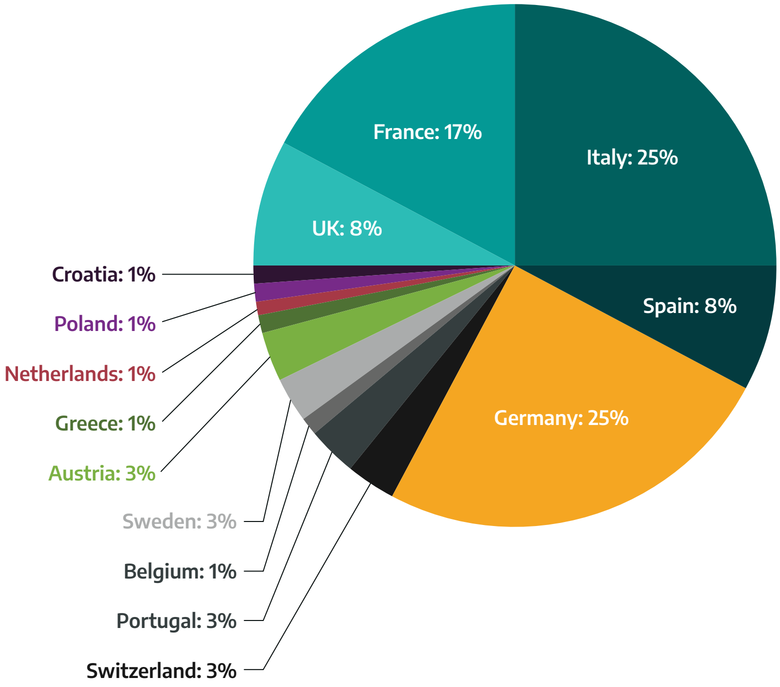
Second, flat networks and lack of asset visibility create an environment where ransomware can spread quickly through both IT and OT networks.[31] Third, Dragos is aware of six ransomware strains that possess built-in OT process kill lists: Cl0p, MegaCortex, Netfilim, LockerGoga, Maze, and EKANS. Finally, ransomware attacks that impact enterprise IT systems only, but lead to the release of proprietary documentation on OT technology on underground forums if the ransom is not paid. This could lead to follow-on attacks targeting OT technology directly by cybercriminals or state-sponsored actors.

Dragos analyzed data from 37 ransomware strains on Dark Web resources leveraged to post victims, leak files, and conduct negotiations. Appearance on a Dark Web resource does not guarantee that ransomware actors successfully compromised a firm, the extent of access achieved by the ransomware actors, or whether a firm made the ransomware payment.

Occasionally, ransomware actors will post inaccurate information on Dark Web resources; for example, listing the name of one firm and the description of a completely different firm. This may be accidental, or an attempt to cause confusion amongst victims. In some cases, ransomware actors will attempt to appear to have compromised a victim by cross-posting documents identified as part of a different ransomware breach, as was the case with Schneider

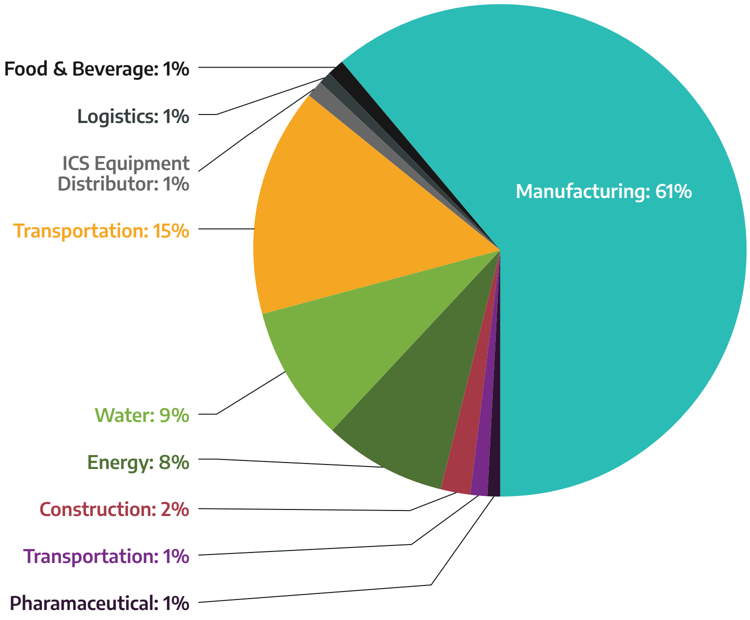
Electric and Vestas.[32] While Dark Web resources are not fully accurate, they provide unique insight into the priorities of ransomware groups, including which sectors and subsectors they most frequently target, which sectors they prioritize, and which areas of the globe are more likely to experience attacks.

