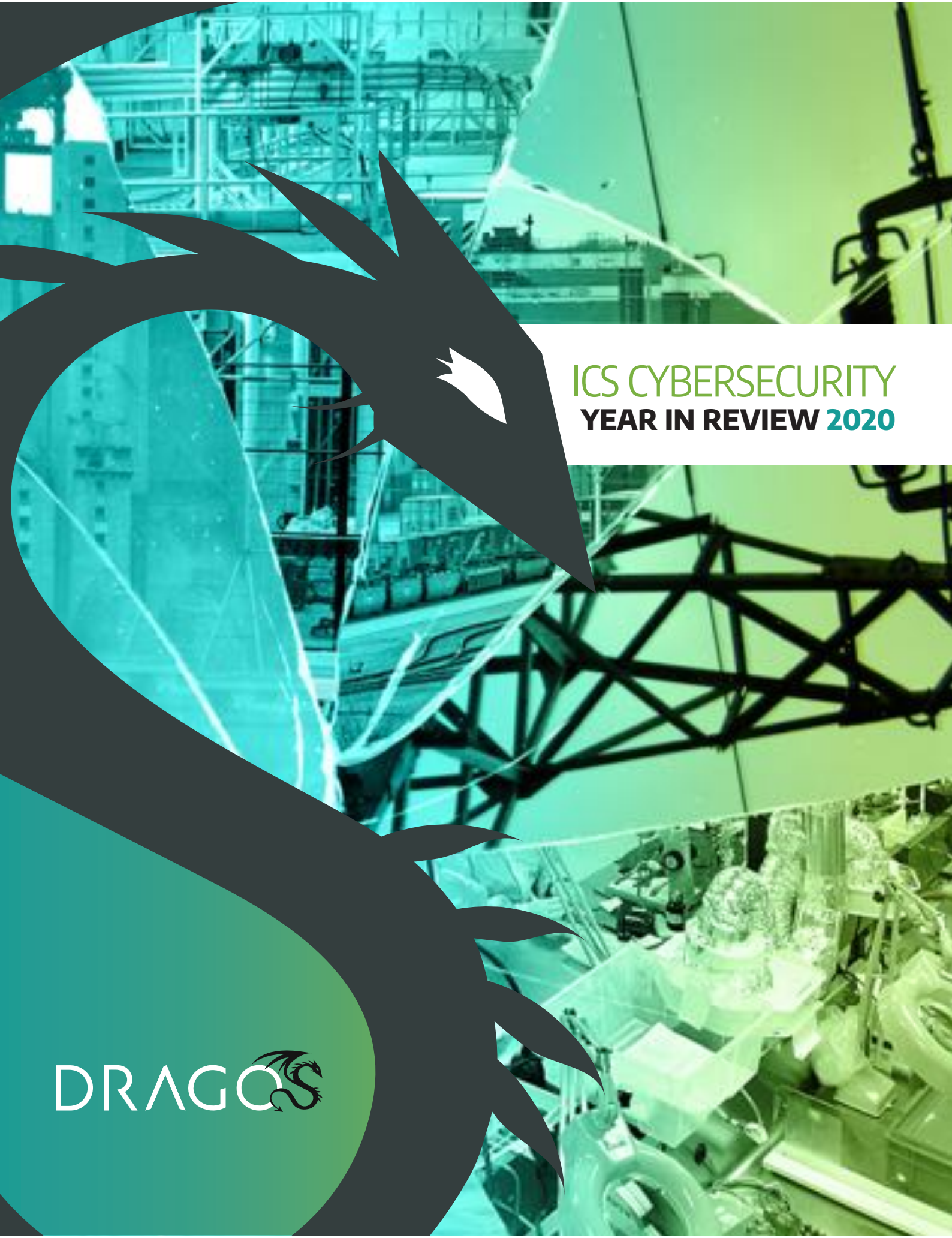


ICS CYBERSECURITY
YEAR IN REVIEW 2020

DRAGOS

Contents

INTRODUCTION

The Dragos Year in Review report is an annual analysis of Industrial Control System (ICS)/Operational Technology (OT) focused cyber threats, vulnerabilities, assessments, and incident response insights.[1] The ICS/OT community has long suffered from a lack of public insights into these types of problem areas to have a meaningful discussion on how to address the issues. It is the Dragos team's goal to share the observations and lessons learned with the industrial community for data-driven analysis and recommendations.

In 2020, the industrial community performed amazing feats to keep civilization running under extremely challenging circumstances with the global pandemic. Infrastructure providers kept key services and goods available including electric power, manufactured goods, water, oil and gas, mining, chemical, rail, and transport while many faced hardships globally. As a result of these efforts, organizations shifted in how they conducted business to include an increasingly connected industrial environment. This is a trend that has existed for many years, even while many organizations still believed they had highly segmented or even air-gapped ICS networks. The risk to ICS is not born from an IT and OT convergence, but instead from a convergence of an increasingly ICS-aware and capable threat landscape with the digital transformation and hyperconnectivity of the industrial community. This report captures how some of the community is performing and progressing, and areas of improvement that will be needed to continue to provide safe and reliable operations.

[1] The terms "ICS" and "OT" will be used interchangeably for the purpose of this report. These terms are used differently in different communities.

KEY HIGHLIGHTS

Four new threat groups with the assessed motivation of targeting ICS/OT were discovered, accounting for a **36% increase** in known groups.

The abuse of valid accounts was the **number one technique** used by named threats.

SERVICE ENGAGEMENT FINDINGS

90% of service engagements included a finding around lack of visibility across OT networks.

54% of service engagements included a finding about shared credentials in OT systems.

88% of service engagements included a finding about improper network segmentation.

VULNERABILITY ADVISORY FINDINGS

43% of ICS vulnerability advisories contained errors that would make it difficult to prioritize mitigations.

64% of advisories that had no patch also had no practical mitigation advice provided by the vendor.

61% of advisories that had a patch did not have any alternate mitigation advice provided by the vendor except for applying the patch, which in many industrial organizations can be difficult or significantly delayed.

IN THE HEADLINES

MITRE ATT&CK for ICS

MITRE introduced ATT&CK for ICS in 2020 to codify and communicate the unique threat behaviors, or Tactics, Techniques, and Procedures (TTPs), that ICS adversaries use against OT targets. This independent and community-sourced framework provides a common lexicon for categorizing ICS-specific TTPs to support reporting and further analysis. Dragos uses the framework internally and continues to contribute to this program and community resource. The Year in Review report leverages information from MITRE ATT&CK about observed activity in ICS environments to help defenders mitigate threats to their organizations.

RIPPLE20, AMNESIA:33

Third-party code integration can pose risks to industrial operations. Many vendors do not track third-party code libraries, and therefore cannot accurately inform customers if their products are impacted. Vendors are beholden to software manufacturers to release fixes for vulnerabilities that may impact thousands of products. For example, security researchers disclosed multiple vulnerabilities in TCP/IP software libraries called Ripple20[2] and AMNESIA:33[3] that potentially impacted many ICS vendors. Example ICS devices impacted include Programmable Logic Controllers (PLCs), Serial to Ethernet Converters, Protocol Converters, Remote Terminal Units (RTUs), digital protective relays, and some managed network switches and routers. Most of the devices impacted by the vulnerabilities were not accurately identified and did not have advisories released due to the difficulty in understanding third-party code adoption. Security design flaws in the impacted devices may make this collection of flaws less relevant to adversaries, but the disclosure highlights supply chain risks and complexity.

EKANS

EKANS represents a specific threat to ICS because of its incorporation of potential process and operational disruption features. This ransomware is capable of stopping ICS-related Windows processes before initiating encryption. EKANS activity could produce an unstable or physically disruptive situation by abruptly ending an operationally significant process. The Dragos Intelligence team assesses EKANS is related to a previous strain of ransomware called MEGACORTEX. Throughout 2020, Dragos identified new EKANS activity targeting multiple verticals including electric, oil and gas, medical, pharmaceutical manufacturing, and automotive. Public targets included Fresenius Kabi, a pharmaceutical division of the European company Fresenius Group; global manufacturer Honda; and Italian energy company Enel.

[2] https://www.jsof-tech.com/disclosures/ripple20/;
[3] https://www.forescout.com/research-labs/amnesia33/

IN THE HEADLINES

GLOBAL SUPPLY CHAIN COMPROMISE

Multiple ICS entities were impacted by a massive supply chain compromise first revealed in December 2020.[4] Adversaries compromised SolarWinds Orion business software to distribute malware. The adversary had unfettered access for more than 14 months and is thought to now have access to other supply chain access points throughout the community.

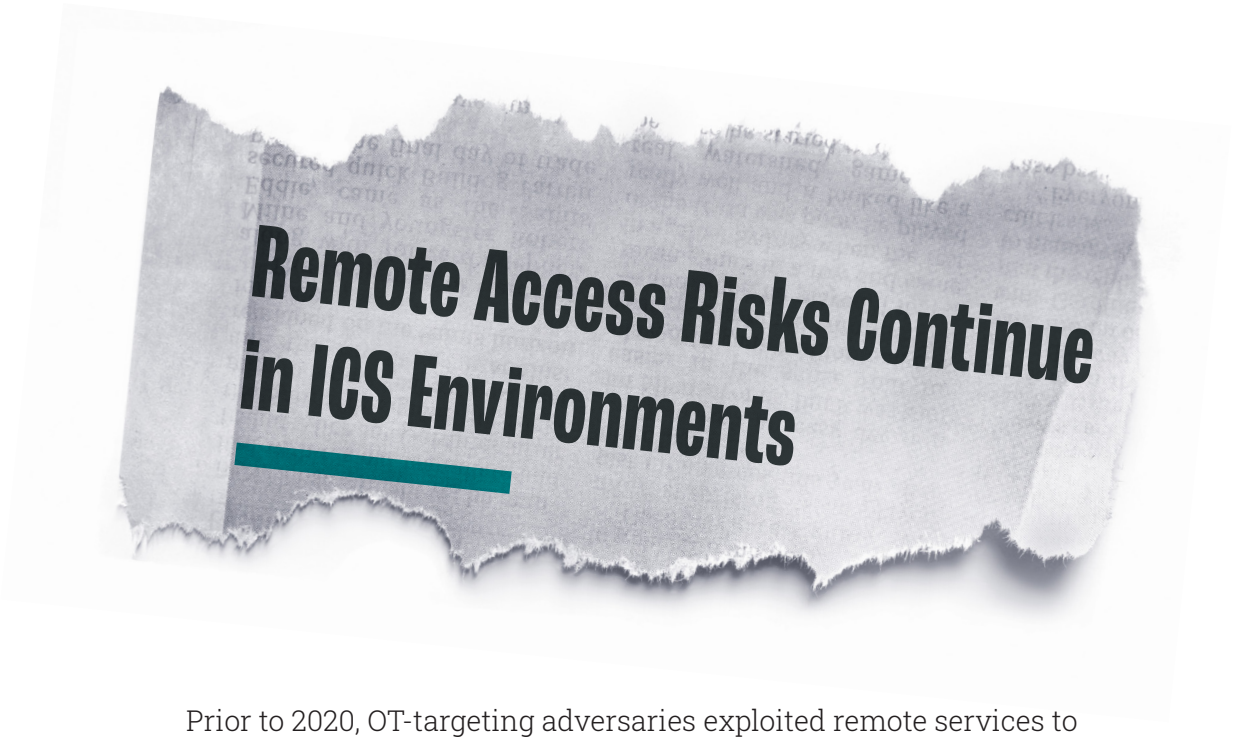
Identifying SolarWinds in ICS environments was challenging. To respond appropriately, facilities required accurate asset lists, software version information, and network monitoring to identity post-exploitation activity. Dragos investigated numerous confirmed compromises. The investigations reverted to limited host-based analysis and could only capture days or weeks in analysis. In an ICS network where not all endpoints can have robust host logging and in compromises where adversaries leverage the network extensively, it is preferred to have network traffic analysis and logging. Given the current lack of visibility in industrial networks the assessment of SolarWinds' compromise impact is likely to not be fully understood for years.

