Trustwave SpiderLabs

2025 Trustwave Risk Radar Report

Manufacturing Sector

Trustwave®

Contents

Last year, Trustwave released its Manufacturing Threat Intelligence Briefing, analyzing attack flows specific to the manufacturing sector. The report provided insight into threat actors, actionable intelligence, and recommended mitigations for each stage of an attack.

Building on that foundation, our 2025 report takes a deeper dive into the evolving challenges and risks facing the manufacturing industry. The Trustwave SpiderLabs team highlights key trends reshaping the sector and offers a comprehensive breakdown of threat actor tactics categorized by attack stage, equipping manufacturers with critical knowledge to strengthen their cybersecurity posture.

In addition, Trustwave SpiderLabs has produced two detailed analyses focusing on pressing areas of concern: the convergence of informational technology (IT) and operational technology (OT) systems and the methods threat actors are using to target manufacturers. These reports provide in-depth research, offering manufacturers a clearer understanding of the current landscape and actionable risk mitigation strategies.

Cybersecurity in manufacturing is especially complex, driven by the increasing integration of IT/OT environments. These environments often span shop floor systems, enterprise networks, and interconnected supply chains, creating numerous attack vectors. Manufacturers are facing a growing array of threats—from ransomware attacks that disrupt production to data breaches exposing sensitive intellectual property. The adoption of Industry 4.0 technologies, including the Industrial Internet of Things (IIoT) and cloud-based platforms, has expanded the attack surface and introduced new vulnerabilities.

The average cost of a data breach in the manufacturing sector is $5.6 million— up from last year's figure of $4.7 million and higher than the overall industry average of $4.8 million. However, the full impact of a cyberattack can extend far beyond financial losses. Disruptions to production lines can lead to substantial financial losses, while breaches of sensitive design data or customer information can erode trust and damage brand reputation.

Critically, security incidents impacting OT can have severe safety implications. A compromised industrial control system (ICS) could lead to equipment malfunctions, hazardous material releases, or even physical injuries to workers on the production floor.

Therefore, robust cybersecurity measures are essential—not only to protect manufacturing operations and ensure business continuity but also to safeguard worker safety and prevent potentially catastrophic accidents.

Key Report Findings for the Manufacturing Sector

87%
of attacks originated from phishing

86%
of credential access techniques were brute-force attempts

19%
of ransomware attacks were conducted by Play

54%
of ransomware attacks were in the US

14%
of ransomware attacks targeted machinery manufacturers

Manufacturing's Unique Threat Landscape

Reliance on Legacy Systems:

- Many manufacturers continue to rely heavily on legacy systems and operational technologies that were designed long before modern cybersecurity challenges emerged. These outdated systems often lack the security features required to defend against today's advanced cyber threats. Due to their age and complexity, legacy systems can be extremely difficult, if not impossible, to update or patch regularly. As a result, they often contain known vulnerabilities that cybercriminals can easily exploit.
- For instance, brute-force attacks against outdated hardware and software can be a simple yet effective way for attackers to gain unauthorized access. Cybercriminals frequently target specific vulnerabilities in legacy systems, which are often widely documented, making it easier for hackers to conduct targeted, highly effective attacks. The risk is further compounded by the fact that many manufacturers lack the resources or expertise to replace or modernize these legacy technologies in a timely manner, leaving them vulnerable to exploitation.

Increasing Connectivity of Manufacturing Systems:

- The rise of IIoT and the increasing adoption of cloud-based platforms have dramatically expanded the connectivity of manufacturing systems. While these innovations offer significant benefits in terms of efficiency, automation, and data analysis, they also introduce a broader attack surface for cybercriminals to exploit. Manufacturing environments that were once isolated from external networks are now interconnected, creating new entry points for malicious actors.
- According to the Cybersecurity and Infrastructure Security Agency (CISA), there are over 1,200 known vulnerabilities and security issues associated with OT systems from more than 300 original equipment manufacturers (OEMs) and system providers. These vulnerabilities are often unpatched or poorly managed, increasing the likelihood of successful cyberattacks. The increased reliance on cloud platforms and remote access further complicates matters, as these systems are vulnerable to external breaches that may not be detected until damage has already occurred.