RANSOMWARE BY VICTIM LOCATION



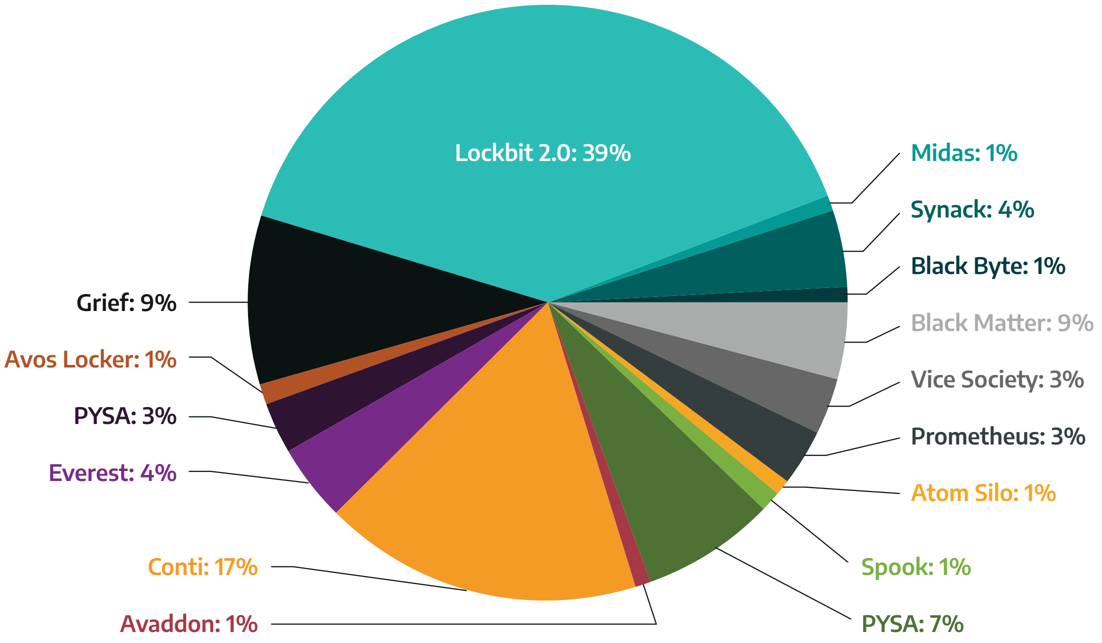
From 1 June to 1 December, victims headquartered in Europe accounted for 26% of Dark Web resource postings. Germany and Italy tied for the largest number of victim postings, with 19 victim firms headquartered in each. Dragos assesses with moderate confidence this is likely due to the high amount of manufacturing in these countries; 26 of the 38 victims, or 68%, were in the manufacturing sector. Comparatively, France had 13 victims across a range of Industrial Infrastructure sectors including Electricity, Food and Beverage, Transportation, and Pharmaceuticals. Spain and the United Kingdom had 6 postings each, respectively.

