




Whitepaper

INFORMATION TECHNOLOGY (IT) THREATS IMPACTING OPERATIONAL TECHNOLOGY (OT) INFRASTRUCTURE

August 2022

Abdulrahman H. Alamri

Senior Threat Analyst II | Dragos, Inc.

 info@dragos.com

 [@DragosInc](https://twitter.com/DragosInc)

TABLE OF CONTENTS

Overview 1

Stage 1 of ICS Cyber Kill Chain as An Entry Point to ICS/OT 3

Ransomware 4

Vulnerability Exploitations 5

Supply Chain 6

Security Misconfiguration and Technical Failures 6

In Conclusion 7

References 8

OVERVIEW

Cyber threats have been rising over the past couple of years, targeting not only information technology (IT) systems but also industrial control systems (ICS) and operational technology (OT). There has been an increase of incidents in the headlines recently of attacks impacting ICS/OT in particular. Threats to industrial organizations' ICS/OT infrastructure are a newer problem that is growing at a faster rate. While IT threats can be very serious and damaging to a business, threats to ICS/OT infrastructure can have a much more powerful impact on a business, potentially disrupting operations, causing property and reputational damage, threatening personal safety, exacting ransoms, exposing proprietary information to cybercriminals, and bringing the entire business to a halt.

Due to the increased awareness of ICS/OT threats, industrial organizations have begun to invest more resources to secure their ICS/OT infrastructure. In 2021, SANS did a survey on ICS/OT cybersecurity that showed an increase in ICS cybersecurity hiring, budget allocations, and ICS cybersecurity investments by organizations around the world.¹

Industrial organizations have traditionally separated their IT and ICS/OT systems and departments. This allowed each camp to identify and focus on its own unique threats, risks, and vulnerabilities. Digital transformation and the need to keep everything connected have recently led to more IT/OT convergence, bringing the threats and risks from both worlds together.

DUE TO THE INCREASED AWARENESS OF ICS/OT THREATS, INDUSTRIAL ORGANIZATIONS HAVE BEGUN TO INVEST MORE RESOURCES TO SECURE THEIR ICS/OT INFRASTRUCTURE.

Security for enterprise IT infrastructure is essential, but with the on-going industrial digital transformation underway in many OT environments, maintaining system availability and the ability to operate is mission critical. Security, availability, and ability to operate for IT and OT cannot be separated as one can affect the other.² There are some similarities between IT and OT regarding some operating systems, technologies, and networks. However, the somewhat proprietary nature of OT-specific technologies, network protocols, and architecture make it more effort and time-consuming for threat groups and cybercriminals to understand and find ways to achieve the objective of impacting the victims' OT environment.

If adversaries aim to disrupt an industrial organization's operations, the attacker might use easier ways to achieve their objectives by initially targeting the IT systems and network. Digital transformation offers better chances for threat groups and cybercriminals to achieve their goals by targeting the IT infrastructure, which they are more familiar with, including its systems, network architecture, and vulnerabilities. Therefore,

digital transformation has been a challenge for the leadership of industrial organizations as the threat of exposure increases.³ Security professionals should not fear that a simple IT threat technique like phishing would bring their whole OT infrastructure down, as targeting specific OT technologies requires significant effort from adversaries, including time and research efforts to understand the nuances of OT technologies and how to disrupt these systems.

However, phishing could be the attacker's entry point to one of the victim's IT

servers, which is crucial for operational continuity or connected to other equally critical infrastructure. In order to protect industrial organizations from such threats, organizations need to do better in terms of IT/OT collaboration between IT operations teams and OT engineers. The responsibility of the IT/OT collaboration falls on the leadership of both organizations to first understand the need for it, and then to implement all the strategic, operational, and technical tools to coalesce these two functions. This paper will discuss some of the ways that IT threats can impact OT operations.