In some cases plant personnel purchased SolarWinds directly, and organizations were unaware they had it in their environments. More commonly though, many integrators, support contracts, and ICS suppliers use software, including SolarWinds, as white-labeled solutions. This means the product is in place but under a different name. Suppliers may use the software themselves on behalf of the client where the compromised SolarWinds software was not in the end-users ICS network. The software may have been present in the supplier or integrator's network and used in the end-user's networks across direct connections or maintenance links. SolarWinds often has access directly to the control level in ICS networks which would allow an adversary to not only have access to these environments, but direct control of them. Many organizations that did not believe they were impacted were compromised directly or accessed from compromised networks due to third-parties.

Dragos is aware of at least two global ICS Original Equipment Manufacturers (OEMs) that were using the compromised SolarWinds software across maintenance links into ICS networks, including where there was turbine control software.[5]

[4] https://www.dragos.com/blog/industry-news/responding-to-solarwinds-compromise-in-industrial-environments/;
[5] Dragos attempted to inform both OEMs and eventually leveraged government organizations to ensure that the risk was understood.

IN THE HEADLINES



Prior to 2020, OT-targeting adversaries exploited remote services to compromise ICS environments. This technique gained popularity as the COVID-19 pandemic spread globally. Companies began requiring some workers to remain at home in 2020, even those working in industrial environments. Multiple ICS-targeting threat groups historically targeted remote access technologies or logon infrastructure including PARISITE, MAGNALLIUM, ALLANITE, and XENOTIME. This includes compromise of Remote Desktop Protocol (RDP) and Virtual Private Network (VPN) assets. VPN equipment is a common access point for OEMs and integrators to gain access to operations environments. Although many organizations focus on prevention and segmentation, obtaining access through a compromised VPN may allow an adversary into an ICS network with limited detection capabilities. For example, in 2019 the Dragos team reported on the threat group PARISITE noting it was the access operations team for the MAGNALLIUM group and explicitly targeted OT boundary equipment, such as VPNs, for the likely purpose of gaining access to ICS networks.

SECTION ONE

ICS Threat Landscape

INTRODUCTION

Cyber risk to industrial sectors has grown and accelerated dramatically, led by ransomware impacting industrial processes, intrusions enabling information gathering and process information theft, and new activity from adversaries targeting ICS. Dragos emphasizes the importance of understanding how adversaries steal information and gain access to better prepare for adversary behavior in the future. Adversaries often build programs and campaigns slowly over time, with later campaigns often being more successful and disruptive due to previous efforts.

Some threats tracked by Dragos may proliferate into disruptive and destructive capabilities later, though no such activity is observed at this time. For example, the team would track a threat that was explicitly targeting electric companies with theming toward engineers, engineering projects, or electric operations, though there may be limited or no visibility to confirm if the adversary gained access to ICS networks. The team would not track a threat if it was simply trying to gain access to an electric company. The fundamental assessment of threats tracked by Dragos is that they are explicitly trying to gain access to ICS networks and operations or are successful in achieving access.

These types of events, where adversaries gain access to ICS networks but do not have the intention of currently disrupting them, are much more common than is publicly reported. The threats are learning ICS. Although not every compromise will relate to an impact today, many may inform the attacks of the future. Dragos tracks 15 threat Activity Groups, or threat groups,[6] with four of the groups discovered in 2020. Threats are growing at a rate **three times faster** than they are going dormant.[7] This is likely due to the increased investment made by adversaries in targeting ICS over the last five to 10 years, and whose investment will continue to accelerate the ICS threat environment.

MAJOR ICS THREAT TRENDS IN 2020

- ICS THREAT ACTIVITY GROUPS INCREASE SIGNIFICANTLY
- PHISHING CONTINUES TO ENABLE ICS INTRUSIONS
- REMOTE ACCESS DIRECTLY TO ICS LEVERAGED OFTEN BY THREATS
- THE BEGINNING OF RANSOMWARE SPECIFICALLY TARGETING ICS
- SUPPLY CHAIN CONCERNS AMPLIFIED BY LIMITED VISIBILITY IN ICS

[6] Organizations track threats in unique ways. At Dragos, analysts utilize the Diamond Model for Intrusion Analysis, which is a common and industry accepted methodology to cluster intrusions into groups representing teams of adversaries that operate in similar ways. The Diamond Model is an open and well-documented framework that allows for transparency in how this analysis is conducted. https://www.activeresponse.org/wp-content/uploads/2013/07/diamond.pdf

[7] Every year feels like the headlines are, "Threats are Getting Worse," or "Risk is Increasing." A useful way to track the evolution of the threat landscape is to determine how many new threat groups are identified compared to how many are going dormant. Groups that are not observed performing new intrusions within a 12-month period are moved to a dormant phase. Typically the growth rate would be less than two groups being created for every group that goes dormant.

Key Updates on Existing Activity Groups

Throughout 2020, the 11 Activity Groups identified prior to 2020 remained active against industrial organizations. While already covered in previous Year in Review reports, the following key activities occurred in 2020 that are worth noting:

In March, **PARISITE** leveraged Citrix vulnerability CVE-2019-19781 in intrusions targeting North American electric and oil and gas entities. This was concerning given that PARISITE conducts initial access operations potentially enabling future disruptive operations associated with **MAGNALLIUM**. This exemplifies the critical need to track any groups interested in ICS through IT networks. In one example, Dragos responded to an incident where PARISITE was identified internal to the organization before MAGNALLIUM could act. Intelligence-informed decisions can and have helped organizations prioritize efforts successfully.

In April, new DTrack malware emerged with the ability to communicate with Fujitsu Systemwalker management software utilized in distributed computing and data center management operations. Dragos associated this activity with the energy-targeting group **WASSONITE**. Interaction with this type of software can significantly impact data center and computational environments resulting in potential ICS or broader operational impacts.

ALLANITE and **DYMALLOY** remain critical threats to infrastructure operations, especially in Europe and North America. In May, Dragos observed ALLANITE conducting credential harvesting via watering hole attacks. This was followed by use of captured credentials and built-in system tools to launch intrusions into the German electric system, and potentially water and wastewater sectors. ALLANITE and DYMALLOY continued to target multiple United States (U.S.) industrial entities from September through October 2020. Operations included use of ZeroLogon to further intrusions into victim networks. **CHRYSENE** showed continued activity with further malware development and used new tools to infiltrate ICS networks in the Middle East for intelligence gathering purposes.

2020's New Activity Groups

STIBNITE

TALONITE

KAMACITE

VANADINITE

STIBNITE

STIBNITE specifically targets wind turbine companies that generate electric power in Azerbaijan. Based on current collection efforts, the activity appears confined exclusively to Azerbaijan. There is ongoing kinetic conflict in the region between Azerbaijan and Armenia due to rights to disputed territory. Historically when there is regional conflict between states, there tends to be targeting of critical infrastructure, including electric operations. There is only a loose correlation between the conflict and STIBNITE operations, and the Dragos team is not making an assessment on who may be responsible for the targeting.[8] Given the specific targeting and the regional conflict, it is a situation and threat group worth watching closely.

STIBNITE's victims share unique technology with wind farms in Ukraine. One possibility for the specific victim targeting is that adversaries targeted the supplier and maintainer for the wind farm itself. The supplier, operator, and maintainer are all based in Ukraine.

STIBNITE used shared Command and Control (C2) infrastructure between multiple intrusions in late 2020 and updated its malware capabilities to avoid detection after public reports on its activity were released. STIBNITE uses PoetRAT remote access malware in its intrusion operations to gather information, take screenshots, transfer files, and execute commands on victim systems. STIBNITE gains initial access via credential theft websites spoofing Azerbaijan government organizations and phishing campaigns using variants of malicious Microsoft Office documents. STIBNITE also used information related to the global COVID-19 pandemic for malicious document themes.

Target Geography

Victimology

Malware
PoetRAT

STIBNITE TTPs from MITRE ATT&CK

INITIAL ACCESS
- T0865 Spearphishing
- T0817 Drive-by Compromise

PERSISTENCE
- T0859 Valid Accounts
- T1050 New Service

LATERAL MOVEMENT
- T0859 Valid Accounts

COMMAND & CONTROL
- T0869 Standard Application Layer Protocol

ICS Enterprise

[8] https://www.wsj.com/articles/armenia-azerbaijan-conflict-11601325097

Ta TALONITE

TALONITE's operations focus on near exclusive interest in initial access compromises in the U.S. electric sector. The group uses phishing techniques to deliver either malicious documents or executables. TALONITE uses two custom malware families known as LookBack and FlowCloud for information gathering operations.[9]

TALONITE's phishing campaigns utilize electric and power grid engineering-specific themes and concepts, indicating an intent to gain a foothold within energy sector entities. Such access could facilitate gathering host and identity information, collecting sensitive operational data, or mapping the enterprise environment to identify points of contact with ICS. The identified infrastructure and phishing emails spoofed the National Council of Examiners for Engineering and Surveying (NCEES), North American Electric Reliability Corporation (NERC), the American Society of Civil Engineers (ASCE), and Global Energy Certification (GEC).

TALONITE employs malware using legitimate binaries maliciously, or modifies such binaries to include additional functionality. For example, LookBack malware contains persistence mechanisms that add two Windows registry keys to execute legitimate but modified files when the infected user next logs in. FlowCloud launches a renamed copy of the legitimate HTML Help Workshop (hhw.exe) utility from Microsoft. The group uses a combination of owned and compromised network infrastructure.