RANSOMWARE BY ICS VICTIM SECTOR



Overwhelmingly, the majority of ransomware victim postings were in the Manufacturing sector – 48 out of 79. This trend is reflected globally. Additionally, 11 postings involved Transportation firms, 7 included Food and Beverage firms, and 6 included Energy firms.

RANSOMWARE BY GROUP/STRAIN



Of the 79 postings involving European victims, Lockbit made the majority, with 30 victim postings. Conti posted 13 potential victims, Grief posted 7, and PYSA posted 5. In June, Lockbit 2.0 developers launched a Ransomware-as-a-Service (RaaS) program to enable affiliates to leverage the platform to conduct ransomware attacks.[33] The platform uses a double extortion model, where data is exfiltrated prior to systems being locked; if the victim refuses to make a payment, attackers will threaten to leak the exfiltrated data. The affiliates who conducted the attack and the developers of the ransomware split any ransom payments between themselves. Researchers have linked Lockbit to the LockerGoga and MegaCortex ransomware families due to shared tactics, techniques, and procedures, particularly the ability to propagate automatically to new targets.

According to an article published on 4 August, Lockbit is actively recruiting corporate insiders to provide Remote Desktop Protocol (RDP), Virtual Private Network (VPN), and email credentials to assist attackers in gaining access to networks in exchange for million-dollar payouts.[34] Lockbit does not operate in countries that are formerly a part of the Soviet Union. This ransomware group leverages tools such as StealBIT, Metasploit Framework, and Cobalt Strike.[35] In late July, reports emerged indicating researchers had uncovered a new version of the Lockbit 2.0 ransomware platform that automates the encryption of a Windows domain using Active Directory group policies.[36] Dragos assesses with low confidence Lockbit, and subsequent iterations of this ransomware group, will continue to develop innovative techniques to increase potency of ransomware operations.

Conti is also a Ransomware-as-a-Service (RaaS) platform; however, a September report by the Cybersecurity and Infrastructure Security Agency (CISA) notes a variation in its structure as it likely pays deployers a wage rather than a percentage of the profits in the event the ransom is paid.[37] Techniques that Conti uses are not especially unique; for example, they maintain persistence using Cobalt Strike or PowerShell. However, unlike many ransomware groups who focus on building the reputation that victims will receive their files if the ransom is paid, Conti is significantly more volatile, occasionally not returning files after victims pay the ransom or only returning a fraction of compromised files. In August 2021, an alleged Conti affiliate leaked the group's *"playbook"* after apparently not receiving full payment following an attack; researchers who viewed the playbook advised network administrators looking for Conti activity to *"scan for unauthorized Atera Agent applications and Any Desk persistence."*[38] These groups are likely to continue indirectly targeting, and potentially directly impacting, Industrial Infrastructure across Europe.

INTELLECTUAL PROPERTY THEFT

Intellectual Property (IP) theft against global organizations facilitates economic espionage and poses a strategic threat to the global economy and sector stability. Industries and technologies associated with the energy sector, environmental protection, and advanced manufacturing are at greatest risk.[39] In addition to the data transfer associated with foreign direct investment and joint ventures, two primary methods of IP theft include supply chain compromises and insider threats. Stolen data or leaked data and the theft of intellectual property provides insights on how to impact or disrupt industrial operations.

Additionally, attempts at intellectual property theft can go awry, causing extensive damage, as was the case in the 2014 German steel mill explosion. Adversaries connected to KAMACITE were allegedly attempting to steal intellectual property for high tensile lightweight steel; antiquated technology caused components of the plant controls to fail, resulting in an unregulated furnace, which then caused physical damage to the steel plant.[40]

INSIDER THREATS

Dragos assesses with moderate confidence insider threats present a key weakness in the European Industrial Control systems landscape. There are two widely accepted types of insider threat, malicious insiders and negligent insiders. Malicious insiders are those who have access to company systems and wish to cause harm to said company; motivations may include political disagreements, restructuring, lack of growth, etc. Malicious insiders may be detected through patterns of behavior prior to causing impact to operations.