STAGE 1 OF ICS CYBER KILL CHAIN AS AN ENTRY POINT TO ICS/OT

Industrial organizations regularly deal with cyber attacks against their IT infrastructure, but these attacks could impact the OT side of the organizations' networks, dramatically increasing risk. Most of the attacks impacting ICS/OT reached the victims' enterprise networks first and then pivoted to the ICS/OT environment. We call this pivot Stage 1 of the ICS Kill Chain. Seventy-seven percent of the Dragos service engagements in 2021 involved issues with poor security parameters between IT and OT networks.

BUT FIRST, WHAT IS THE ICS CYBER KILL CHAIN?

Figure 1 at right shows Stage 1 of the ICS Cyber Kill Chain. Stage 1 of the ICS Cyber Kill Chain is very similar to the Lockheed Martin cyber kill chain, defined as "a cybersecurity model created by Lockheed Martin that traces the stages of a cyber attack, identifies vulnerabilities, and helps security teams to stop the attacks at every stage of the chain."⁴ However, we cannot consider an intrusion a Stage 1 of the ICS Kill Chain without one of the below conditions:

- Evidence suggests that the intrusion is targeting ICS/OT.
- Previous knowledge that the intrusion has been used to target ICS/OT.
- A known intent of attacking ICS/OT.
- An obvious opportunity allows the attacker to explore ICS/OT.
- The targeting of any IT components explicitly used to handle ICS/OT.



Figure 1: ICS Cyber Kill Chain

Dragos considers intrusion as Stage 1 of the ICS Kill Chain if the attacker aims to target the ICS/OT infrastructure by one of the above conditions. Otherwise, it would be considered an intrusion targeting the IT network regardless of the impact on the organization's operation. Dragos has observed the usage of the IT infrastructure as a pivot point to reach the ICS/OT side of the network by various threat groups. Among the techniques that threat groups are using to gain access to targeted infrastructure are spearphishing, supply chain compromise, exploitation of public-facing applications, and drive-by compromise techniques.⁵

Asset owners should evaluate the cost, benefits, and risk of the convergence or hyperconnectivity of IT and OT environments, especially when there is no absolute need for such connections or automation. According to the National Security Agency (NSA), OT connected to an IT network can be at risk of severe

destructive attacks.⁶ NSA recommends ICS/OT owners follow administrative recommendations to help mitigate the risks facing their critical systems and networks connected to IT networks. The 2015 Ukraine power event is an example of using the IT network as initial access to reach the OT network later. The attacker used spearphishing to

target IT employees using a weaponized Microsoft Word document with embedded BlackEnergy3. After the initial compromise, the attacker established a foothold in the IT environment, which enabled the attacker to move laterally to the ICS/OT network and cause the 2015 Ukraine power outage affecting approximately 225,000 customers in multiple areas.^{7,8}

RANSOMWARE

During the past couple of years, the risk of ransomware gangs' activities has increased to the point that ransomware will become the most common attack and the primary vector of compromise in industrial organizations in 2021. Looking back to the 2021 Dragos Year in Review report, manufacturing was the most impacted sector with 65% of all industrial organizations targeted, followed by the food & beverage sector with 11%, and the transportation sector with 8%.⁹ One of the reasons for the increase in ransomware activity in the industrial sector is the COVID-19 pandemic, where organizations adopted remote work policies allowing their employees to connect to the enterprise infrastructure remotely.

Even though most ransomware attacks target IT infrastructure, their effect can also impact OT systems that are connected to them or dependent on them. By crippling the IT systems that ICS/OT owners depend on, ransomware gangs had a tremendous impact on the business and operational continuity that could require lengthy recovery times for organizations.¹⁰ In most cases, the ransomware gangs usually post the leaked data from the targeted victims to sell them to other adversaries on dark websites. Once this happens

