Cyber Threat Perspective

MANUFACTURING SECTOR

NOVEMBER 2020

DRAGOS, INC.
Intel@Dragos.com
@DragosInc

EXECUTIVE SUMMARY

Cyber risk to the manufacturing sector is increasing, led by disruptive cyberattacks impacting industrial processes, intrusions enabling information gathering and process information theft, and new activity from Industrial Control Systems (ICS)-targeting adversaries. Dragos currently publicly tracks five ICS-focused activity groups targeting manufacturing: CHRYSENE, PARISITE, MAGNALLIUM, WASSONITE, and XENOTIME in addition to various ransomware activities capable of disrupting operations.

Manufacturing relies on ICS to scale, function, and ensure consistent quality control and product safety. The sector produces crucial materials, finished goods, and medicine and is classified as critical infrastructure. Due to the interconnected nature of facilities and operations, an attack on a manufacturing entity can have ripple effects across the supply chain that relies on timely and precise production to support product fulfillment, health and safety, and national security objectives.

Ransomware adversaries are adopting ICS-aware functionality with the ability to stop industrial related processes and cause disruptive – and potentially destructive – impacts. Dragos has not observed ICS-specific malware targeting manufacturing operations on the same scale or sophistication as that used in the disruptive TRISIS[1] and CRASHOVERRIDE[2] malware attacks that targeted energy operations in Saudi Arabia and Ukraine, respectively. However, known and ongoing threats to manufacturing can have direct and indirect impact to operations. This report provides a snapshot of the threat landscape as of October 2020 and is expected to change in the future as adversaries and their behaviors evolve.

1 TRISIS: Analyzing Safety System Targeting Malware – Dragos
2 CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack – Joe Slowik,

KEY FINDINGS

- Ransomware with the ability to disrupt industrial processes is the biggest threat to manufacturing operations. Adversaries are increasingly adopting ICS-aware mechanisms within ransomware that could stop operations.
- Dragos publicly tracks five activity groups that target manufacturing.
- Disruptions within manufacturing industrial processes have supply chain implications that impact businesses and potentially operations elsewhere.
- The theft of proprietary and confidential manufacturing process details – often considered intellectual property – remains a high risk for manufacturers.
- A growing convergence of interconnected enterprise, operations, and process control networks contributes to a growing threat landscape.

Table of Contents

ACTIVITY GROUPS

DRAGOS TRACKS AT LEAST FIVE PUBLICLY IDENTIFIED ACTIVITY GROUPS[3] TARGETING OR DEMONSTRATING INTEREST IN MANUFACTURING ENTITIES.

CHRYSENE targets manufacturing, petrochemical, oil and gas, and electric generation sectors. Targeting has expanded beyond the group's initial focus on the Persian Gulf region, and the group remains active in more than one area.[4]

Links: APT 34, GREENBUG, OilRig[5]

MAGNALLIUM has targeted energy, aerospace, and supporting entities since at least 2013. Although MAGNALLIUM has not specifically targeted manufacturing operations, chemical manufacturing processes are within the scope of victimology for this group. The activity group initially targeted firms based in Saudi Arabia but expanded targeting to include entities in Europe and North America, including U.S. electric utilities. MAGNALLIUM lacks an ICS-specific capability, but the group remains focused on initial IT intrusions.[6]

Links: PARISITE, APT 33, Elfin[7]

PARISITE, operating since 2017, targets manufacturing, electric utilities, aerospace, oil and gas entities, and government and non-governmental organizations. Its geographic targeting includes North America, Europe, and the Middle East.

Links: MAGNALLIUM, Fox Kitten, Pioneer Kitten[8]

WASSONITE targets manufacturing, electric generation, nuclear energy, and research entities in India, and likely South Korea and Japan. The group's operations rely on DTrack malware, credential capture tools, and system tools for lateral movement. WASSONITE has operated since at least 2018.