In this sense, negligent insiders are often considered more dangerous. There are many examples of potential negligent insider threats to Industrial Infrastructure and, more specifically, OT. Requirements that engineers use laptops containing overly aggressive security measures that prevent critical job functions could cause engineers to use unsecured devices instead. Many firmware manuals are locked behind a paywall or login, causing employees to use unsecured PDFs instead. Negligent insiders inadvertently allow adversaries into environments that would otherwise be difficult to access due to proper segmentation and conservative architecture.

A 2019 Crowdstrike report revealed extensive collaboration between People's Republic of China (PRC) state-sponsored actors and insiders at aircraft design and manufacturing companies in Europe and North America. According to the report, adversaries conducted espionage with the goal of strengthening Beijing's domestic airline industry by leveraging stolen intellectual property to accelerate development of the C919 aircraft.[41]

Beyond IP theft, insider threats can also cause damaging consequences, including operational losses, environmental harm, reputational effects, and even physical destruction. In 2014, an anonymous malicious insider at a nuclear plant in Brussels caused $100-$200 million in damages by opening a valve, draining lubricant from a turbine and causing it to burn out.[42]

RECOMMENDATION

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

THIRD-PARTY AND SUPPLY CHAIN COMPROMISES

Increasingly, adversaries target industries using an increasingly common and effective method of attack that is difficult to defend against: third-party compromise. This attack vector preys upon implicit trust between companies and suppliers or supporting entities. Organizations in energy, ONG, manufacturing, and logistics are especially at risk because of the variety of security zones and trust relationships.[43]

XENOTIME is one Industrial Infrastructure- robust segtargeting group that attempts to compromise vendors in the ONG and electric sectors, including original equipment manufacturers (OEMs) involved in electric generation and safety systems, hardware manufacturers, software suppliers, and integrators. Dragos is aware of XENOTIME specifically operating against European ICS vendors.[44]

Dragos identified a series of malicious documents targeting Russian state-owned nuclear energy company ROSATOM from early May through June 2020. The documents deployed a credential harvesting mechanism similar to techniques previously observed in DYMALLOY and ALLANITE operations, while the infrastructure used for collection aligns closely with recently observed SANDWORM operations. The nature of ROSATOM and targeting mechanisms indicate a potential interest in the company for OT-specific reasons. Implications range from attempting to gain a foothold in Russian generating assets through potential supply chain possibilities given ROSATOM's export of reactor designs and construction to various other countries.[45]

The French National Agency for the Security of Information Systems (ANSSI) published details on 15 February 2020 of alleged Sandworm activity targeting and exploiting information technology providers leveraging compromised Centreon servers. Centreon is used for monitoring equipment, middleware, and applications. Additionally, Centreon provides plugins for Industrial Infrastructure products and services, enabling asset owners and operators to monitor equipment within the OT with the same monitoring software as the enterprise. An adversary could leverage a network monitoring software compromise to gain access to OT networks, elevate credentials on a compromised device, move laterally within the network, and conduct reconnaissance. Though Dragos cannot definitively attribute the attacks, adversaries used malware in the compromise associated with KAMACITE and ELECTRUM.[46]

RECOMMENDATION

Asset owners and business units should adopt a *"zero trust,"* or work toward a *"trust and always verify,"* mentality with vendors and supply chain managed devices that have direct access to OT environments or credentials to access OT environments from RDP or VPN connections. Zero Trust is a security concept which eliminates the concept of trust from an organization's network architecture to prevent data breaches. This concept leverages network segmentation, prevents lateral movement, and simplifies user-access control at a tactical level.[47]

PREPOSITIONING FOR LATER EFFECTS

Any disruptive or destructive Industrial Infrastructure cyberattack requires an adversary to complete a series of prior steps in the ICS Cyber Kill Chain to achieve their ultimate goal.[48]