[9] For more public information on these malware families reference Proofpoint's reporting here: https://www.proofpoint.com/us/threat-insight/post/lookback-malware-targets-united-states-utilities-sector-phishing-attacks

Target Geography

Victimology

Infrastructure

Appears to be shared or reused through the overlapping LookBack and FlowCloud campaigns

TALONITE TTPs from MITRE ATT&CK

INITIAL ACCESS
- T0865 Spearphishing Attachment

EXECUTION
- T1106 Native API

PERSISTENCE
- T1078 Valid Accounts

DISCOVERY
- T1046 Network Scanning Service

LATERAL MOVEMENT
- T1078 Valid Accounts

COLLECTION
- T1113 Screen Capture
- T1005 Data from Local System

COMMAND & CONTROL
- T1090 Proxy

ICS Enterprise

KAMACITE

In 2020, **KAMACITE** targeted U.S. energy companies by leveraging stolen credentials or brute force logons of remote services to access victim networks. Dragos tracks KAMACITE as a significant threat to industrial operations because of strong overlaps between KAMACITE and the Sandworm group, which enabled a disruptive cyberattack to electric operations in Ukraine.

Sandworm is a group tracked by FireEye analysts covering a wide variety of ICS and non-ICS specific targeting. KAMACITE represents the specific, ICS-targeting access enablement component observed by Dragos. KAMACITE also represents a long-running set of related behaviors targeting critical infrastructure and industrial verticals. KAMACITE is a unique group due to new intrusions and evolution in tradecraft distinct from original Sandworm activity.[10]

Dragos assesses KAMACITE is an access-enablement team that operates to support other teams conducting disruptive and destructive effects.[11] Previously, Dragos identified ELECTRUM as the group responsible for the Ukraine 2016 electric transmission substation cyberattack. The important distinction is that in Dragos's analysis, KAMACITE conducted the access operations, enabling ELECTRUM to create and use CRASHOVERRIDE malware to carry out the attack. Dragos determined this based on behavioral differentiations from ELECTRUM activity and earlier access operations demonstrating two distinct groups of activity.

In 2020, KAMACITE was observed performing reconnaissance against numerous energy companies in the U.S. Following its reconnaissance, it attempted to take advantage of webmail of those companies and cloud-based logon services including Microsoft Active Directory (AD) and Office 365 services. In addition to this activity, Dragos verified Server Message Block (SMB) (TCP 445) connections from KAMACITE infrastructure to victims that could indicate some successful access attempts. The precise nature of this connectivity is unknown.

[10] It is common for the information security community to look at threat group names as names, when in reality they are definitions. Sandworm is tracked by FireEye. While links can be seen to others' groups, the definition, collection efforts, and analysis of the FireEye analysts are distinct from those at Dragos and proprietary. Dragos decided to start tracking KAMACITE, associated with a link to Sandworm, upon new activity and unique collection emerging in 2020. [11] Dragos has unique visibility and tracks intrusions that are still active as of this past year. Dragos tracks KAMACITE separately from Sandworm activity. Dragos is not attempting to rename Sandworm, but is merely organizing the ICS activity explicitly to support the development of defenses against this group.

Target Geography

Victimology

Major Incidents
BE2, BE3, CRASHOVERRIDE

Links
SANDWORM, ELECTRUM

KAMACITE TTPs from MITRE ATT&CK

INITIAL ACCESS
- T1190 Exploit Public Facing Application
- T0866 Exploitation of Remote Services

EXECUTION
- T0853 Scripting
- T0807 Command-Line Interface

PERSISTENCE
- T1078 Valid Accounts

DISCOVERY
- T0840 Network Connection Enumeration
- T0846 Remote System Discovery

LATERAL MOVEMENT
- T1078 Valid Accounts
- T0866 Exploitation of Remote Services

COMMAND & CONTROL
- T0885 Commonly Used Ports
- T0884 Connection Proxies

ICS Enterprise

VANADINITE

VANADINITE conducted various initial access operations targeting industrial entities across the energy, manufacturing, and transportation sectors in North America, Europe, Australia, and Asia. Dragos assesses this group's activity is focused on information gathering operations, including specifically ICS compromise and data theft. Obtaining documents and intellectual property relating to ICS processes, function, and design could enable this group's sponsor entity to develop ICS capabilities. VANADINITE's activity supports long-term strategic advances rather than disruptive or destructive effects. Dragos assesses with low confidence VANADINITE is responsible for the ColdLock ransomware attack that targeted Taiwanese state-owned ICS companies and caused indirect disruption to operations. The objective of this attack — whether financial gain or disruptive messaging — is unclear.

Dragos consistently observed a pattern in VANADINITE behavior, including the targeting of recently disclosed "n+1" vulnerabilities in a range of networking and gateway devices impacting remote access services like VPNs. Asset owners and operators should treat vulnerabilities in external-facing network appliances as a serious issue. Dragos observed multiple entities, including PARISITE, increasingly adopt this methodology. These remote access technologies often directly enable access to ICS networks bypassing enterprise networks and are commonly used by integrators and ICS OEMs.

Target Geography

North America, Europe, Asia, Australia

Victimology

Links

Winnti, LEAD

VANADINITE TTPs from MITRE ATT&CK

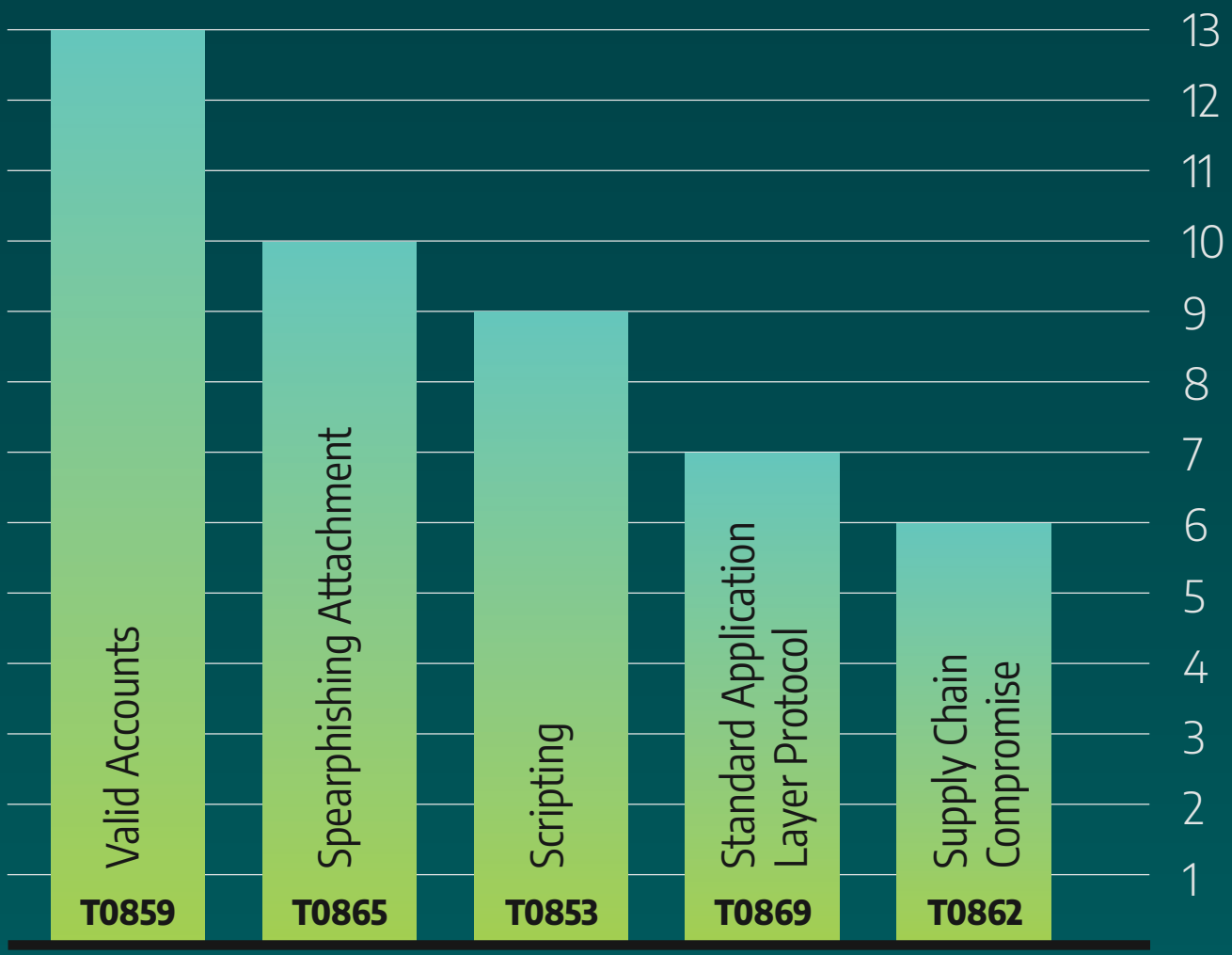
INITIAL ACCESS	
T1190	Exploit Public Facing Infrastructure
T1133	External Remote Services
T1110	Brute Force
T1555	Credentials from Password Stores
T1003	Operating System Credential Dumping
T1111	Two-Factor Authentication Interception
EXECUTION	
T1059	Command and Scripting Interpreter
T1047	Windows Management Instrumentation
PERSISTENCE	
T1133	External Remote Services
T1078	Valid Accounts
LATERAL MOVEMENT	
T1078	Valid Accounts

ICS Enterprise

Most Common TTPs Across All Industries

The following chart demonstrates how many of the 15 Activity Groups Dragos tracks leverage a specific MITRE ATT&CK for ICS TTP. As shown below, Valid Accounts usage is the most common TTP among the groups.

Top Activity Group 5 TTPs



SECTION TWO

ICS Vulnerabilities

INTRODUCTION

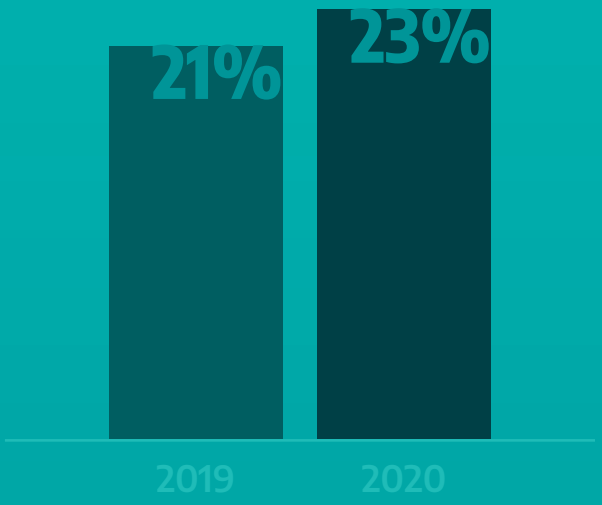
Dragos researchers analyzed 703 ICS/OT vulnerabilities in 2020. For each vulnerability, Dragos independently assesses and confirms – and often corrects – the advisories describing flaws in firmware or software. The vulnerabilities Dragos analyzes are identified by independent security researchers, the Department of Homeland Security's ICS-Computer Emergency Readiness Team (CERT), vendors, and Dragos analysts.