Links: Lazarus Group, COVELLITE[9]

XENOTIME compromised several ICS vendors and manufacturers, posing a potential supply chain threat.[10] This group is known for the TRISIS attack that caused disruption at an oil and gas facility in Saudi Arabia in August 2017. In 2018, XENOTIME activity expanded to include electric utilities in North America and the Asia-Pacific region; oil and gas companies in Europe, the United States (U.S.), Australia, and the Middle East. Expanded activity also includes control system devices beyond the Triconex controllers targeted in the 2017 incident.

Links: Temp.Veles[11]

3 Dragos categorizes ICS-targeting activity into activity groups based on observable elements that include an adversary's methods of operation, infrastructure used to execute actions, and the targets they focus on. The goal, as defined by the Diamond Model of Intrusion Analysis, is to delineate an adversary by their observed actions, capabilities, and demonstrated impact– not implied or assumed intentions. These attributes create a construct around which defensive plans can be built. At this time, two activity groups possess ICS-specific capabilities and tools to cause disruptive events: XENOTIME and ELECTRUM.
4 CHRYSENE – Dragos
5 OilRig – MITRE ATT&CK
6 MAGNALLIUM – Dragos
7 APT33 – MITRE ATT&CK
8 Fox Kitten – Widespread Iranian Espionage-Offensive Campaign – Clear Sky; Who is PIONEER KITTEN? – CrowdStrike
9 COVELLITE – Dragos
10 XENOTIME – Dragos
11 TEMP.Veles – MITRE ATT&CK

ICS MALWARE

Currently two activity groups, XENOTIME and ELECTRUM, have demonstrated the ability to interact with and disrupt operations with malware specifically targeting ICS processes: TRISIS and CRASHOVERRIDE[12] malware respectively.[13] Although Dragos has not observed either malware family disrupting manufacturing operations, it is possible these adversaries will target manufacturing companies in the process of developing such malware, even if they are not the ultimate target.

For example, the 2016 CRASHOVERRIDE malware specifically targeted Siemens SIPROTEC protective relays and ABB equipment, including all relevant communication protocols excluding OPC Data Access (DA), at an electric transmission substation in Ukraine. Dragos observed some large manufacturing companies may have their own power operations onsite containing the same equipment. An adversary could theoretically leverage manufacturing operations as a "testing ground" for disruptive attacks targeting critical infrastructure, like electric utilities, if the same equipment is used. Dragos assesses it is likely manufacturing is a more attractive target for an adversary's offensive development due to generally less sophisticated cybersecurity infrastructure and less government oversight.

The most infamous ICS malware, Stuxnet, also targeted manufacturing. First discovered in 2010, the worm targeted Iranian-owned Programmable Logic Controllers (PLCs) responsible for controlling centrifuges used in Uranium enrichment. Unprecedented at the time, this cyberattack was the first to cause physical damage to computerized systems.[14]

12 CRASHOVERRIDE: Reassessing the 2016 Ukraine Electric Power Event as a Protection-Focused Attack – Dragos
13 ELECTRUM – Dragos
14 An Unprecedented Look At Stuxnet, the World's First Digital Weapon – Wired

THREATS TO MANUFACTURING

Ransomware

The most common threat to manufacturing is ransomware. Dragos observed a significant rise in the number of non-public and public ransomware events that have affected ICS environments and operations over the last two years.

This year, Dragos identified multiple ransomware strains adopting ICS-aware functionality, including the ability to "kill" (i.e., stop) industrial processes if identified in the environment, with activity dating back to 2019. EKANS,[15] Megacortex, and Clop are just a few ransomware strains that contain this type of code.[16] Past concerns with ransomware in ICS focused on propagation. IT-focused ransomware could impact control system environments if it is able to migrate into Windows-based portions of control system networks and disrupt operations.

EKANS and other ICS-aware ransomware represent a unique and specific risk to industrial operations not previously observed in ransomware operations.

In 2020, the number of publicly reported ransomware attacks on manufacturing entities has more than tripled compared to 2019, based on data tracked by Dragos. Although most ransomware strains impacting ICS and related entities are IT-focused, ransomware can have indirect impacts on operations and process control networks by impacting resources such as logistics, fleet management, sales operations and fulfillment, or loss of view to enterprise resource management tools. For example, enterprise technologies like Enterprise Resource Planning (ERP) software are integrated with data historians containing process data to distribute information across a company. By encrypting ERP and related files on a workstation, a ransomware adversary could stop vital communication and record keeping, indirectly impacting manufacturing process and logistics operations.