An intrusion into an IT or OT environment may not immediately cause or indicate an effects portion of a cyberattack. Adversary dwell time – or the time spent within a target environment before executing an attack – can be months or years within Industrial Infrastructure. In the case of CRASHOVERRIDE, based on available evidence and intelligence that Dragos gathered, ELECTRUM entered the target environment as early as January 2016, possibly through a phishing campaign.[49] The CRASHOVERRIDE attack, which occurred on 17 December 2016, required an intimate knowledge of the target environment to transition from an IT to OT network and a fundamental understanding of OT communications protocols. Long dwell time can enable an adversary to gather intelligence and assess a victim environment to tailor an attack appropriately, while also studying a target's defensive posture and potential for attack obfuscation.

In the case of NorskHydro, the adversary achieved access to systems through business email compromise (BEC) and leveraged dwell time before launching the destructive LockerGoga ransomware attack. Given the initial intrusion method and deployment mechanism at Hydro, attackers would need to first expend effort to identify appropriate customer communication to spoof or modify a document. From there, initial access required pivoting to compromise the Active Directory instance, then stage the LockerGoga malware. While Dragos cannot assign a firm timescale to such an event, the above activity could take weeks or even months, factoring in the work required to enable the initial access mechanism.[50]

RECOMMENDATION

Asset owners and operators should understand the evolution of adversary tradecraft and behavior. Utilizing OT-specific threat intelligence can inform and guide proactive decision-making and ensure defense-in-depth methodologies are implemented across IT and OT. Identifying and alerting on threat behavior patterns in addition to indicators of compromise can help identify initial intrusion and reconnaissance activity before a disruptive attack occurs.[51]

DIGITAL TRANSFORMATION

As more OT systems become internet-or-cloud connected, the traditional OT focus on ensuring high availability with less regard for confidentiality and integrity has evolved. The expanded connectivity increases risk and makes the IT environment a potential attack vector into the OT environment.

One example of this is wormable ransomware attacks that take advantage of Windows vulnerabilities to propagate throughout a network. WannaCry ransomware leveraged this method in 2017, and in a recent security advisory, Microsoft warned of a newly disclosed remote desktop services vulnerability that adversaries could use for a similar attack.[52]

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

In Industrial Infrastructure, system reliability is crucial, and taking machines offline to receive patches means experiencing potential downtime and loss of production, and potentially, revenue. This balancing act often favors foregoing necessary security updates to keep operations up and running. But patches for some vulnerabilities such as Common Vulnerabilities and Exposures (CVE) CVE-2019-0708, or MS17-010,[53] and patches for the remote desktop vulnerability and WannaCry, respectively, are all vital to apply.

RECOMMENDATION

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

OBSERVED ACTIVITY FOLLOWING RUSSIAN INVASION OF UKRAINE

As of early March, Dragos has been monitoring activity potentially related to the Russian invasion of Ukraine:

- On 23 February 2022, security researchers from Symantec Threat Intelligence and ESET Research Labs disclosed their discovery of a new wiper malware variant, which they are calling HermeticWiper. The adversary uses a legitimate code signing certificate to sign the malware binary and abuses a legitimate driver to corrupt data. The security researchers did not disclose any information indicating an explicit impact on industrial companies or OT networks but did note that the wiper was installed on hundreds of machines across multiple countries. Dragos assesses with low confidence the adversary may be positioning to target entities in the electric, water/wastewater, and Oil and Natural Gas (ONG) industries. Dragos assesses with moderate confidence that this new wiper malware variant has the potential to impact OT networks, given the rapid spread of the malware and the indiscriminate nature of wiper attacks.[54]
- On 25 February 2022, the Conti ransomware group announced support for the Russian government on their Dedicated Leak Site (DLS), stating if a cyber attack or other warfare were directed by any entities against Russia they would use *"all possible resources to strike back at the critical infrastructure of an enemy."* Conti later amended the statement to say they *"do not ally with any government and condemn the ongoing war"* but that they would still "use our full capacity to deliver retaliatory measures in case the Western warmongers attempt to target critical infrastructure in Russia or any Russian-speaking region of the world." Dragos assesses with moderate confidence that this has the potential to impact OT networks, based on past ransomware infections resulting in OT impacts and the Conti group's specific reference to critical infrastructure in their original announcement.[55]
- On 27 February 2022, an adversary uploaded a video to the internet demonstrating how to alter a Russian Fornovogas Human Machine Interface (HMI) for a gas compressor. The video demonstrates an unknown operator clicking through menus on the HMI, altering the off-delay time, exiting the HMI software, deleting the profile configuration, and browsing to the host operating system root user configuration directory. Commentary surrounding the video mentions the unknown operator watching the system administrator trying to restore profiles that were no longer available. Dragos assesses with low confidence that industrial companies do not use this gas compressor in large-scale industrial operations and that this will not affect the gas supplies in Russia.[56]
- On 28 February, 2022, around 8:54 UTC, news about alleged cyber-attack on German wind turbines appeared on a social media platform. The message mentioned that a large-scale attack was underway on German wind turbine infrastructure. More specifically, the reference was about the satellite connections, with mention of a non-specified "new firmware update that has destroyed the router." This put the SCADA data of the Wind Turbine Generators (WTG) offline preventing them from being remotely controlled or managed. From our initial analysis, Dragos has not observed this to be a targeted attack against German wind turbine infrastructure. Dragos assesses with moderate confidence the outage of the German wind turbine infrastructure is linked to the Viasat European Network outage that started on the 24th of February.[57]
- On 02 March 2022, the hacktivist group, "Belarusian Cyber Partisans", announced they had successfully compromised the network infrastructure of the Belarusian Railway. The hacktivist group claimed that the compromise had affected the GUID system (online train schedule), the manager's notebook, the subscriber stations, and the automated dispatcher systems. Dragos Intelligence has not directly observed the compromise or incident data against the network infrastructure of the Belarusian Railway.[58]

- On 14 March 2022, security researchers from ESET Research Labs disclosed their discovery of a third wiper malware variant called CaddyWiper.
- On 24 March 2022, the Cybersecurity and Infrastructure Security Agency (CISA) released an alert on adversary employed Tactics, Techniques, and Procedures (TTPs) that CISA assessed to be Russian sponsored.[59] CISA issued this alert jointly with Federal Bureau of Investigation (FBI) and Department of Energy (DoE), after the U.S. Department of Justice (DoJ) issued an indictment earlier in the day against four Russian government employees alleged to be responsible for two historical hacking campaigns targeting "critical infrastructure" worldwide.
  - The DOJ described activity in the indictment maintains technical overlaps to Dragos-tracked Activity Groups (AGs) such as, XENOTIME, DYMALLOY, and ALLANITE. Dragos assesses with high confidence that these activity groups continue to pose a real and significant threat to industrial infrastructure and defenders should exercise increased vigilance given current geopolitical factors.[60]
  - Even considering that context, availability constraints and related considerations inherent to operational technology (OT) networks make portions of the mitigation guidance from the CISA alert impractical and in some cases potentially dangerous.

DEFENSIVE RECOMMENDATIONS

INITIAL INTRUSION DEFENSE RECOMMENDATIONS

- Identify vulnerabilities and known exploits related to the environment. Remediate vulnerabilities and monitor for attempts to leverage them. Specifically, scan exposed VPN appliances from the Internet. Make sure appliances are up to date, not vulnerable to known exploitable vulnerabilities, such as CVE-2019-11510, CVE-2019-1579, CVE-2018-13379, or CVE-2019-19781.
- After updating, change account credentials and generate new VPN keys and certificates.
- Enable logging to track VPN activity to identify and monitor access and audit access regularly.
- VPN technology should provide access to business resources, DMZ, and not directly to OT environments without additional steps such as MFA (Multi-Factor Authentication) and jump hosts, etc. Perform architecture review if access and network topologyis unknown.
- Monitor for brute force techniques on service accounts and domain administrators. Separate business AD (Active Directory) infrastructure from OT infrastructure.
- Perform reconnaissance against the business organization and identify potential targeted phishing campaigns.
- Utilize intelligence sources to identify phishing infrastructure and watering holes with ICS-themed websites.
- View emails in plain text only (do not render HTML) and disable Microsoft Office macros. Monitor for malicious VBA macros and PowerShell via phishing documents.