Potential for Physical Damage and Disruption:

- Cyberattacks on manufacturing operations carry significant risks that go beyond data theft or financial loss. These attacks can result in direct physical damage to critical infrastructure, production lines, and even employee safety. A successful cyberattack can disrupt entire manufacturing processes, leading to downtime, loss of production, or the destruction of expensive equipment. In some cases, such attacks can trigger safety incidents, including machine malfunctions or accidents that endanger workers.
- This combination of physical and operational risks makes cybersecurity a critical concern for manufacturers, as a breach could potentially have life-threatening consequences. For instance, attacks on ICS can cause machinery to operate in unintended ways, resulting in physical damage to products or equipment or even posing a risk to the health and safety of employees working in the affected environment.

TSMC Confirms Data Breach After LockBit Cyberattack on Third-Party Supplier

June 2023, **TechCrunch**

Ransomware Attack on US Navy Shipbuilder Leaked Information of Nearly 17,000 People

January 2024, **The Record**

Lack of Visibility and Control:

- Despite increasing awareness of cybersecurity threats, many manufacturers have yet to develop the necessary capabilities to secure their critical operational systems. While a large number of manufacturers have established procedures for detecting cyber events in their IT systems, far fewer have extended this monitoring to their OT environments, where the majority of critical manufacturing operations take place. Without proper visibility into their OT systems, manufacturers are unable to quickly identify and respond to threats, leaving them vulnerable to cyberattacks.
- Alarmingly, data suggests that 73% of OT devices are unmanaged, meaning they are not regularly monitored or updated by IT departments. This lack of visibility significantly increases the risk of undetected cyber incidents, as compromised devices could remain unnoticed until the damage is already done. In many cases, IT departments may not even be aware that a device is malfunctioning or has been compromised until the issue escalates to a point where it disrupts production or causes safety issues.

Cultural Mindset Gap:

- A major challenge in improving cybersecurity within the manufacturing sector is the cultural mindset gap that exists between traditional office-based enterprise environments and the industrial settings in which manufacturing occurs. Historically, the manufacturing sector has placed a greater emphasis on physical safety—such as ensuring that machines operate correctly and that workers are not exposed to hazardous conditions—while cybersecurity has often been seen as a secondary concern. This disparity can create resistance to implementing necessary cybersecurity measures, as the urgency of protecting digital assets may not be immediately apparent to those focused primarily on physical operations.
- Additionally, the broader manufacturing sector's risk management approach tends to prioritize short-term production goals over long-term cybersecurity investments, making it difficult to foster a culture of cybersecurity awareness. This cultural divide is reflected in risk assessments, with the manufacturing sector's cybersecurity risk score being 11.7% lower than the global average across all industries, indicating a systemic underestimation of digital risks and a lack of preparedness to address them.

Trustwave SpiderLabs

With more than 250 cybersecurity experts across the globe, the Trustwave SpiderLabs team puts its resources to task researching the top threats in today's landscape. We are uniquely positioned to do so, as we perform over 200,000 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 10k per day that are uniquely identified by Trustwave SpiderLabs. Our diverse coverage of infosec disciplines, including Advanced Continuous Threat Hunting, Digital 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 examines the myriads of threats facing the manufacturing industry. In addition to supplemental reports focused on IT/OT convergence and how threat actors are attacking manufacturing, Trustwave SpiderLabs will offer recommendations to help manufacturers mitigate risks and keep their operations undisrupted.

Notable and Prominent Trends in Manufacturing

Convergence of IT and OT

The Threat

We explore IT and OT convergence in depth in our accompanying report. At a high level, here are some key points to consider:

The convergence of IT and OT in manufacturing, while offering significant benefits like increased efficiency and automation, dramatically expands the attack surface and introduces complex cybersecurity risks.

Historically separated due to differing priorities (IT focusing on data and security, OT on physical processes and safety), the integration driven by Industry 4.0 and IoT exposes OT systems to a wider range of cyber threats.

OT systems, often legacy and lacking robust security measures, become vulnerable entry points for attackers. Breaches can lead to production downtime, safety incidents, reputational damage, and even pose risks to human life. The challenge lies in balancing the operational advantages of convergence with the critical need to secure these newly interconnected environments.