CASE STUDY

On 04 March 2020, a Ryuk infection at the manufacturer EVRAZ impacted North American operations including email, shipping, product certification, internet availability, and corporate networks. The attack resulted in shutdowns of steel and pipe divisions, and temporary layoffs for over 1,000 workers for at least four days.[17]

Ransomware operators are increasingly incorporating data theft techniques into their campaigns to further ransom demands. An adversary may steal data from a target company before encrypting infected machines and threaten to publish the data online either on adversary-run websites or hacking forums if a ransom demand is not paid. This method could encourage companies to pay ransoms demanded by hackers. Data stolen or leaked by adversaries could contain sensitive information on the target company such as proprietary process details and information about its equipment suppliers. Although a ransomware adversary

15 EKANS Ransomware and ICS Operations – Dragos
16 Financially Motivated Actors Are Expanding Access Into OT: Analysis of Kill Lists That Include OT Processes Used With Seven Malware Families – FireEye
17 Evraz Steel shuts down Regina plant after continent-wide computer hack – 980 CJME, One of Roman Abramovich's companies got hit by ransomware – ZDNet

may only be interested in leveraging data for financial purposes, adversaries interested in specifically targeting manufacturing operations could use leaked data to aid in attack development. For example, an adversary could use customer data to identify potential opportunities for third-party or supply chain compromise. Data like schematics, process details, network diagrams, or other internal documentation could be used to identify targets for operational gain and assess the level of obscurity a target has from internal and external resources.

Ransomware is not just for financially motivated operators. State-sponsored actors may also leverage ransomware in cyber operations targeting manufacturers. In May 2020, the Republic of China (Taiwan) government attributed ransomware events targeting oil and gas and semiconductor companies to the Winnti Group[18] a threat group that is likely state-associated activity. The LockerGoga ransomware attack on Norsk Hydro in 2019 may have been the work of state-sponsored adversaries aiming to cause disruption rather than make money from the operation.[19]

Internet-Exposed Assets

Industrial and networking assets exposed to the internet are a high risk for manufacturing that can facilitate initial access to a victim environment. Various tracked ICS-targeting activity groups – PARISITE, MAGNALLIUM, ALLANITE, and XENOTIME – have previously targeted or currently attempt to exploit remote access technology or logon infrastructure.

According to the 2019 Dragos Year in Review report detailing lessons learned from the incident response and services team, 66 percent of incident response cases involved adversaries directly accessing the ICS network from the internet, and 100 percent of organizations had routable network connections into their operational environments.[20] Recent cyber intrusions targeting water infrastructure[21] in Israel were the result of Programmable Logic Controllers (PLCs) exposed to the open internet. Dragos also responded to ransomware events at industrial entities that leveraged internet-connected remote access portals to infiltrate the operations network and deploy ransomware.

In July 2020, the U.S. Department of Homeland Security Cybersecurity and Infrastructure Security Agency (CISA) and the National Security Agency (NSA) published an alert encouraging asset owners and operators to take immediate actions restricting exposure of OT assets to the internet.[22] According to the alert, behaviors observed recently before publication include: spearphishing to gain initial access to Information Technology (IT) before pivoting to Operational Technology (OT), deploying commodity ransomware to impact both IT and OT environments, connecting to internet accessible PLCs that require no authentication, using common ports and standard application layer protocols to communicate with controllers and download modified control logic, using vendor engineering software and program downloads, and modifying control logic and parameters on programmable logic controllers.