NETWORK ACCESS DEFENSIVE RECOMMENDATIONS

- Monitor for use of open-source tools that have been leveraged against industrial entities such as SSH.NET, MASSCAN, dsniff, Impacket, and TUNNA within the environment.
- Leverage intelligence sources to identify and track emerging threats and active and current tooling.

- Use consequence-driven, Crown Jewel Analysis Model to identify risks to industrial processes. Focus on critical operational systems, such as Safety Instrumented Systems and monitor access and communication to these systems.
- Perform an architecture review for routing protocols between operational technology and outside networks.
- Identify where and how IEC104, IEC61850, DNP3, and OPC protocols are used within critical infrastructure. stablish baselines of normal operations and monitor for changes to that baseline.
- Monitor for credential compromise and re-use activity within the environment. Monitor for newly established SMB sessions to external resources.
- Implement MFA to remotely access systems within the OT network.
- Utilize intelligence sources to identify and track communication to C2 infrastructure.
- Monitor for Cobalt Strike payloads and communication to known C2 servers.

HOST-BASED DEFENSIVE RECOMMENDATIONS

- Monitor for malicious PowerShell, Windows Management Instrumentation (WMI), and Python activity on engineering workstations and other Windows hosts within OT environment.
- Do not execute code from unsigned, or untrusted binaries. Prevent or flag and review execution of new and unsigned binaries.
- Monitor for malicious HTA payloads that lead to PowerShell execution on Windows hosts in the operational environment, especially HMIs and EWS.
- Monitor for Windows registry keys that write an executable to %PROGRAMDATA% or add files to run on system start.
- Monitor for use of credential stealing tools such as mimikatz.
- Monitor for unusual enumeration and use of system tools such as systeminfo, tasklist, netstat, dir to name a few.
- Establish a baseline network configuration and communication for normal operations and identify changes, unknown, or malicious behaviour.
- Monitor and investigate new services and scheduled tasks on hosts. Establish a known-good list of services and scheduled tasks as a baseline.

REFERENCES

1 Industrial infrastructure refers to all industrial operations which provide necessary functions to support humanitarian, economic, and other civil functions including elements such as food production,water and wastewater management, energy production, transportation, etc. This helps differentiate industrial operations from what is traditionally overly generalized and ambiguously described as 'critical infrastructure.'