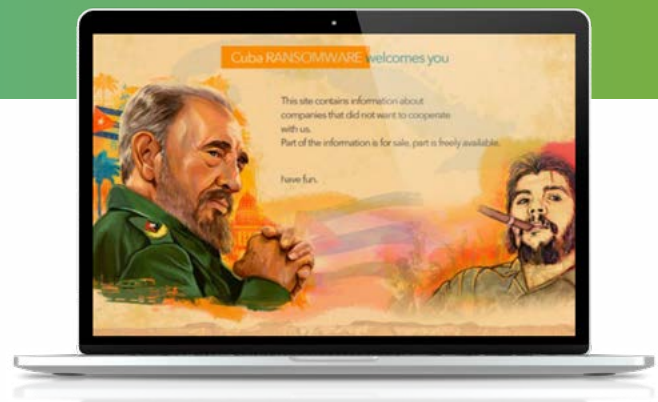


Figure 2: Cuba's dedicated leak site

victims can suffer from reputational damage, harm to or loss of human life, financial loss, the risk of data being leaked to other criminal groups, or the exposure of their customers' sensitive data.¹¹

In addition, Ransomware as a Service (RaaS) as a source of financial profits is growing as the number of RaaS cybergangs increased in recent years. In May 2021, the DarkSide ransomware gang caused the Colonial Pipeline operation to halt its OT operations after the group targeted the company's enterprise IT infrastructure. The DarkSide group compromised the Colonial Pipeline's domain controllers and then moved laterally to the other company's IT assets. Due to the lack of OT network visibility and proper segmentation between the IT and OT networks, the company decided to isolate the attack by halting the OT operations as a precaution to stop the attacker from reaching the

OT side of the network.¹² Even though the financial consequences of halting the Colonial Pipeline operation were enormous, the company knew that would be less

significant than the impact that might have occurred if the attacker had been able to get to the OT environment.¹³

VULNERABILITY EXPLOITATIONS

One of the ways that attackers might impact industrial organizations is by exploiting unpatched, public-facing applications in enterprise IT and OT infrastructures. Several of the Dragos-designated Threat Groups rely heavily on exploiting vulnerable public-facing applications that provide them with remote code execution capabilities. These threat groups include ELECTRUM, KAMACITE, PARASITE, and XENOTIME. Exploiting vulnerable public-facing applications is one of the most successful ways to compromise the victim's environment while sparing the attacker the effort of trying other techniques that the victims have detection or prevention controls in place against.

Threat groups take advantage of the noise following trendy vulnerabilities that are made public, making it difficult for government agencies and cybersecurity companies to attribute the activities to them. As an example of such a case, Dragos has observed successful exploitation of the Log4j vulnerability (CVE-2021-44228) among industrial organizations.¹⁴ Even though Dragos is not aware of any OT operational impact, the successful exploitation of the vulnerability could provide easy access to a victim's environment and adversaries can use this to disrupt the operations or even allow the attackers to move laterally to the OT side of the network. In 2021, the number of IT/OT security vulnerabilities broke the record of all time with 18,376 by the end of December 2021.¹⁵

THE TOP FIVE CRITICAL VULNERABILITIES FOR 2021 WERE:

VULNERABILITY NAME	COMMON VULNERABILITIES & EXPOSURES (CVE)
ProxyLogon	2021-26855
PrintNightmare	2021-1675 2021-34527
PetitPotam	2021-36942
PulseSecure	2021-22937
Log4shell	2021-44228

While there are many incidents of attackers successfully exploiting different vulnerabilities in industrial organizations' IT infrastructures, Dragos is unaware of any successful exploitation that led to the compromise of OT networks. However, the probability of using these vulnerabilities to get to the victims' OT networks is high because the mean time to detect (MTTD) for ICS/OT incidents is longer than it is in IT.

SUPPLY CHAIN

Supply chain attacks have been a hot topic after the widespread campaign launched by a state actor that modified the SolarWinds Orion business software. Around 18,000 organizations had installed the affected software out of a total of 300,000 SolarWinds customers globally.