18 國內重要企業遭勒索軟體攻擊事件調□說明 – Taiwan Ministry of Justice Investigation Bureau; Bureau Names Ransomware Culprits – Taipei Times
19 Spyware, Stealer, Locker, Wiper: LockerGoga Revisited – Joe Slowik, Dragos
20 Dragos Year In Review 2019 Lessons Learned – Dragos
21 Hackers Target PLCs and SCADA Systems at Water Facilities in Israel – Control Automation
22 NSA and CISA Recommend Immediate Actions to Reduce Exposure Across all Operational Technologies and Control Systems – U.S. Department of Defense

CASE STUDY

In March 2020, Dragos identified an intrusion at a North American entity aligned with PARISITE activity that leveraged a vulnerability in Citrix Netscaler Application Delivery Controller (ADC) for initial access. CVE-2019-19781 was first identified in December 2019. PARISITE is known for quickly incorporating publicly identified vulnerabilities into attack operations and has also exploited vulnerabilities in Virtual Private Network (VPN) services.

Adversaries are quick to weaponize and exploit vulnerabilities in internet-facing services including Remote Desktop Protocol (RDP) and VPN services. New vulnerabilities revealed in the summer of 2020 impact critical network infrastructure services including F5, Palo Alto Networks, Citrix, and Juniper network devices will likely be exploited by ICS-targeting adversaries, if they are not already.[23] These vulnerabilities can enable adversaries to gain initial access to enterprise operations and potentially pivot into industrial operations.

ICS Vulnerabilities

In addition to the vulnerabilities in remote services discussed above, vulnerabilities in ICS-specific devices and services can introduce risk to the manufacturing environment. As of October 2020, Dragos researchers assessed and validated 108 advisories containing 262 vulnerabilities impacting industrial equipment found in manufacturing environments. Dragos found that almost half of the advisories described a vulnerability that could cause a loss of view and/or loss of control within a compromised environment.

Of the vulnerabilities assessed by Dragos impacting manufacturing industrial equipment, 70 percent require access to the victim network to exploit, 26 percent require an adversary to have access to the vulnerable device itself, and 8 percent require an adversary to be on the local area network to facilitate exploitation. Asset owners and operators are encouraged to be aware of the threat these vulnerabilities pose to manufacturing operations. A loss of view or control, for instance, may cause safety concerns and potentially put workers' lives or the environment at risk.

IP Theft

Dragos assesses with high confidence intellectual property theft and industrial espionage are major threats to manufacturing entities, especially by state-sponsored adversaries and malicious insiders. In the 2018 report Foreign Economic Espionage in Cyberspace,[24] the U.S. National Counterintelligence and Security Center stated China, Russia, and Iran are, "...three of the most capable and active cyber actors tied to economic espionage and the potential theft of U.S. trade secrets and proprietary information."

For example, insiders working on behalf of Chinese state interests have stolen or attempted to steal data from manufacturing and related entities including Dow Chemical[25] wind turbine manufacturer Sinovel Wind Group,[26] GlaxoSmithKline,[27] and biopharmaceutical company Genentech[28] In July 2020, the U.S.

23 Caught In The Middle With You – Joe Slowik, Dragos
24 Foreign Economic Espionage in Cyberspace – NCSC
25 Ex-Dow Scientist Is Convicted of Selling Secrets in China – New York Times
26 Chinese Company Sinovel Wind Group Convicted of Theft of Trade Secrets – U.S. DOJ
27 Second Former Glaxosmithkline Scientist Pleads Guilty to Stealing Trade Secrets to Benefit Chinese Pharmaceutical – Company – U.S. D
28 Former Genentech Employees Charged With Theft Of Trade Secrets – U.S. DOJ

Department of Justice (DOJ) published an indictment charging two Chinese nationals with hacking hundreds of victim organizations globally for over a decade on behalf of the Ministry of State Security and other Chinese government interests. Manufacturing and related companies accounted for at least five of the targeted victims, in addition to multiple other ICS entities. The adversaries operating under the Winnti Group umbrella have targeted manufacturing and other industrial entities globally, conducting initial access and espionage operations. The information could support China's Belt and Road Initiative (BRI), a massive land and sea infrastructure and economic development project across Asia, Europe, Indian Ocean, South Pacific, and East Africa.

CASE STUDY

In 2019, Bayerischer Rundfunk reported adversaries infiltrated automotive manufacturers BMW and Hyundai. These adversaries were linked to Vietnamese interests.[29] Car manufacturer VinFast – a subsidiary of VinGroup, the Vietnamese conglomerate with close ties to the country's government[30] – had recently closed a deal with BMW to license the carmaker's technology, architecture, and an engine, but not the manufacturing process or sequencing automation details.[31] It is possible adversaries were looking for data to further enrich the automotive manufacturing data already obtained by VinFast to improve production quality, though this is not confirmed. According to BMW, no sensitive data was obtained.