Dragos analyzed 29 percent more vulnerabilities in 2020 than 2019, demonstrating a rise in publicly known flaws in systems supporting industrial operations. Of individually reviewed vulnerabilities, 33 percent contained errors in the Common Vulnerability Scoring System (CVSS) score, potentially impacting patching decisions made by asset owners and operators. Over one-third of vulnerabilities could cause a loss of view and control if exploited by an adversary. Public Proof of Concepts (POCs) were available for 30 vulnerabilities reviewed by Dragos, meaning available resources indicated specifically how an adversary could operationalize the flaw.

2020 Vulnerability Details

Twenty-three percent of vulnerabilities Dragos analyzed applied to products bordering the enterprise. This can include networking communication equipment, VPNs, data historians, or firewalls commonly deployed in ICS networks. This number is up from 21 percent in 2019. ICS-targeting adversaries, including VANADINITE and PARISITE, have historically leveraged such vulnerabilities for initial access to target environments and pose a risk to industrial operators. These vulnerabilities are of particular interest, as they can provide immediate access to the ICS networks bypassing enterprise security controls.

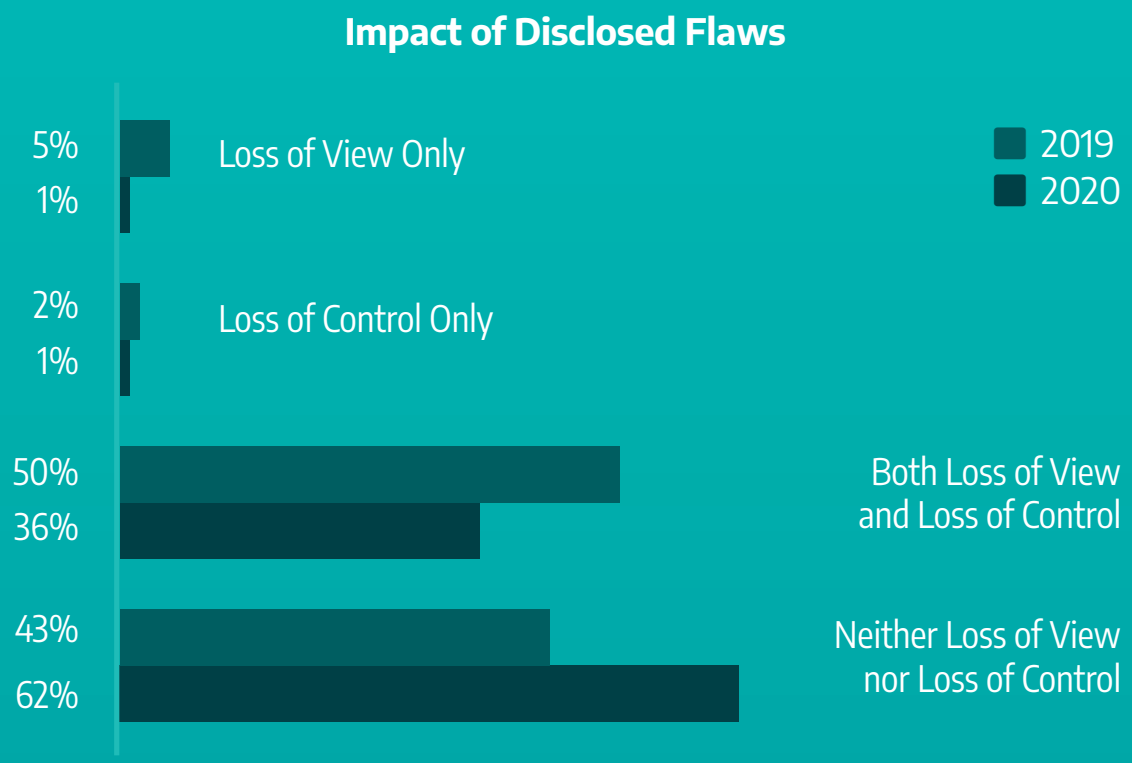
Advisories Applied to Products Bordering the Enterprise



Vulnerabilities Deep Within ICS Networks

Most vulnerabilities resided deep within the ICS network, meaning they apply to equipment on Levels 0 to 3 of the Purdue Model.[12] This includes engineering workstations, PLCs, sensors, and industrial controllers. These vulnerabilities require access to a control system network to exploit, offering some mitigation for organizations provided they implement proper network segmentation. With the increasing connectivity in organizations, this security control is diminishing in value and should be enhanced with efforts such as network monitoring, and where possible, Multi-Factor Authentication (MFA) for remote sessions.

[12] https://en.wikipedia.org/wiki/Purdue_Enterprise_Reference_Architecture



The percentage of disclosed flaws that could be used to cause a loss of view and loss of control in ICS systems decreased significantly from 50 percent in 2019 to 36 percent in 2020. This decrease is likely attributed to the increase in identified vulnerabilities bordering the enterprise that do not have direct operational impacts.

2020 Vulnerability Severity

In addition to validating the CVSS, Dragos categorizes vulnerabilities based on severity. The following taxonomy is used:

Immediate Action

A far-reaching threat or vulnerability calling for action broadly across at least one industry.

Limited Threat

A limited threat, risk, or vulnerability requiring an applicability assessment before taking action.

Possible Threat

Threat scenarios, research, and vulnerabilities relating to operations but not requiring direct/immediate action.

No Action Required

Items of interest but likely requiring no action except in unique threat models.

Hype

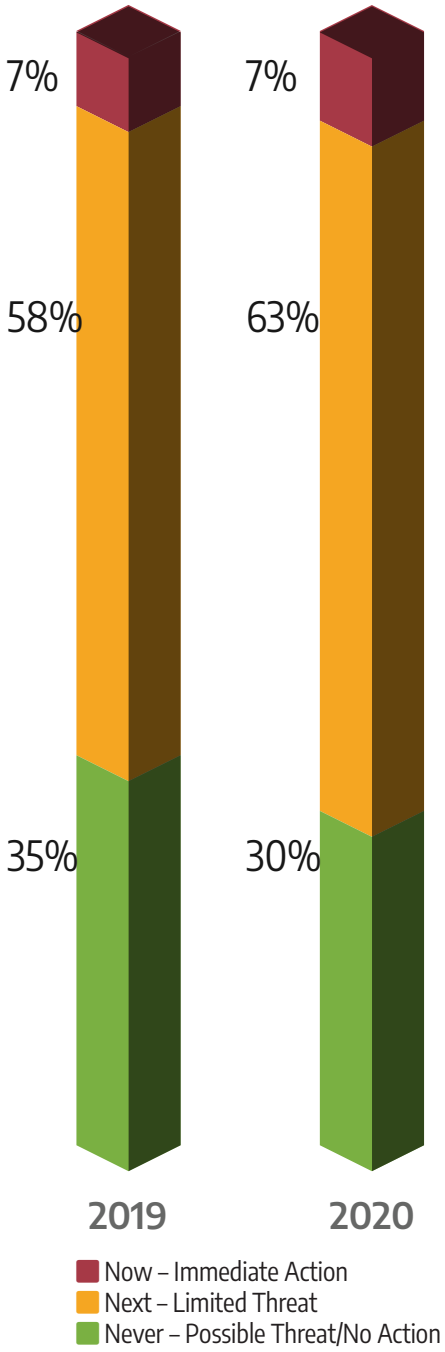
A story or vulnerability receiving coverage but not yet worth the attention of operators.

In examining individual vulnerabilities, Dragos also categorizes them based on the **"Now, Next, Never"** system, a malleable framework developed by CERT/Coordination Center (CC) to help asset owners and operators identify vulnerabilities and prioritize patching. The framework is not a one-size-fits-all solution for patch management. When combined with consequence-driven threat modeling, it can help OT security practitioners determine when and if to fix flaws in industrial control equipment.

The **"Now"** flaws require immediate action. These flaws include critical vulnerabilities such as perimeter-facing and network exploitable vulnerabilities, and other vulnerabilities that should be addressed as soon as practicable.

Limited Threat vulnerabilities fall into the **"Next"** category. These might be network exploitable but are present deeper in the network and require more work, access, and knowledge for an adversary to exploit or impact OT processes. If an operations network does not have proper segmentation or is accessible from the internet, asset owners and operators should consider the "Next" vulnerabilities a greater risk. In most cases, these vulnerabilities can be mitigated simply by updating firewall rules. It is important that customers conduct a firewall rule audit on a regular basis and justify every allow rule. In 2020, close to two-thirds of vulnerabilities assessed by Dragos were considered "Next," a Limited Threat.

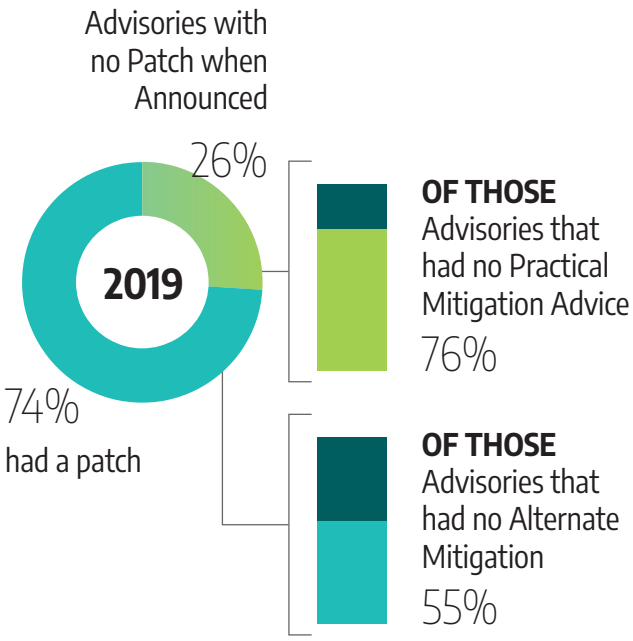
Low vulnerabilities pose a possible threat but rarely require action in vulnerability prioritization. They can be considered **"Never"** vulnerabilities. It is more beneficial for an organization to monitor its environment for signs of exploitation rather than to take devices and services offline to patch, or take appropriate mitigation measures. Although considered "Never" vulnerabilities, Dragos analysts do not recommend ignoring them entirely if time and resources permit. The reality is patching in ICS is more difficult than in most enterprise IT networks, and the value presented from patching these vulnerabilities is minimal. Asset owners and operators should conduct risk assessments to determine if it is safe to continue operations without addressing the identified vulnerabilities.