A key issue is the frequent prioritization of production uptime over cybersecurity concerns within OT environments, leading to vulnerabilities being overlooked until a disruptive incident occurs. The financial impact is substantial, with cybercrime costing manufacturers billions annually.

What Trustwave Is Seeing

At Trustwave, our experts help manufacturers tackle IT and OT convergence issues daily. They frequently encounter the following challenges:

- **The inherent conflict between production uptime and cybersecurity:** OT environments prioritize continuous operation, often at the expense of robust security measures. This conflict creates a vulnerability, as cybersecurity concerns are frequently addressed only after a production or safety incident occurs. This "if it ain't broke, don't fix it" mentality leaves systems vulnerable.
- **Skills gap in OT cybersecurity:** A significant shortage exists in professionals with the specialized knowledge to secure OT environments. This shortage is compounded by the cultural and priority differences between IT and OT teams, making it hard to find individuals who truly understand both worlds.
- **Limitations of traditional endpoint security in OT:** Many OT devices lack the processing power, memory, and storage required for traditional endpoint security software. This limitation necessitates alternative security approaches, such as passive network monitoring, which becomes a crucial line of defense.
- **Challenge of asset inventory in OT environments:** There is difficulty in maintaining a comprehensive inventory of OT assets. This lack of visibility makes it harder to identify vulnerabilities, manage patches, and effectively secure the environment. Often, even OT engineers only have deep knowledge of their specific production line, creating information silos.
- **Increasing attack surface:** While convergence offers benefits, it dramatically expands the attack surface. Previously isolated OT systems are now exposed to a wider range of cyber threats through their connection to IT networks. This interconnectivity creates new pathways for attackers to exploit.
- **Critical need for cross-functional collaboration:** It's vital to bridge the gap between IT and OT teams. Their differing priorities and risk perceptions can hinder effective security. Regular communication, joint training, and cross-functional exercises are essential for building a unified security approach.

Mitigations to Reduce Risk

- **Comprehensive Asset Inventory:** Developing and maintaining a detailed inventory of all OT assets, including their function and dependencies, is essential. This is crucial for understanding the attack surface and prioritizing security efforts.
- **Network Segmentation and Micro-segmentation:** Implementing robust network segmentation to isolate IT and OT networks and further micro-segmentation within OT to limit the impact of breaches.
- **Vulnerability Management and Patching:** Establishing a structured vulnerability management program, considering the unique constraints of OT environments, including limited downtime and the need for careful testing before patching. Prioritize patching based on risk and implement compensating controls where patching is infeasible.
- **Strong Authentication and Access Control:** Enforcing strong authentication and access control mechanisms, especially for legacy systems that may have inherent vulnerabilities. This work includes addressing weak default credentials and implementing multi-factor authentication where possible.
- **Security Monitoring and Incident Response:** Implementing robust security monitoring of OT networks, focusing on detecting anomalies and malicious activity. Developing and regularly testing OT-specific incident response and recovery plans, considering the critical nature of production environments. Passive monitoring is highlighted as a key technique due to the limitations of endpoint security in OT.
- **Cross-Functional Teams:** Building cross-functional IT/OT teams to foster communication, collaboration, and shared understanding of security risks and responsibilities.

Methods Used to Target Manufacturing

The Threat

We cover the ways manufacturers are targeted and breached in our accompanying report. At a high level, here are some key points to consider:

The most recent cyberattacks waged against our clients in the manufacturing industry highlight the increasing frequency of web shell deployments, the exploitation of system vulnerabilities, and the rise of social engineering tactics—especially phishing—used by cybercriminals to gain unauthorized access.

As manufacturers continue to digitize and integrate more connected technologies, the risk of sophisticated cyberattacks becomes ever more pronounced. The tactics employed by attackers are evolving, with many choosing to exploit weak spots in existing infrastructure, human vulnerabilities, or the digital supply chain.

Ransomware Attack Disrupts Bassett Furniture Manufacturing Facilities

July 2024, **SecurityWeek**

What Trustwave Is Seeing

We go into different tactics and techniques in the accompanying report, but one to highlight is vulnerability exploitation.