The risk of the SolarWinds supply chain campaign to the industrial organization was that many ICS Original Equipment Manufacturers (OEMs) are known to use Orion directly in their products or as white-labeled security products. This campaign, dubbed Sunburst, installed a trojan malware that would create a backdoor for the hackers to the systems and networks of the SolarWinds' customers. In addition, there was a risk of leveraging the established foothold in an IT infrastructure of the entities that downloaded the trojanized software to enable the attacker to pivot to the OT network.¹⁶ Not all the supply chain attacks are massive, like the Sunburst campaign. Other supply chain attacks could be small and target a specific victim. For example, in August 2020, a supply chain attack targeted and impacted a mining and metals company. An end-user downloaded a trojanized piece of management software to administer an FS Network product from a digital video disk (DVD) they received from a high-speed networking solutions provider. The trojanized software contained a keylogger and remote access trojan (RAT). Luckily, the anti-virus was triggered, and the end-user did not execute the software.¹⁷

SECURITY MISCONFIGURATION & TECHNICAL FAILURES

The rapid increase of digital transformation and the dependency of OT systems on IT technologies add the risk of carrying over the IT problems to the OT realm. IT-centric problems and attack paths are rapidly becoming OT-oriented challenges.¹⁸ Lack of understanding and cooperation between IT and OT operators could affect ICS/OT systems' availability, security, and ability to operate. The recent event of the Polish railway's countrywide outage is an example of how IT-centric problems can impact industrial organizations' business and operational continuity. A data coding flaw in the traffic control system in several locations across the country caused a countrywide outage for more than 24 hours.^{19, 20}

An adversary can easily detect misconfigured servers, cloud services, and applications if exposed to the internet, and the risk that this issue poses to the infrastructure is significant. Misconfiguration has become a challenging IT security issue in the past few years as it is one of the top security vulnerabilities. "Misconfiguration" means outdated systems in the environment, default account settings, weak firewall protection, and improper infrastructure zoning.²¹

The best course of action to mitigate these risks would be to allocate budgets to the problem, hire qualified employees, and properly train staff. Undoubtedly, many industrial organizations are currently struggling with all of these mitigations. Among the top 10 most critical risks and vulnerabilities to application security, security misconfiguration moved from the 6th in 2017 to the 5th in 2021, as per the Open Web Application Security Project (OWASP).²²

2017	2021
A01:2017 – Injection	A01:2021 – Broken Access Control
A02:2017 – Broken Authentication	A02:2021 – Cryptographic Failures
A03:2017 – Sensitive Data Exposure	A03:2021 – Injection
A04:2017 – XML External Entities (XXE)	A04:2021 – Insecure Design [NEW]
A05:2017 – Broken Access Control	A05:2021 – Security Misconfiguration
A06:2017 – Security Misconfiguration	A06:2021 – Vulnerable and Outdated Components
A07:2017 – Cross-Site Scripting (XSS)	A07:2021 – Identification and Authentication Failures
A08:2017 – Insecure Deserialization	A08:2021 – Software and Data Integrity Failures [NEW]
A09:2017 – Using Components with Known Vulnerabilities	A09:2021 – Security Logging and Monitoring Failures*
A10:2017 – Insufficient Logging and Monitoring	A10:2021 – Server-Side Request Forgery (SSRF)* [NEW]

*From the Survey

Figure 3: OWASP Top 10 critical risks and vulnerabilities 2017/2021 comparison

IN CONCLUSION

It has been established that security threats and attacks can pose significant risk to a company's enterprise IT environment and its ability to thrive as a business. The risks amplify almost exponentially, however, when applied to an industrial organization's ICS/OT infrastructure.

The threats against industrial organizations and ICS/OT assets are not limited to the known direct ICS/OT threat vectors or the ICS-focused adversaries. The increased integration of IT and OT infrastructures in industrial organizations have been helpful for asset owners and industrial operators pursuing the higher productivity levels and other benefits gained from digital transformation. This has also helped episodically in periods like the COVID-19 pandemic when many employees had to work from home. However, the IT/OT convergence comes with multiple risks threatening industrial organizations' security, availability, and ability to operate ICS/OT assets. Adversaries can use the IT environment as a pivot point to move laterally to the ICS/OT infrastructure, use ransomware to disrupt organizations' operations, exploit vulnerable public-facing IT applications, or leverage supply chain compromise to gain access to victim's environments. In addition, human mistakes and systems technical failure can impact the organizations' ability to operate. Industrial asset owners and operators have a lot of different threat types to look out for and protect against.