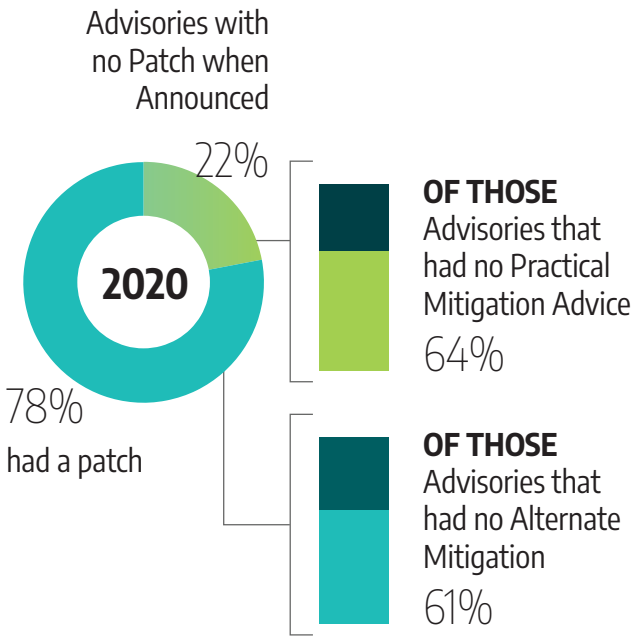


Actionable Guidance Missing in Most 2020 Advisories

An increase in the reported number of ICS vulnerabilities overall coincided with an increase in vendors providing patches alongside publicly disclosed flaws. Twenty-two percent of advisories did not have a patch when announced, down from 26 percent year-over-year. Of those, more than two-thirds did not contain practical mitigation advice.

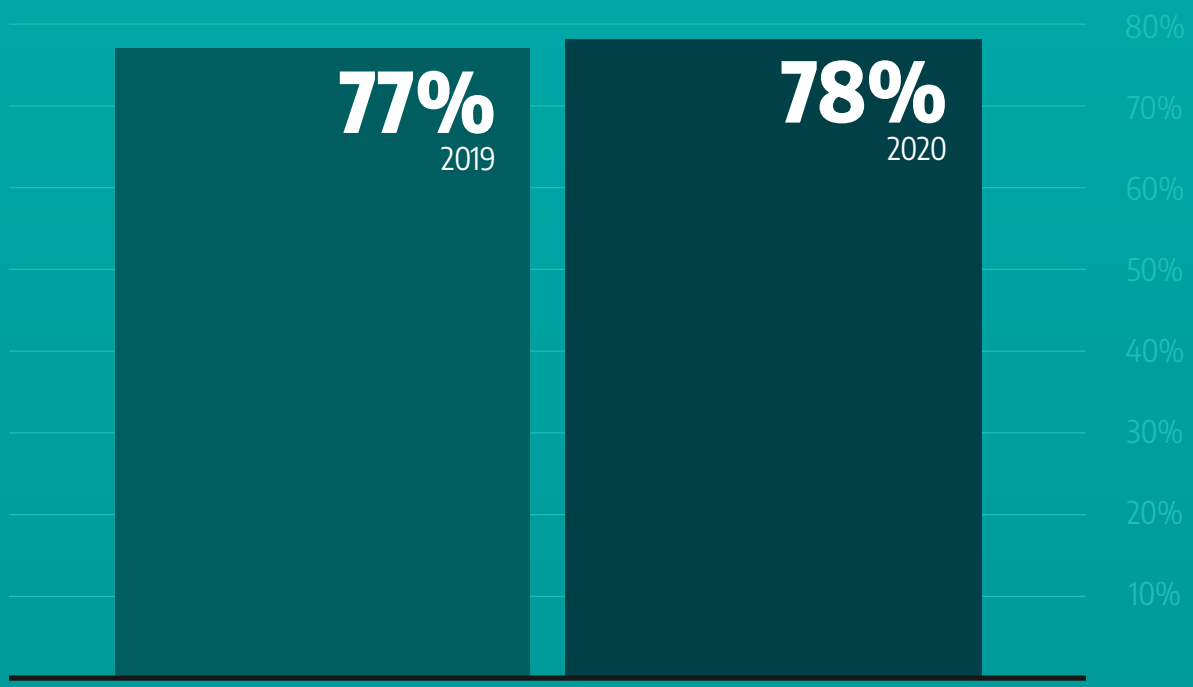
Frequently, vendors will not provide advice to asset owners and operators if they are unable to patch the identified vulnerability. Dragos identified 61 percent of advisories contained a patch to fix the vulnerability, but no alternative mitigation if patching was not an option.





Dragos provides customers with insight into managing risks about disclosed ICS vulnerabilities beyond what is included in advisories by the vendor. In 2020, Dragos provided additional mitigation advice for 78 percent of advisories that did not provide this information.

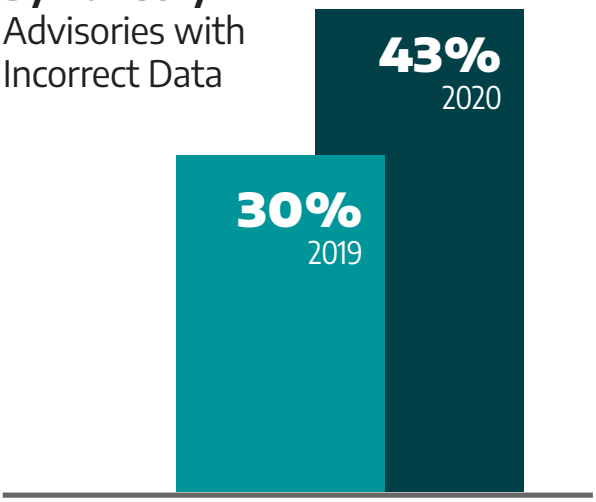
Mitigation Advice: Advisories Without Mitigation Advice for which Dragos Provided a Mitigation



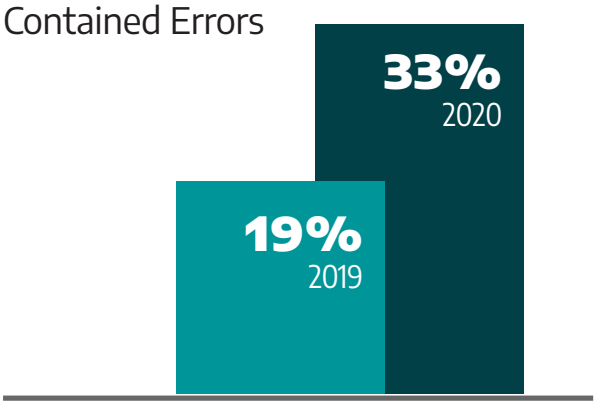
Severity Ratings of Vulnerabilities Remain Error-Prone

In addition to a lack of actionable information from most ICS-related vulnerability advisories in 2020, many advisories and individual vulnerabilities contained errors that could inadvertently mislead practitioners who use CVSS scores to triage for mitigation or patching.

By Advisory
Advisories with Incorrect Data

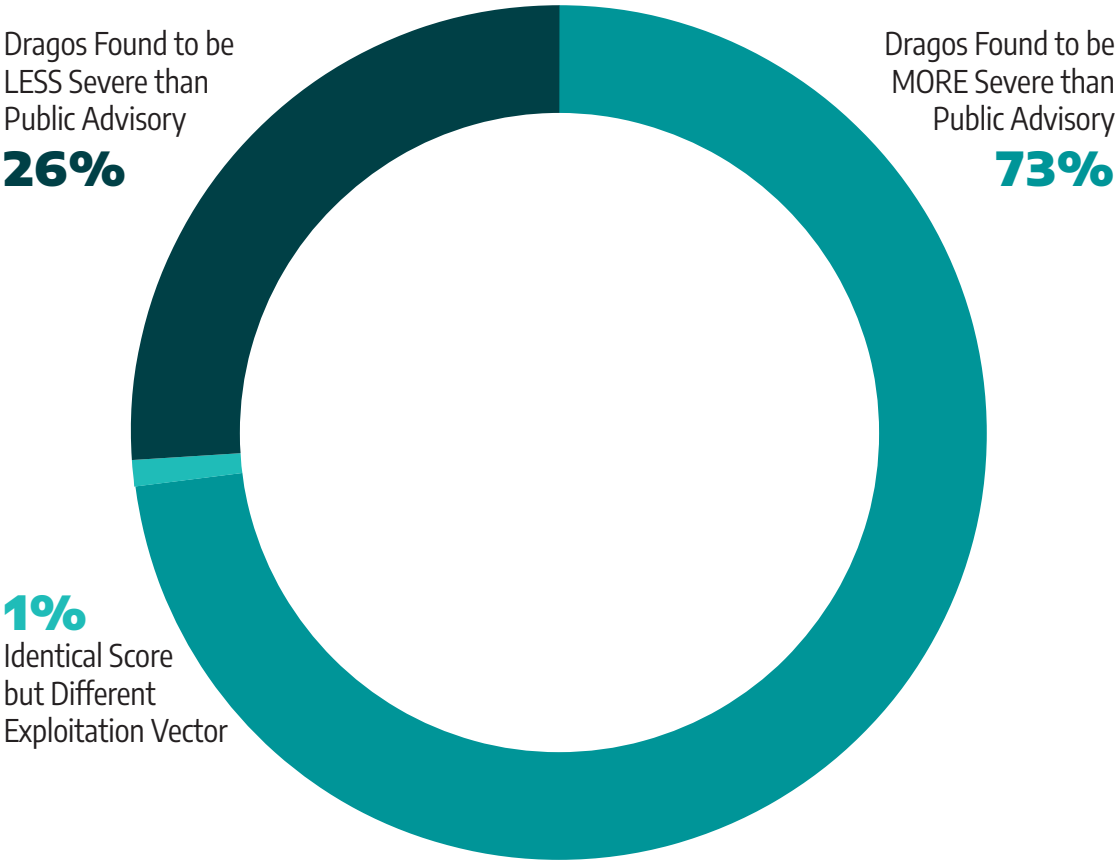


By CVE
(Error Rate)
Individual CVEs Contained Errors



The Dragos assessment of 2020 ICS-related vulnerabilities shows that among advisories and vulnerabilities containing errors, most of them understated severity levels. Seventy-three percent of corrected advisories were more severe in the context of an operational environment than the public advisory indicated.