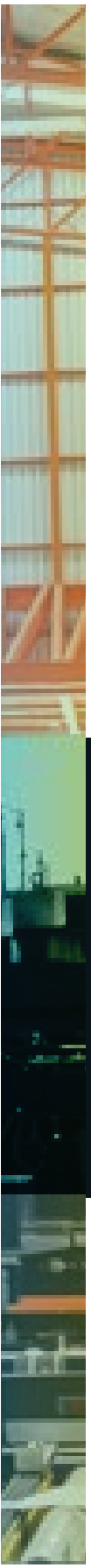
The coronavirus pandemic is also causing an increase in attacks targeting manufacturing related entities. As countries race to develop a vaccine for the pandemic that has killed more than one million people globally, adversaries have increasingly targeted pharmaceutical and healthcare organizations to steal ongoing research and development related to the virus and potential vaccines.[32] Currently, publicly reported attacks targeting entities researching and/or developing coronavirus vaccines and prevention have demonstrated intrusion and reconnaissance activities within enterprise resources, which could facilitate movement into operations or vaccine production tampering or disruption in a worst-case scenario.

IP and theft of trade secrets related to process and automation functions can enable industrial organizations and interested states and governments to fast-track development of critical infrastructure, including manufacturing. It can also support state-sponsored espionage activities for political or national security efforts. Obtaining material specifications for products is likely not enough to replicate them. Businesses rely on engineering and industrial design schematics, and sequencing automation details. According to Dragos researchers, adversaries may want to steal the algorithms, engineering designs, and programming specifications to replicate the entire production process, not just the material goods and services output.

Third-Party/Supply Chain

Since 2017, multiple threats migrated toward compromising vendors, Managed Service Providers (MSPs), and external network services as the first step in victim compromise. Adversaries can abuse existing trust relationships and interconnectivity to gain access to sensitive resources – including ICS

29 Autoindustrie im Visier von Hackern: BMW ausgespäht – BR
30 The Rise and Rise of a Vietnamese Corporate Empire – FT
31 VinFast – Follow The Birth of a Car Company Using BMW Tech and Italian Design from Pininfarina – TopSpeed
32 Exclusive: Iran-linked hackers recently targeted coronavirus drugmaker Gilead – sources – Reuters; DOJ says Chinese hackers targeted coronavirus vaccine research – Politico ; Advisory: APT29 targets COVID-19 vaccine development – NCSC; Chinese hackers accused of stealing information from Spanish centers working on Covid-19 vaccine – El País



systems in some cases – with little likelihood of detection.

Examples of this activity include activity groups DYMALLOY and ALLANITE that compromised vendors and contractors for subsequent phishing campaigns targeting the electric sector,[33] XENOTIME that targeted several original equipment manufacturers and vendors, and a widespread hacking campaign by APT10 that hijacked connections between MSPs and their customers, which included manufacturing organizations.[34]

Contractors, vendors, and other third-party individuals often have direct access to operational environments for activities like updates, inspections, or new equipment installations. It is possible for adversaries to compromise equipment used by these individuals as an access point into their ultimate target.

CASE STUDY

In 2018, a shipping industry group detailed an incident in which a bunker surveyor accidentally infected shipboard computers with malware.[35] The ship had completed bunkering operations, transporting oil to another ship, and the bunker surveyor came aboard to conduct quality assurance and documentation efforts. The surveyor asked to use a host in the engine control room to print documents and inserted a USB drive containing malware. The ship operators did not identify the malware until a subsequent cybersecurity assessment.