2 AG-2019-04: PARISITE – Dragos WorldView Intelligence

3 European Oil and Gas Threat Perspective – Dragos

4 AA-2022-02: LNG-focused XENOTIME Research and Reconnaissance - Dragos

5 TR-2020-04: Possible MAGNALLIUM Activity – Dragos

6 MAGNALLIUM – Dragos

7 APT33 – MITRE ATT&CK

8 DYMALLOY – Dragos

9 TR-2019-18: Activity Group Watering Hole Attacks – Dragos

10 Group: Dragonfly 2.0, Berserk Bear, DYMALLOY Beserk Bear – MITRE ATT&CK

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

12 TR-2020-14: Possible ELECTRUM Related Activity – Dragos

13 Sandworm Team - MITRE ATT&CK

14 TR-2020-27: Analysis of Possible ALLANITE Activity in Germany – Dragos

15 ALLANITE – Dragos

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

17 CHRYSENE – Dragos

18 OilRig – MITRE ATT&CK

19 KAMACITE - Dragos

20 COVELLITE - Dragos

21 TR-2020-19: LAZARUS-Linked Activity Targeting the Aerospace Sector – Dragos

22 AA-2020-33 Chinese-Related Network Intrusion Activity and Links to VANADINITE – Dragos

23 VANADINITE - Dragos

24 Industrial Production Statistics – Eurostat

25 2021 ICS Cybersecurity Year In Review – Dragos

26 Great Britain Power System Disruption – 9 August 2019 – Department for Business, Energy, and Industrial Strategy

27 DHS and FBI Issue a Joint Technical Alert with UK Warning Russian State-Sponsored Cyber Attacks – Alston & Bird

28 Russian state-sponsored cyber actors targeting network infrastructure devices – National Cyber Security Centre

29 TRISIS Malware – Dragos

30 Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure – CISA

31 Flat networks are defined here as lack of discrete separation of industrial operations and non-operational technology which may be evidenced by the lack of use of the Purdue model.

32 AA-2021-32: Schneider Electric Appears as Victim on Lockbit 2.0 Ransomware Leak Site- UPDATE – Dragos

33 The Rising Threat from LockBit Ransomware – CyberEason

34 LockBit ransomware recruiting insiders to breach corporate networks – Bleeping Computer

35 LockBIT 2.0 Ransomware – Cyble

36 LockBit ransomware now encrypts Windows domains using group policies – Bleeping Computer

37 Conti Ransomware – CISA

38 Angry Affiliate Leaks Conti Ransomware Gang Playbook – Threatpost

39 2018 Foreign Economic Espionage In Cyberspace – The National Counterintelligence and Security Center

40 German Steel Plant Suffers Significant Damage from Targeted Attack – Trend Micro

41 Report: Underground Hackers and Spies Helped China Steal Jet Secrets – Rollcall

42 Brussels Attacks Stoke Fears About Security of Belgian Nuclear Facilities – Washington Post

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

44 Year in Review 2018 – Dragos

45 TR-2020-35: Initial Access Activity Targeting Russian Nuclear Industry – Dragos

46 AA-2021-03: Centreon Monitoring Software Exploited – Dragos

47 Achieving Manageable Zero Trust for OT Networks – Dragos

48 The Industrial Control System Cyber Kill Chain – SANS

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

50 TR-2019-30: Revisiting LockerGoga - Dragos

51 Why You Need OT Specific Threat Intelligence – Dragos

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

53 Microsoft Security Bulletin MS17-010 – Critical – Microsoft

54 5AA-2022-06: Security Researchers Disclose Wiper Malware Targeting Ukrainian Entities – Dragos

55 AA-2022-07: Conti Threatens Western Critical Infrastructure – Dragos

56 AA-2022-11: Video Demonstrating the Altering of a Russian HMI Uploaded to the Internet - Dragos

57 AA-2022-09: German Wind Generation Disruption – Dragos

58 AA-2022-12: Belarusian Railway Network Infrastructure Compromised - Dragos

59 Tactics, Techniques, and Procedures of Indicted State-Sponsored Russian Cyber Actors Targeting the Energy Sector – CISA

60 AA-2022-20: CISA Alert on Indicted State-Sponsored Russian Adversaries

ABOUT DRAGOS, INC.

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

Dragos codifies the knowledge of our cybersecurity experts into an integrated software platform that provides customers critical visibility into ICS and OT networks so that threats and vulnerabilities are identified and can be addressed before they become significant events. Our solutions protect organizations across a range of industries, including power and water utilities,energy, and manufacturing, and are optimized for emerging applications like the Industrial Internet of Things (IIoT).

Dragos is privately held and headquartered in the Washington, DC area with regional presence around the world, including Canada, Australia, New Zealand, Europe, and the Middle East.

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

TAGS:

Europe,
Oil and Natural Gas, Electric,
Ransomware,
Manufacturing,
United Kingdom,
Germany, Italy,
Austria