By Advisory (Error Rate) — Rate was consistent from 2019 to 2020



By CVE

Flaws in TCP/IP Stacks

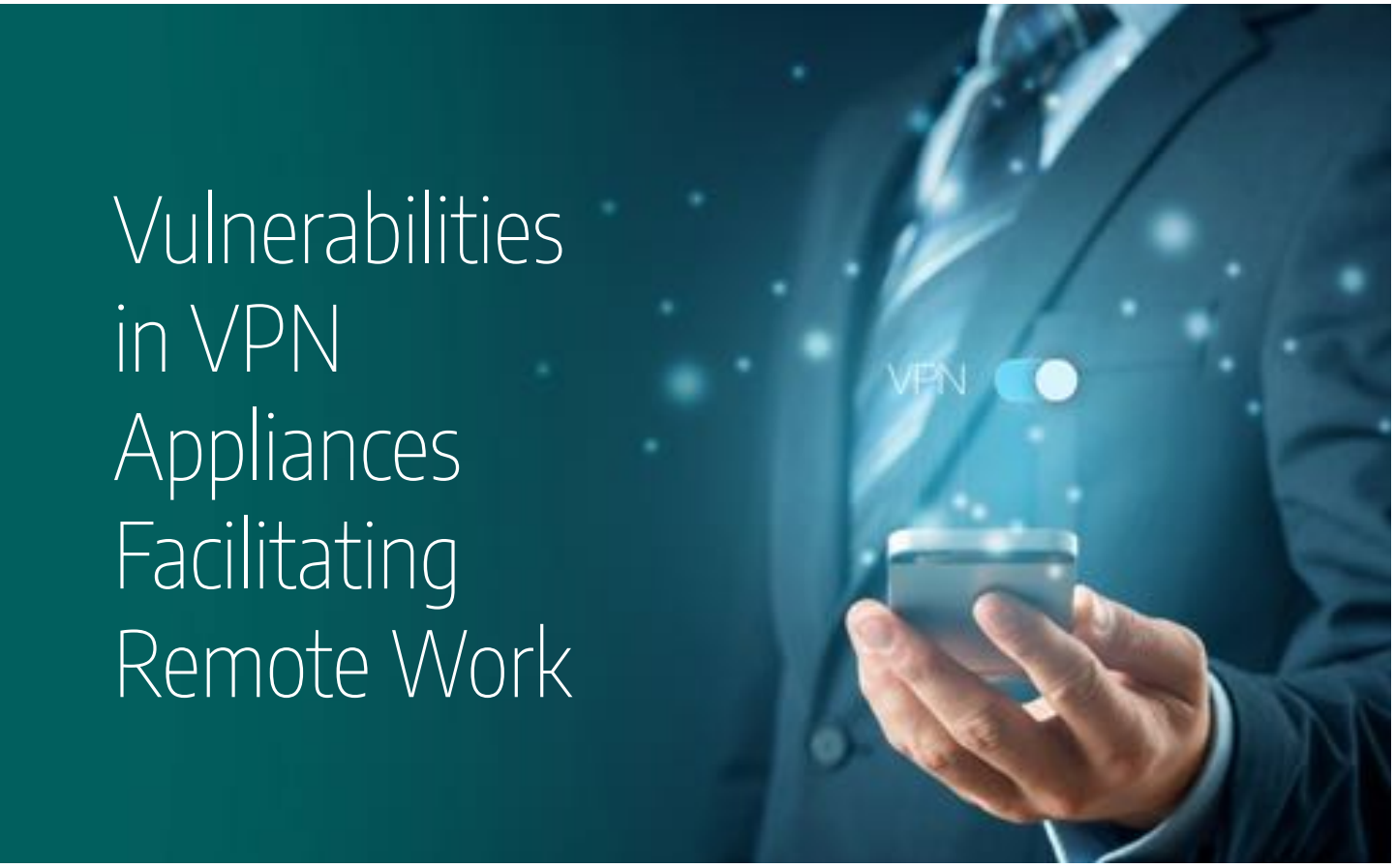
Researchers identified several third-party vulnerabilities in the software supply chain that impacted ICS systems. Most notable were Ripple20 and Amnesia:33, commercial names for vulnerabilities in third-party Internet Protocol (IP) stacks. These third-party stacks are used in many embedded products, including some used in industrial products and industrial-supporting Information Technology (IT) systems. Example ICS devices impacted include PLCs, Serial to Ethernet Converters, Protocol Converters, Remote Terminal Units (RTUs), digital protective relays, and some managed network switches and routers.

Mass exploitation of these vulnerabilities, like the similar URGENT/11 vulnerabilities reported in 2019, is rare. No organizations have provided evidence of public exploitation.

Devices that use third-party protocol stacks are often deeply embedded systems. Exploitation requires understanding the Central Processing Unit (CPU) architecture, memory layout, and hardware connections of the vulnerable device. Developing a working exploit requires a deep understanding of embedded systems. Once an exploit is developed, it may not even function on the same product if, for example, the product undergoes a hardware revision.

Fundamentally, these vulnerabilities are not a high risk for the industrial sector. In the industrial space, embedded systems are still most often "insecure by design," or lacking some security protections. An example of this is the APC Uninterruptible Power Supply (UPS) susceptibility to the Ripple20 vulnerabilities. The researchers of the vulnerabilities developed a working exploit for CVE-2020-11901 against the UPS, which could result in shutting off the UPS. However, the UPS speaks an industrial protocol called BACnet that lacks basic security protections. According to the device instruction manual, and verified by Dragos, a BACnet control point can be used to achieve the same effect using freely available tools.

Vulnerabilities in VPN Appliances Facilitating Remote Work



Several VPN appliance vulnerabilities were disclosed and fixed in 2020. These include issues in non-industrial appliances that Dragos tracks and models that are specifically marketed toward industrial customers. In 2020, Dragos tracked 13 advisories that include VPN software and hardware commonly used in industrial environments and gateways with optional VPN features. Impacted devices include Palo Alto Networks Global Protect VPN client, Citrix Application Delivery Controller and Netscaler, and ICS-specific VPN services Ewon, Cosy, and Flexy.

Enterprise VPN appliances are often used by industrial operators to provide remote access to corporate and operations networks. Some OEMs provide VPN access specifically for their ICS equipment, restricting connections or lateral movement to the rest of the OT network. Many of these products are identified as belonging to utilities via the popular search engine Shodan. Vulnerabilities in these products should be remediated quickly.

End users should determine the exposure of VPN appliances. Industrial-specific VPN appliances may provide direct access to process control systems. These devices are best secured by using them in "client" mode where they may connect to a central server. The central server may be hardened to prevent site-to-site communications between field sites, and to monitor for suspicious behavior originating from field sites.

SECTION THREE

Lessons Learned From The Front Lines

INTRODUCTION

For the last two decades, the prevailing strategies for safeguarding ICS were focused on protecting the perimeter, preventative security countermeasures, and internal segmentation. In that time, standards, regulations, and best practices codified these methods. Other focuses, such as detection, response, and recovery were included but without equal emphasis or examples. The disparity has left industrial organizations underdeveloped in these core capabilities in an understandable, yet undesirable, situation. In general, the industry lacks visibility into their ICS assets and activities, hampering the overall cyber readiness and ability to understand and manage cyber risk. These themes are confirmed based upon analysis of Dragos service engagements in 2020.

The data set includes engagements from many industrial infrastructure sectors including electric, oil and gas, food and agriculture, manufacturing, chemical, transportation, water and wastewater, technology (data center building automation equipment), and mining.

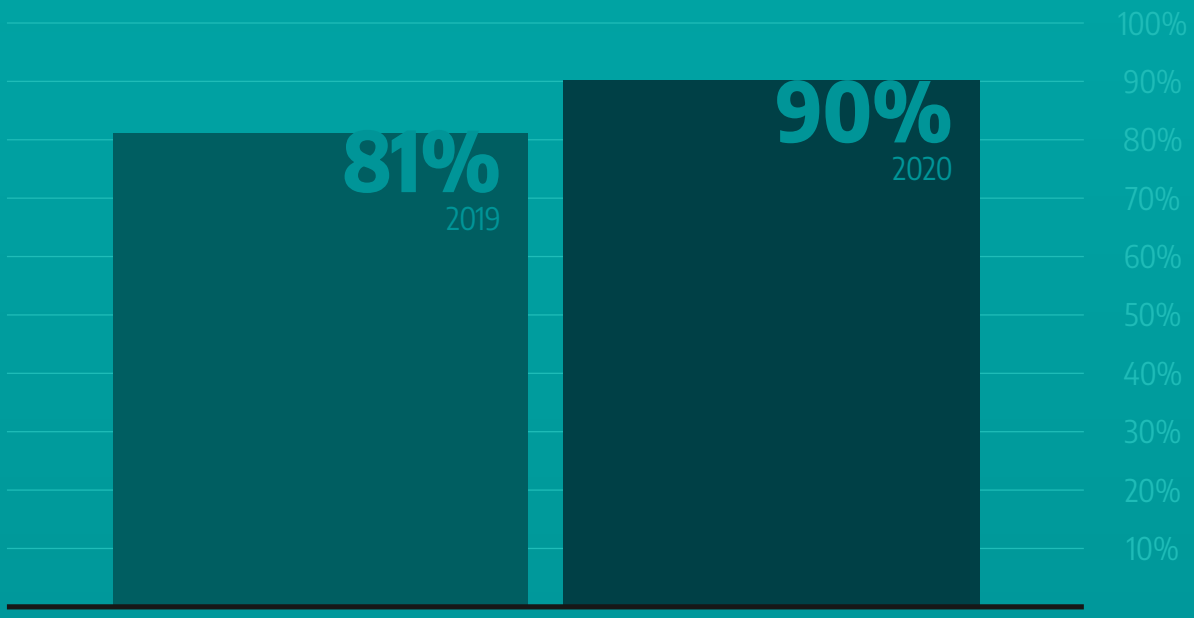
THE FOLLOWING DATA IS BASED ON A GROWING SET OF ANNUAL ENGAGEMENTS CONDUCTED BY THE DRAGOS TEAM OF ICS CYBERSECURITY EXPERTS ON SEVERAL SERVICE TYPES, INCLUDING:

- ARCHITECTURAL REVIEWS
- VULNERABILITY ASSESSMENTS
- PENETRATION TESTS
- TABLE TOP EXERCISES
- INCIDENT RESPONSE (IR)

Visibility

Over the course of the year, Dragos found that 90 percent of its services customers had limited to no visibility into their ICS environments. While most clients demonstrated a focus on an enhanced asset inventory, this effort is only the foundation for asset visibility. Many customers only monitored the IT to OT boundary without monitoring activity inside the ICS network. Network analysts were blind to critical network traffic. Some collected logs, but few utilized centralized logging to correlate various segments with network traffic analysis. These steps are critical for developing a full picture of what occurred across industrial assets and sites.

Extremely Limited / No Visibility into OT Environment



Compared to the Dragos 2019 Year in Review report, 90 percent represents a small increase in this statistic. Note that this is not indicative of the same customers failing to improve year-over-year. Lack of visibility, a common finding in architecture reviews, is skewed heavily towards new customers. Architecture reviews conducted with repeat customers are typically not for the same facility either. While not a perfect comparison, the statistic indicates the state of cybersecurity for those customers early in their OT cyber maturity.