Manufacturing organizations had 4,370 unique vulnerabilities (out of a total of 24,920) publicly exposed on the Internet. 3,843 of these vulnerabilities are critical vulnerabilities, and 3,532 were listed in the Cybersecurity and Infrastructure Security Agency (CISA) Known Exploited Vulnerability (KEV) list, as seen in Table 1.

CVE ID	Description	Count
CVE-2021-40438	A Server-Side Request Forgery (SSRF) vulnerability in Apache HTTP Server versions up to 2.4.48. Exploiting this flaw allows attackers to force the server to forward requests to arbitrary destinations, potentially accessing internal systems.	1,603
CVE-2023-44487	Known as the "HTTP/2 Rapid Reset" vulnerability, this flaw allows attackers to exploit the HTTP/2 protocol to cause denial-of-service (DoS) conditions by rapidly resetting streams, leading to server resource exhaustion. In October 2023, multiple organizations reported large-scale DDoS attacks leveraging this vulnerability, prompting widespread advisories and patches.	836
CVE-2019-0211	A privilege escalation vulnerability in Apache HTTP Server versions 2.4.17 to 2.4.38. A local user with the ability to run scripts could execute arbitrary code with the privileges of the Apache server process.	471
CVE-2024-4577	A critical remote code execution vulnerability affecting PHP versions 5.x and onwards on Windows servers configured in CGI mode. Improper input validation allows attackers to execute arbitrary code on the server.	381
CVE-2020-0796	Also known as "SMBGhost," this is a remote code execution vulnerability in Microsoft's Server Message Block 3.1.1 (SMBv3) protocol. An attacker could exploit this flaw to execute code on the target server or client.	60
CVE-2012-1823	A vulnerability in PHP-CGI-based setups that allows remote attackers to execute arbitrary code or cause a denial of service via query strings, leading to code injection.	57
CVE-2014-0160	Known as "Heartbleed," this is a severe vulnerability in OpenSSL versions 1.0.1 through 1.0.1f. It allows attackers to read sensitive memory contents, potentially exposing confidential data.	41
CVE-2019-11043	A remote code execution vulnerability in PHP-FPM when used with NGINX. Improper handling of certain FastCGI requests can lead to arbitrary code execution.	31
CVE-2015-1635	A remote code execution vulnerability in the HTTP.sys component of Microsoft Windows. An attacker could send a specially crafted HTTP request to execute arbitrary code on the target system.	22
CVE-2019-0708	Dubbed "BlueKeep," this is a remote code execution vulnerability in Microsoft's Remote Desktop Services. Unauthenticated attackers can connect via RDP and execute arbitrary code on the target system.	15

Table 1. Vulnerabilities in manufacturing with respect to the CISA known exploited vulnerabilities catalog

Mitigations to Reduce Risk

For vulnerability exploitation specifically, which is only a fraction of what's covered in the report, mitigations include:

- **Patching and Vulnerability Management:** Implement a robust vulnerability management program that includes regular scanning (using tools like Nessus, Qualys, or OpenVAS) to identify weaknesses in systems and applications. Prioritize patching critical and high-severity vulnerabilities as soon as possible, following a documented and tested process. Establish a process to test patches in a non-production environment before deploying them to production systems to avoid introducing new issues. Consider using automated patching solutions where appropriate.
- **Vulnerability Scanning and Remediation:** Conduct frequent vulnerability scans (at least monthly and more often for critical systems) using automated tools. Prioritize identified vulnerabilities based on their severity (CVSS score) and exploitability. Develop a clear process for remediating vulnerabilities, including assigning responsibility, setting timelines, and tracking progress. Use vulnerability scanning results to inform patching priorities and other security measures.
- **Network Security (Firewall, IDS/IPS, Segmentation):** Implement and maintain firewalls to control network traffic, blocking unauthorized access and limiting communication between network segments. Deploy Intrusion Detection/Prevention Systems (IDS/IPS) to monitor network traffic for malicious activity and automatically block or alert on suspicious patterns. Segment the network to isolate critical systems (like OT) and limit the "blast radius" of a breach, preventing lateral movement by attackers.
- **Access Control (Authentication, Authorization, Least Privilege):** Implement strong authentication mechanisms, including Multi-Factor Authentication (MFA) wherever possible, to verify user identities. Enforce the principle of least privilege, granting users only the minimum necessary access rights to perform their job functions. Use Role-Based Access Control (RBAC) to manage user permissions efficiently. Regularly review and revoke access for terminated employees or those who no longer need it.