REFERENCES

1. <https://www.sans.org/white-papers/SANS-2021-Survey-OTICS-Cybersecurity/>
2. https://www.researchgate.net/publication/352330231_ITOT_convergence_and_cybersecurity
3. https://securitydelta.nl/media/com_hsd/report/403/document/HSD-Rapport-OT-mei-2021.pdf
4. <https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html>
5. https://hub.dragos.com/hubfs/116-Whitepapers/Dragos_Intel_WP_InitAccess-IndEnviorns-Final.pdf?hsLang=en
6. https://media.defense.gov/2021/Apr/29/2002630479/-1/-1/1/CSA_STOP-MCA-AGAINST-OT_UOO13672321.PDF
7. <https://www.sans.org/blog/ukrainian-grid-attack-how-nerc-cip-like-measures-might-have-helped/>
8. [https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt6a77276749b76a40/607f235992f0063e5c070fff/E-ISAC_SANS_Ukraine_DUC_5\[73\].pdf?_ga=2.152185275.388594624.1655285200-1150768955.1655285200](https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt6a77276749b76a40/607f235992f0063e5c070fff/E-ISAC_SANS_Ukraine_DUC_5[73].pdf?_ga=2.152185275.388594624.1655285200-1150768955.1655285200)
9. <https://hub.dragos.com/hubfs/333%20Year%20in%20Review/2021/2021%20ICS%20OT%20Cybersecurity%20Year%20In%20Review%20-%20Dragos%202021.pdf?hsLang=en>
10. <https://hub.dragos.com/hubfs/333%20Year%20in%20Review/2021/2021%20ICS%20OT%20Cybersecurity%20Year%20In%20Review%20-%20Dragos%202021.pdf?hsLang=en>
11. <https://hub.dragos.com/hubfs/Whitepapers/Risk%20Assessment%20for%20Ransomware%20Prevention%20in%20OT%20Environments%20-%20Dragos%202021.pdf?hsLang=en>
12. <https://blogs.manageengine.com/corporate/manageengine/pam360/2021/06/15/the-colonial-pipeline-ransomware-attack-lessons-for-cybersecurity-teams.html>
13. <https://hub.dragos.com/hubfs/333%20Year%20in%20Review/2021/2021%20ICS%20OT%20Cybersecurity%20Year%20In%20Review%20-%20Dragos%202021.pdf?hsLang=en>
14. <https://portal.dragos.com/#/products/AA-2021-33>
15. <https://socradar.io/vulnerability-round-up-socradars-curation-of-critical-vulnerabilities-for-2021/>
16. <https://www.dragos.com/blog/industry-news/responding-to-solarwinds-compromise-in-industrial-environments/>
17. <https://portal.dragos.com/#/products/AA-2021-25>
18. <https://www.dragos.com/blog/industry-news/the-false-choice-of-it-vs-ot/>
19. <https://www.reuters.com/world/europe/technical-fault-halts-polish-railways-key-ukraine-exit-route-2022-03-17/>
20. <https://portal.dragos.com/#/products/AA-2022-16>
21. <https://outpost24.com/blog/What-are-security-misconfigurations-and-how-to-prevent-them>
22. <https://owasp.org/Top10/>

ABOUT DRAGOS, INC.

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

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

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

**TO LEARN MORE
ABOUT DRAGOS AND
OUR TECHNOLOGY,
SERVICES, AND THREAT
INTELLIGENCE FOR
THE INDUSTRIAL
COMMUNITY,
PLEASE VISIT**

www.dragos.com



THANK YOU