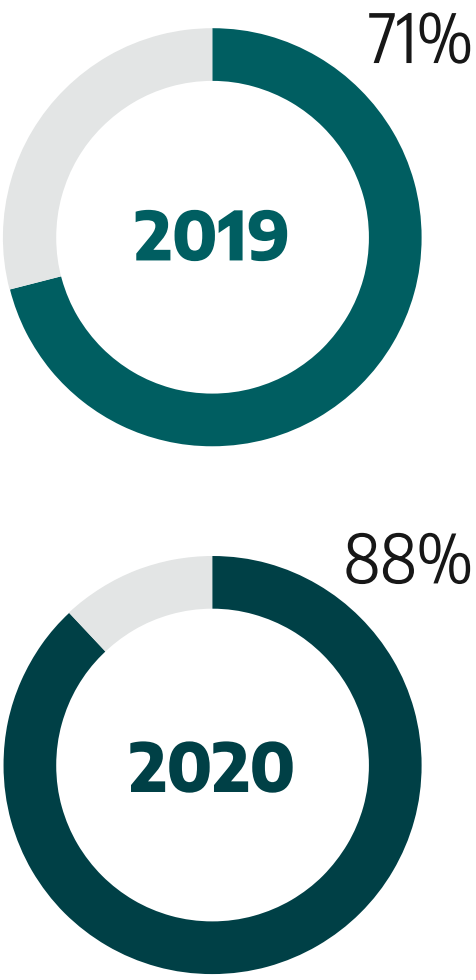
Dragos's incident response cases for 2020 provide further support for this lack of visibility because none of them were augmented with any centralized or automated host and network traffic logging. This significantly slows down the incident response process, and in multiple cases, means that the asset owner or operator is not able to get critical questions answered. In at least one case, the impact led to public reporting without an understanding of root cause analysis where cyber activity was heavily suspected, but no evidence was available.

IR Cases Facilitated by Automated Logging or Visibility into ICS Network

Segmentation and Connections

Although asset owners and operators follow many of the best practices and their applicable regulation, Dragos continues to observe instances of poor segmentation with unexpected or unknown connections from the ICS network. About 88 percent of Dragos services engagements involved significant issues with network segmentation. Examples of observations contributing to this statistic include flat networks, where the only segmentation is the initial firewall between the IT-OT boundary, and unnecessary communication pathways to critical assets within the network. To further illustrate the incidence of poor segmentation, consider that adversaries accessed ICS networks directly from the internet in 100 percent of Dragos's 2020 incident response cases. These findings are directly related to the previous statistic of 90 percent of organizations that lacked OT visibility. Identifying architecture bypasses and rogue connections and devices is nearly impossible without visibility through network monitoring.

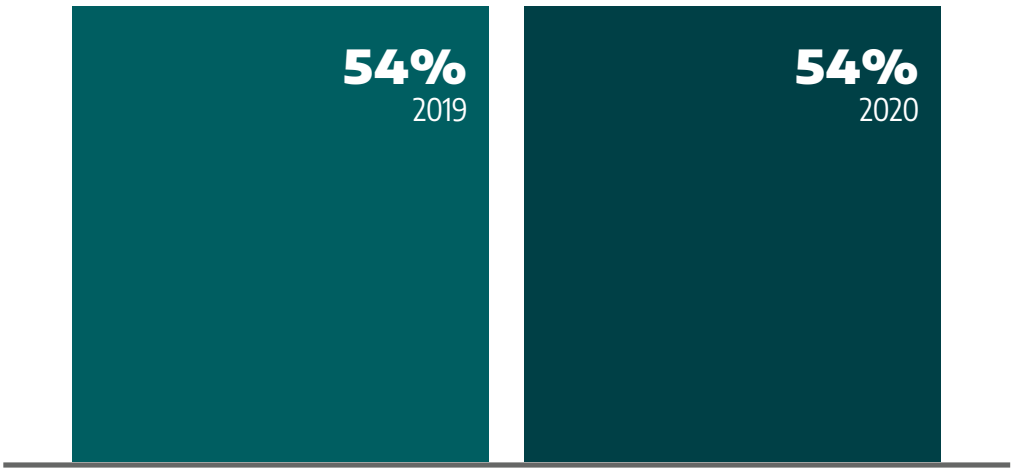
Engagements Exhibiting Poor Security Perimeters



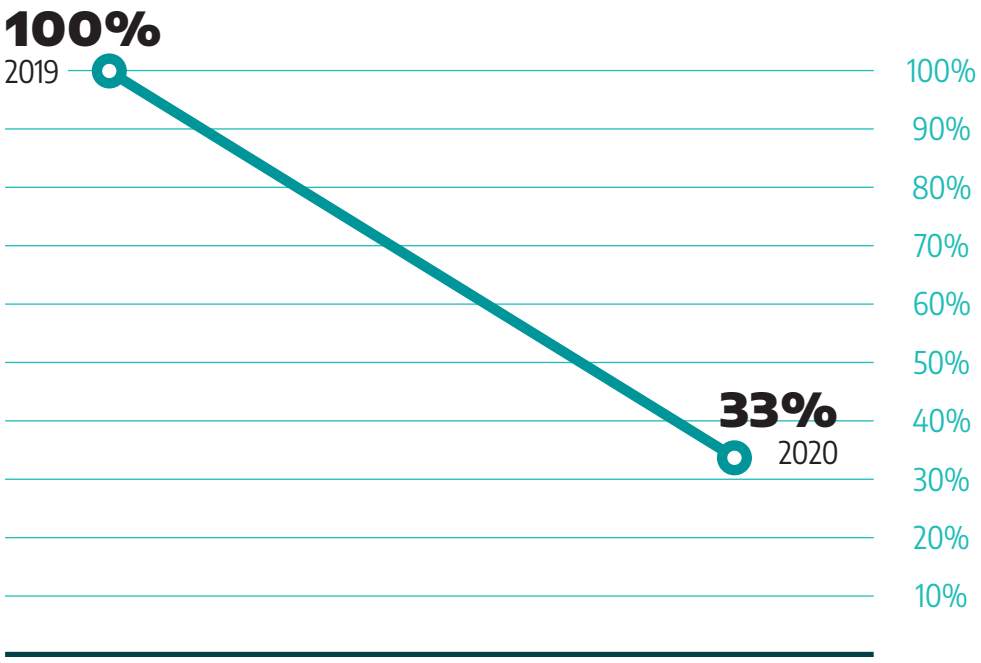
While the annual comparison shows a 17-point increase in engagements exhibiting poor security perimeters, Dragos does not believe the industry is regressing on this security principle. Dragos attributes the growth to a rise in the number of engagements conducted. However, this statistic does support the assertion that cyber strategies focused on segmentation and prevention are not sufficient.

Adversary usage of shared credentials exacerbates the severity of poor security perimeters. Just over half of service engagements found shared credentials between IT and OT networks. For example, an organization may leverage the same credential management on the IT network as it does on the Demilitarized Zone (DMZ) and ICS network. This is another configuration that leads to a weakening of perimeters and may enable an adversary to easily traverse to ICS assets using credentials obtained from IT accounts. For example, 100 percent of incident response cases that confirmed adversary activity involved the adversary leveraging shared credentials for lateral movement. During one case, Dragos analysts responded to an Activity Group that harvested credentials from an IT asset, and then leveraged a vulnerability in a VPN appliance to gain initial access to the ICS environment. In this case, the adversary also used the compromised credentials to move laterally in the ICS network and access the critical assets.

Organizations that Lacked Separate IT and OT User Management



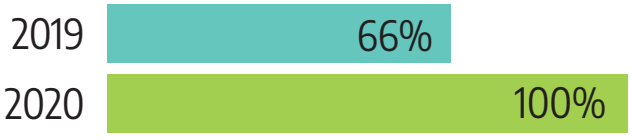
External Routable Network Connection to ICS Environments Believed to be Air-Gapped



A recurring theme from the previous Year in Review reports is the disconnect between expectations and reality about air-gapped systems. There was significant improvement in 2020 in this area, with a two-thirds drop in the discovery of external routable network connections to air-gapped ICS environments. During one engagement, a client who believed their network to be air-gapped had two external connections bypassing their architecture and terminating deep within their gas transmission systems. The purpose of the connections was to monitor gas quality and heating values, and ensure exported product met demand and quality specifications. Problematically, communications took place directly between critical controllers used for the industrial process and PLCs used only for data exchange with the remote connection. This connection could have been leveraged by an adversary to gain initial access to the network and move laterally across Level 1 systems within the Purdue model. Some systems in Level 1 had communication pathways through network allowlists to Safety Instrumented Systems (SIS) in the Safety Zone. Access to the Safety Zone may be the goal of an adversary who intends to cause a loss of safety impact, such as XENOTIME.

Shared credentials and poor security perimeters allow adversaries to leverage Valid Accounts and gain persistent access to remote ICS. Valid Accounts is the most common TTP used across all Dragos ICS Activity Groups. Analysis of 2020 Dragos incident response cases indicates its effectiveness.

IR Cases where Adversary Accessed ICS Network from Internet



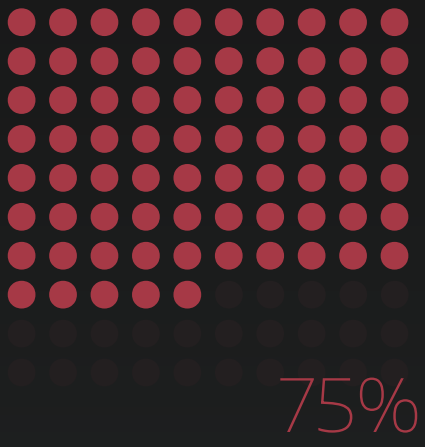
IR Cases Involving Shared Credentials for Lateral Movement

Cyber Readiness

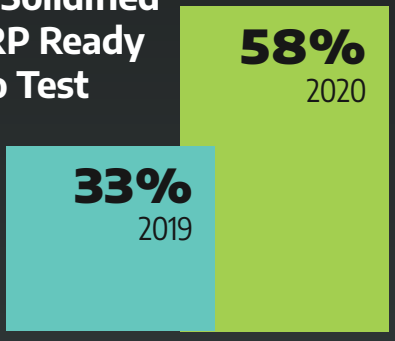
In 2020, Dragos conducted several tabletop exercises and incident response readiness workshops. The findings and outcomes of these engagements further illustrate the industry's deep-seated, over-reliance on prevention and the necessity of strengthening the pillars of a successful ICS cyber strategy; detection, response, and recovery.

Dragos observed that 75 percent of clients did not have clearly defined incident declaration thresholds or categories of severity within response plans. Detecting threat behaviors and analyzing correlated datasets are generally the first steps an organization takes to recognize an incident. The threshold for declaring an incident depends on many factors including threats, tactics, operational risk requirements, governing laws, and industry regulations. Once incidents were declared, incident managers were often observed by Dragos to have no documented guidance or playbook for how to employ resources or capabilities. Nearly 60 percent of organizations did not have a solidified Incident Response Plan (IRP). Incident managers were often left to create tactical response plans in real-time and in the middle of rapid escalations. In 2020, Dragos observed that 75 percent of 2020 clients did not have clearly defined or documented incident declaration thresholds or categories of severity available during activation of their incident response plans.