Ransomware Groups Continue to Target Manufacturers

The Threat

Ransomware attacks represent a significant and growing threat to manufacturers, with devastating consequences that extend far beyond financial loss. These cyberattacks are designed to infiltrate a company's network, encrypt critical files, and demand a ransom payment in exchange for decryption keys or to avoid the release of stolen data. Manufacturers are particularly vulnerable due to their reliance on outdated systems, the increasing interconnectivity of their operations, and the lack of adequate cybersecurity infrastructure in many cases.

Ransomware attacks disrupt business operations, halt production lines, and jeopardize supply chains. Beyond the immediate financial impact—such as ransom payments and recovery costs—there is the broader risk of damaging long-term relationships with customers, losing intellectual property, and facing regulatory consequences from data breaches.

Manufacturers' dependence on critical infrastructure, ICS, and operational technologies makes them even more susceptible. Compromised systems can not only lead to financial losses but also cause safety incidents, machine malfunctions, and even physical damage to production equipment, threatening people and assets.

Keytronic Reports Losses of Over $17 Million After Ransomware Attack

August 2024, **Bleeping Computer**

What Trustwave Is Seeing

Trustwave SpiderLabs analyzed ransomware incidents targeting the manufacturing sector and identified Play and Ransomhub as the predominant groups operating in this space. In our 2023 report, Play accounted for 9% of attacks, but this year, their share has increased to 19%. LockBit was the predominant group at 36%, but this year it has dropped to 12%.

Top Ransomware Groups

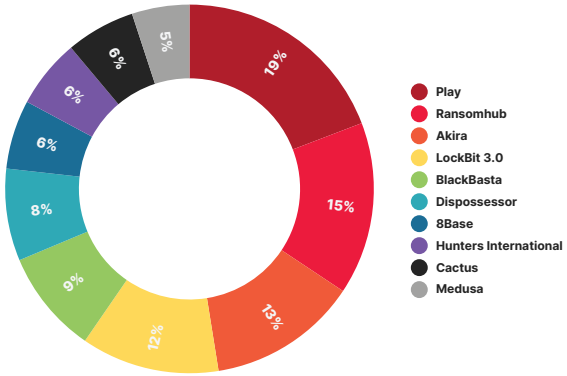

Figure 1: Top ransomware groups targeting manufacturing

From a global perspective, ransomware groups exhibit a clear focus on certain regions, with the United States bearing the brunt of attacks. Over half of the incidents in the dataset target US-based companies, highlighting their prominence in global manufacturing and their perceived capacity to pay high ransoms. The proportion of breaches affecting US companies stayed steady – accounting for 54% in our 2023 and 2025 reports.

In Europe, Germany and Italy emerged as critical hotspots, with attackers targeting advanced manufacturing technologies and niche industries such as automotive components and ventilation systems. These findings align with the broader strategy of ransomware actors, who prioritize victims with significant operational or intellectual value. Notably, the UK dropped from 12% in our 2023 analysis to 4% this year.

Top Countries Impacted

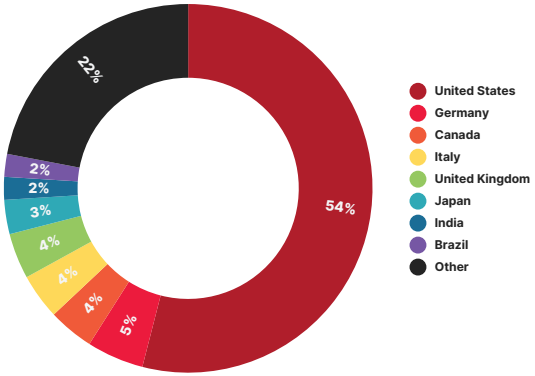

Figure 2: Manufacturing organizations affected by ransomware by country

Machinery manufacturers are the top target for ransomware attacks, accounting for 14% of incidents, followed closely by computer and electronics manufacturers and fabricated metal manufacturers, both accounting for 10%. It's important to note that no subsector is immune from these attacks. This distribution underscores the need for robust cybersecurity measures across all manufacturers.