Enterprise Resource Planning (ERP) providers also provide potential infection vectors that could bridge the IT and OT gap if proper segmentation and security are not in place. ERP services require access to operations assets like data historians to monitor and store information relating to production, supply chain, inventory, and safety. They should be integrated into enterprise functions, like compliance or finance. Recent vulnerability exposures highlight the threat and potential exploitation of these systems. In July 2020, major ERP provider SAP published details and patches for a critical vulnerability affecting the SAP NetWeaver Application Server (AS) Java component impacting numerous SAP business solutions, including ERP. An adversary could use the vulnerability to take control of trusted SAP connections.[36]

Manufacturing entities are part of a global supply chain supporting multiple other industries, making them a target for adversaries targeting industries like electric utility or pharmaceutical. Some manufacturing companies' activities stretch into multiple industrial verticals. Automotive manufacturer Volkswagen in 2019 became a renewable power provider and aims to compete with energy companies on battery energy storage and management [37]

Leveraging third-party connections can enable an adversary to conduct espionage, reconnaissance, and data theft operations to pre-position themselves for a potentially disruptive OT attack. Due to interconnected relationships manufacturing companies have across industrial verticals, asset owners and operators should be aware of threats to all ICS entities and incorporate ICS-specific threat intelligence into security operations and risk management.

33 America's Electric Grid has a Vulnerable Back Door – and Russia Walked Through It – The Wall Street Journal
34 Inside the West's failed fight against China's 'Cloud Hopper' hackers – Reuters
35 The Guidelines on Cyber Security Onboard Ships – International Chamber of Shipping
36 Critical Vulnerability in SAP NetWeaver AS Java – CISA
37 Volkswagen plans to tap electric car batteries to compete with power firms – Reuters

IT/OT CONVERGENCE

Network Segmentation

The cybersecurity maturity of manufacturers varies based on industry, regulatory requirements, geographic location, and a variety of other factors. However, it is not unusual to see "flat networks" in manufacturing environments. This is when network connections are shared across both enterprise and operational segments. This makes it easier for an adversary to bridge the IT and OT boundary, and disrupt manufacturing operations after pivoting from an access point in IT.

If segmentation does exist between enterprise and operations leveraging jump hosts and access restrictions, manufacturing facilities often leverage the same Wide Area Network (WAN) connection across all manufacturing plants. This could enable an adversary to compromise an entire company's operations if they are able to access one facility's operations.

The perils of flat networks were broadly demonstrated in 2017. That year, WannaCry and NotPetya wormable ransomware and malware attacks spread across the globe, disrupting operations at numerous manufacturers.[38] The worms exploited a vulnerability in an old version of Microsoft's Server Message Block (SMB) protocol and continuous credential theft and reuse to spread. Due to interconnections between IT and OT via poor network segmentation, maintenance interconnections between environments, and a lack of access restrictions, malware wormed its way through industrial operations causing billions of dollars in losses.

Although the WannaCry and NotPetya events served as a wakeup call across manufacturers globally, three years later improper network segmentation remains an issue.

CASE STUDY

In 2020, Dragos observed EKANS ransomware incorporating domain checks to identify if a victim network's Windows Active Directory (AD) instance could be contacted. Honda was one of its victims, and the ransomware disrupted the automotive manufacturer's operations across five countries. This suggests poor network segmentation in at least parts of its global operations.[39]

Wi-Fi Connections

In addition to internet-connected process automation and other "smart" manufacturing processes, operators are adopting Wi-Fi enabled machine tools and diagnostic equipment that enable workers to move around plants and factories without tripping over power cords. Internet connected tools connect to historian databases for quality assurance, regulatory, and logistics purposes, among others. Often these tools are connected to enterprise or operations resources and can be used as network access points or targeted in an attack meant to

38 What is WannaCry ransomware, how does it infect, and who was responsible? – CSO Online; Honda halts Japan car plant after WannaCry virus hits computer - Reuters; The Untold Story of NotPetya, the Most Devastating Cyberattack in History – Wired

39 Honda's global operations hit by cyber-attack – BBC

disrupt production and impede operations.

Logistics applications and services enable moving parts of manufacturing assets – such as vehicles, drivers, and goods – to communicate and interact with static assets like warehouses or human resources. Employees and contractors use mobile and desktop hardware with Wi-Fi connections to use applications and services, and regularly access enterprise, and in some cases, operations networks.