Organizations that did not have clear cyber incident thresholds



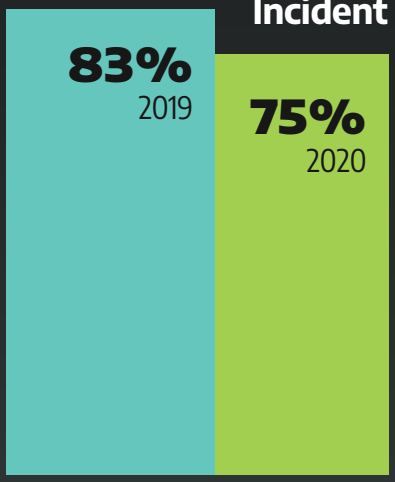
Organizations that had a Solidified IRP Ready to Test



In 2020, 62 percent of Dragos client organizations did not tie a dedicated communications plan to their cybersecurity incident response activations. This is a continuance of an industry trend from 2019. Communication plans are critical in enabling incident managers and stakeholders to quickly activate, assemble, and employ resources and capabilities. During an incident, the need to react appropriately is immediate, followed by the need to communicate. Lack of effective communication during a crisis can lead to inadequate resource allocation, compound risks to assets and personnel, and create lingering effects on bottom-line operations. The periodic testing of IRPs can act as a roadmap for corporate leadership to convey strategic directives and objectives to an incident response team. 100 percent of Dragos exercise participants strongly agree that exercises are beneficial to long-term incident response preparation and are a valuable way to identify areas of improvement for industrial cybersecurity IRPs.

Organizations that did not have Communications Plans Linked to IRP Activations

Organizations that had Difficulty Understanding when to Declare an Incident



Dragos customers who Agree Tabletop Exercises are Beneficial to IRPs

100%

Dragos Red Team

In penetration tests, Dragos focuses on demonstrating adversary behavior that could have physical impacts on industrial processes. The team utilizes Crown Jewel Analysis to identify high consequence events, the assets that can cause them, and pathways to those assets specific to the client and the process.[13] The team often deploys the same TTPs of specific ICS Activity Groups to provide real-world applicability.

Below are examples of real-world findings from Dragos penetration testing engagements:

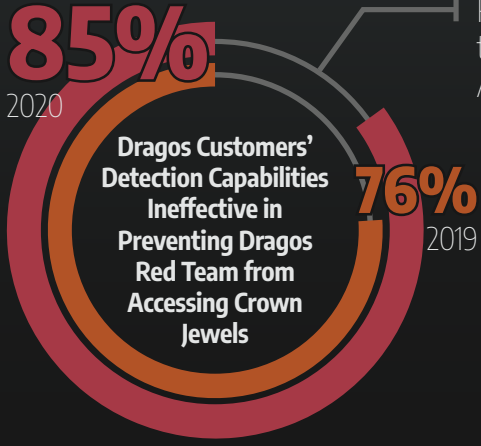
- Executed the propagation of malicious logic file updates from one asset to the entire deployment.
- Identified a Zero Day exploit to remotely execute arbitrary code as a read-only user on a Crown Jewel Human Machine Interface (HMI).
- Discovered hard-coded credentials on an ICS that monitors Crown Jewels.

Among all 2020 Red Team Engagements

100% Resulted in situations where the team could have made changes in controller logic

85% 2020

Remaining 15% that Detected Red Team Activity in 2020



0%

- detected activity in real-time
- deterred lateral movement to other critical systems

[12] https://www.dragos.com/resource/dependency-modeling-for-identifying-cybersecurity-crown-jewels-in-an-ics-environment/

Recommendations

As organizations strategize a path forward, Dragos recommends five key OT cybersecurity initiatives to improve on in 2021 and beyond. These are based on the empirical evidence provided throughout the report.

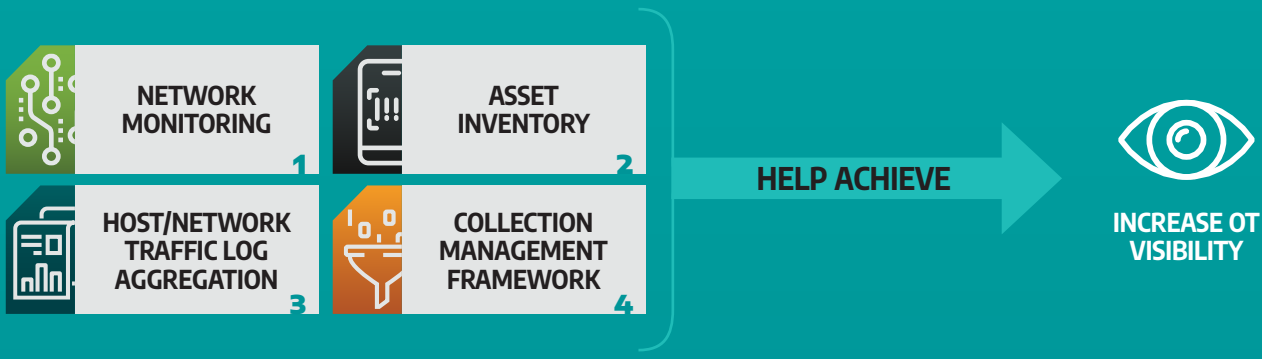
Dragos has included a graphic below each recommendation as a reference for asset owners looking to implement the top five the recommendations of 2020. The recommendations listed on the right are in descending order according to priority. Each recommendation has three or more actions that may help asset owners achieve the desired goal of the recommendation. These actions are numbered with the positive impact on that recommendation.

The top five recommendations to enhance the security of an ICS environment are:

Increase OT Network Visibility

Visibility includes network monitoring, logging, and maintaining a Collection Management Framework (CMF).

Logging and monitoring of OT systems is essential for detection and incident response in addition to providing actionable data regarding device performance, operation, and reliability. Network traffic analysis should be prioritized based on the considerations of the networks and their risks.



Identify and Prioritize Crown Jewels

Crown Jewels are those assets that exercise control over the components most critical to the safe operation of the industrial process. Examples include HMIs, engineering and operator workstations, gateways, and controllers.

Prioritizing the assets that, if compromised, could cause major impacts to the organization is key principle of risk management.

Example: At one facility, Instrumentation and Control (I&C) staff could connect into the production network using a VPN. Once connected, they utilized RDP to access their engineering laptop. Their laptops had read/write permissions to any PLC in the Production Network, including the crown jewel PLCs. Additionally, control staff left PLC Run/Remote/Program key switches in remote mode meaning anyone with network access could edit PLC configurations and logic. Lastly, they did not have a mechanism to proactively detect changes to these PLC configurations. In summary, a compromised I&C technician account could modify PLC configurations and operations would not detect it, until an operational issue or periodic maintenance occurred.

Boost Incident Response Capabilities

Incident response refers to an organization's approach for handling cybersecurity incidents.

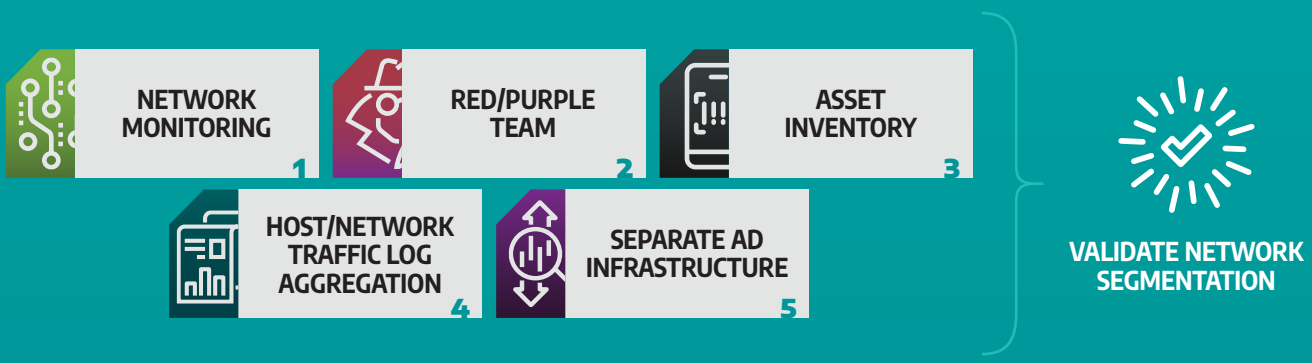
An incident response capability is necessary to minimize loss and restore safe operations. Many organizations have an enterprise IT incident response plan that does not account for, or significantly misunderstands, ICS incident response efforts.

Validate Network Segmentation

This includes issues like weak segmentation between IT and OT networks, permissive firewall rulesets, and externally routable network connections.

Network segmentation should be continuously monitored to ensure it is not bypassed or negated.

Example: A client believed their SIS devices were properly segmented. An external connection was found that could have allowed an adversary to bypass multiple network boundary devices with only a Virtual Local Area Network (VLAN) between the connection and the Safety Zone.

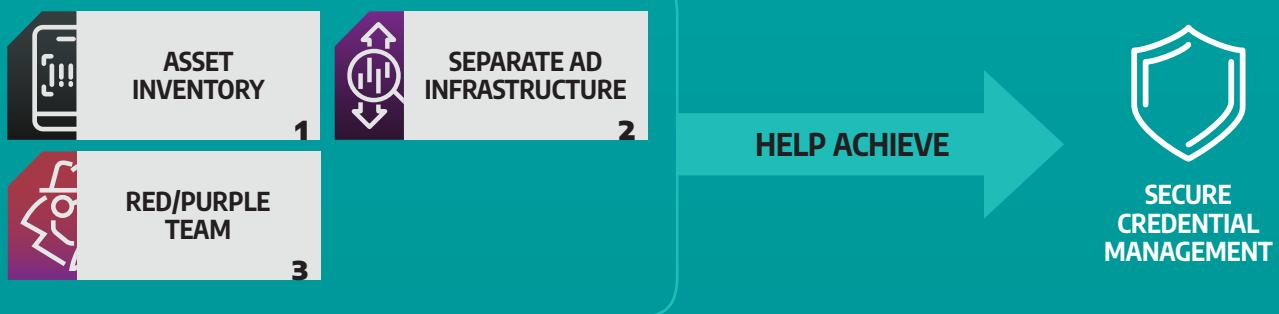


Secure Credential Management

This includes accounts shared between IT and OT, default accounts, and vendor accounts. AD shared between the enterprise and ICS networks is one of the most common findings that should be mitigated.

Adversaries seek to compromise and leverage valid accounts as a means to access critical industrial systems.

During one assessment, Dragos obtained root access to the affected entities by successfully identifying the root password for all the impacted systems related to the client's HMI. This was accomplished through guessing and using common default passwords.



Dragos is an industrial (OT/ICS/IIoT) cybersecurity company on a mission to safeguard civilization.

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

Dragos.com