Top Subindustries Impacted

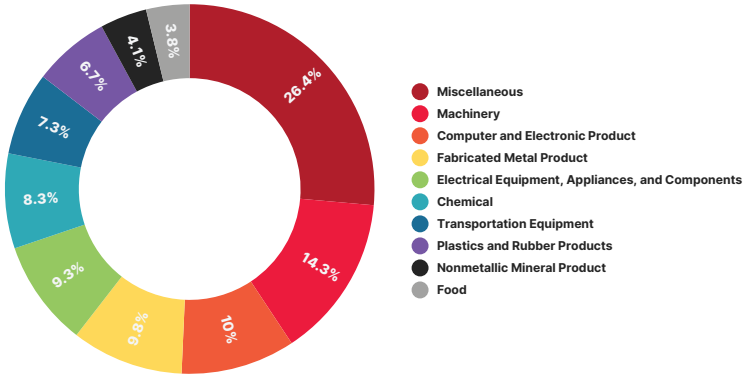

Figure 3: Ransomware attacks by manufacturer type

Mitigations to Reduce Risk

- **Enhance Cybersecurity Hygiene and Patch Management:** Many ransomware attacks exploit known vulnerabilities, especially in legacy systems. Manufacturers should ensure that all systems, including OT and IT infrastructure, are regularly updated with the latest security patches. The CISA Known Exploited Vulnerabilities (KEV) catalog is a useful resource for identifying and prioritizing patches for critical systems.
- **Implement Robust Backup and Recovery Plans**: Maintaining regular, encrypted backups of critical systems and data is essential to mitigating the impact of a ransomware attack. Backups should be stored offline or in isolated environments to prevent them from being encrypted during an attack. Manufacturers should also regularly test their recovery plans to ensure that systems can be restored quickly and with minimal operational disruption.
- **Network Segmentation:** Segregating operational networks (OT) from corporate networks (IT) is critical in limiting the spread of ransomware. In the event of an attack, this segmentation can prevent cybercriminals from accessing sensitive production systems. Additionally, manufacturers should adopt strict access controls and monitor network traffic for unusual activity that may indicate an ongoing attack.
- **Employee Training and Awareness:** Phishing emails and credential theft are common entry points for ransomware attackers. Educating employees on recognizing phishing attempts, practicing good password hygiene, and reporting suspicious activities can reduce the risk of initial compromise. Manufacturers should also conduct regular security training and simulated phishing exercises to reinforce these practices.

- **Multi-Factor Authentication (MFA) and Strong Credential Management:** Many ransomware groups gain access to systems through stolen credentials. Implementing MFA across all systems, especially for remote access, can significantly reduce the risk of unauthorized entry. Manufacturers should also ensure that access to critical systems is restricted to only those who need it, and credentials should be regularly updated.
- **Incident Response Planning:** A comprehensive incident response plan is essential to minimizing the impact of a ransomware attack. This plan should include clear steps for containing and mitigating the attack, restoring systems, and communicating with stakeholders. Manufacturers should test their incident response plans through tabletop exercises and ensure that external cybersecurity experts are ready to assist if needed.
- **Collaboration with Law Enforcement:** In the event of an attack, manufacturers should report the incident to relevant law enforcement agencies. These organizations can assist in tracking down perpetrators, identifying trends, and offering support for recovery. Additionally, collaborating with other industry players and cybersecurity experts can help manufacturers stay informed about emerging threats and best practices.

Mexico's 'Timbre Stealer' Campaign Targets Manufacturing

February 2024, **Dark Reading**

Threat Actor Techniques by Attack Stage

Data breaches and compromises come in many forms but often follow a similar pattern. Attackers gain access, escalate privileges, establish a foothold, steal or destroy data, and then vanish. Trustwave SpiderLabs analyzed data from across our clients to understand the path that threat actors take within the manufacturing industry and the techniques they deploy at each stage.