CASE STUDY:

New Zealand meat processing company Affco experienced a ransomware attack in March 2020. The attack disrupted Affco's meat processing and delivery, sales and order fulfillment, and other business services. Although the initial infection vector is not publicly known, the ransomware had widespread disruption across the company's supply chain in IT and OT operations.[40]

Logistics technologies can ensure a timely, streamlined supply chain, but are very sensitive to any disruption. If one device in the logistics network is compromised, malware or adversaries can spread through all segments where the device connects. Time-sensitive operations rely on these services, and even a small incident can mean significant disruption to manufacturing operations and impact customers, products, and services..

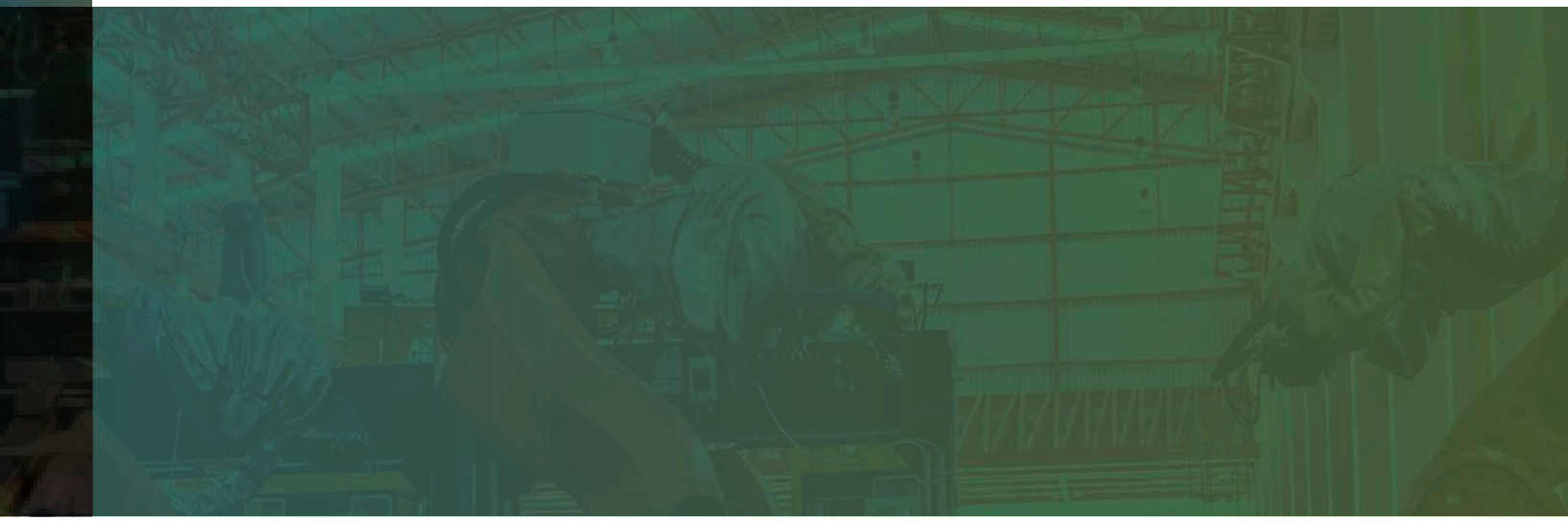
Lack of Visibility

As manufacturing operations become increasingly connected, a lack of visibility into processes, assets, and connections remain within these environments. It is difficult to defend against threats operators do not see.

According to the Dragos 2019 Year in Review report, 81 percent of organizations the Dragos Services team worked with had extremely limited or no visibility into the ICS/OT network. Observations from incident response engagements found no instances of security and process data aggregation for incident analysis requiring manual retrieval of logs and distributed analysis.

It is crucial that, moving forward, asset owners and operators across all manufacturing sectors and operations – including engineering, assembly, and logistics – improve network and host visibility to identify and defend against the growing threat landscape.

40 Affco and meat runs hit by computer snag – Newsroom



DEFENSIVE RECOMMENDATIONS

Manufacturing entities are all different, and the cybersecurity mechanisms, network architecture, and risk they are willing to accept will vary between industries. For instance, in food and pharmaceutical industries, regulations are in place to monitor safety and security of products manufactured and distributed to the public. However, the following recommendations should be practiced by all manufacturing entities to improve overall security of environments.

- Conduct architecture reviews to identify all assets, connections, and communications between IT and OT networks. Identify Demilitarized Zones (DMZs) to restrict traffic between enclaves. Critically examine and limit connections between corporate and ICS networks to only known, required traffic.
- Ensure an understanding of network interdependencies and conduct crown jewel analysis to identify potential weaknesses that could disrupt business continuity.
- Enforce Multi-Factor Authentication (MFA) wherever possible, especially on perimeter devices and login portals. Focus critically on connections to integrators, maintenance, vendor personnel, and crown jewels such as safety equipment. If MFA cannot be implemented on internal equipment, ensure strong, hard-to-guess passwords are used for all credentials.
- Ensure backups of enterprise network systems are maintained and test backups during disaster recovery simulations. Create an ICS specific incident response plan and conduct tabletop exercises to practice how to handle different incidents.
- Passively identify and monitor ICS network assets to identify key assets, chokepoints, and external communications in the network.
- Look for threat behaviors and known Tactics, Techniques, and Procedures (TTPs) that adversaries targeting manufacturing use, like those mapped to MITRE® ATT&CK for ICS.
- Monitor outbound communications from ICS networks to detect malicious threat behaviors, indicators, and anomalies. Understanding malicious behaviors exhibited by threat activity groups is crucial for defending against them.
- Identify and label critical ICS assets to aid with detection and monitoring. Dragos Asset Identification allows for certain analytics to function by detecting malicious behaviors against asset types.
- Leverage industrial-specific threat detection mechanisms to identify malware within OT and reinforce defense in depth strategies at the network level, leading to a more robust investigation ability by defenders and analysts.
- Ensure corporate networks are patched to prevent malware infections from entering the environment and to prevent subsequent propagation.
- Ensure that critical network services, such as Active Directory (AD) and the servers hosting it, are well-defended and that administrative access to hosting devices is restricted to the greatest degree possible.
- Evaluate and limit AD federation and sharing between IT and ICS networks to

the greatest extent possible. Among other items, create dedicated security groups for OT systems within a shared AD environment and limit permission for deploying Group Policy Objects (GPOs) or other changes to only a subset of administrators to reduce attack surface.

- Ensure networks are segmented to the greatest extent possible. If segmentation is not possible, ensure emergency response plans are well-documented to detail segmentation efforts in case of emergency such as a malware infection. For example, implement firewall rules to segment off critical ICS components from the network that can be activated and deactivated depending on the safety and security of the environment and any potential malicious activity.
- Services and equipment that are not needed for real-time communications or direct access to operations should be virtualized. This can improve vulnerability management and enable improved security for interdependencies. For example, Engineering Workstations (EWS) and Human Machine Interface (HMI) operations may be able to be virtualized.
- Isolate equipment and services used for Building Access Control (BAC) and Heating, Ventilation, and Air Conditioning (HVAC). These services can be considered secondary or support systems that are critical to maintaining safe, reliable manufacturing operations and considered potential targets for adversaries seeking to disrupt manufacturing production.

CONCLUSION

A concerning upward trend of ransomware targeting manufacturing companies leading to operations disruptions exists. Internet exposed assets, supply chain and third-party compromise risks, and a growing convergence of interconnected enterprise and operations networks are contributing to a growing threat landscape.

Dragos continues to monitor malicious activity groups and threats targeting manufacturing operations, including concerning ICS-aware ransomware capable of disrupting operations. Additionally, adversaries do not need to specifically target industrial processes to achieve widespread disruption across plants, fleets, or automation processes, as detailed in this report.

Dragos assesses with high confidence the threats to manufacturing will continue to increase over the next year.

TO LEARN MORE ABOUT DRAGOS AND OUR TECHNOLOGY, SERVICES, AND THREAT INTELLIGENCE FOR THE MANUFACTURING SECTOR, PLEASE VISIT WWW.DRAGOS.COM.