Initial Access Techniques

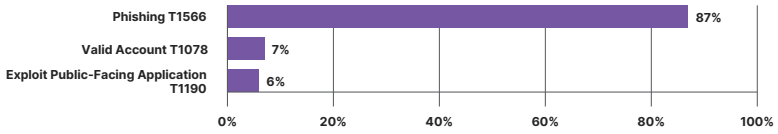

Figure 4: Initial access techniques used by attackers of manufacturers

A majority of all initial access techniques used by threat actors to gain entry to manufacturing entities were phishing (87%). Most of the phishing attempts were generic and leveraged social engineering with links to external websites. However, use of malicious .xlsx attachments with macros was also observed.

Following that, threat actors exploited valid accounts (7%) and public-facing applications (6%). Exploit procedures observed in the initial access attempts against web applications were mostly Log4j CVE-2021-44228 – accounting for 69% of the observed cases and ZeroLogon CVE-2020-1472 – 7%. Notably, some attackers also tried to leverage Microsoft Exchange Server vulnerabilities, which are known to be exploited by ransomware groups.

Execution Techniques

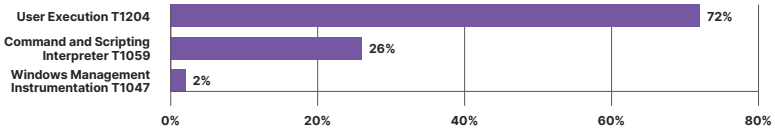

Figure 5: Execution techniques used by attackers of manufacturers

Execution techniques observed in the manufacturing security incidents mostly involved User Execution of malicious files and links (72%), followed by malicious uses of PowerShell scripts and commands (26%). Some commands were found to be a result of CrackMapExec toolkit execution. In one case, the execution of a malicious word document (.doc) with a macro downloader was observed.

We observed very few execution cases of malicious java scripts and Windows command shell commands. Windows Management Instrumentation (WMI) commands used to download payloads and remote process execution were also noted.

Persistence Techniques

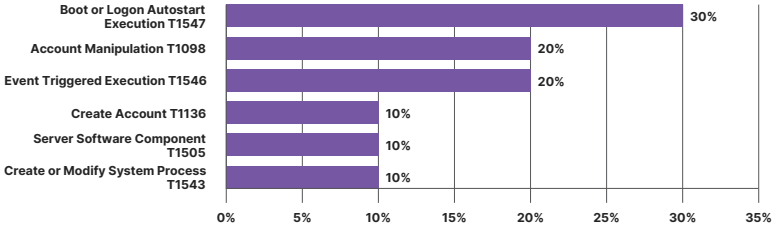

Figure 6: Persistence techniques used by attackers of manufacturing

The persistence techniques observed were Boot or Logon Autostart Execution (30%), Account Manipulation (20%), Event Triggered Execution (20%), and other techniques such as Account Creation (10%).

Account manipulation involves modifying existing accounts to either maintain access or escalate privileges. For example, an attacker might change account permissions or add their credentials to an existing user account to retain access. Account creation refers to the creation of new user accounts by attackers. Threat groups use these new accounts to maintain access or to disguise their activities as legitimate users.

Defense Evasion Techniques

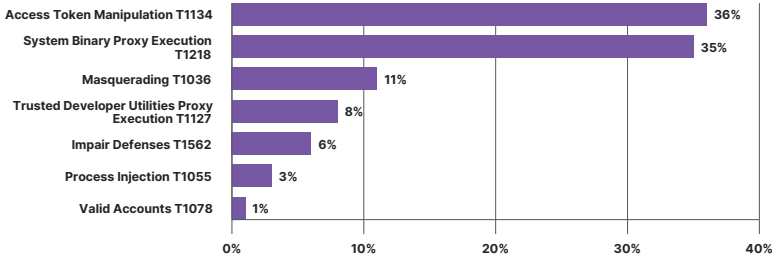

Figure 7: Defense evasion techniques used by attackers of manufacturing

Defense evasion techniques observed in the manufacturing security incidents mostly utilized access token manipulation (36%) and system binary proxy execution (35%) using Rundll32, WScript. Masquerading using process names such as setup.exe, pdfconverter.exe, and uses of multiple file extensions such as .pdf.exe were observed (11%).

Credential Access Techniques

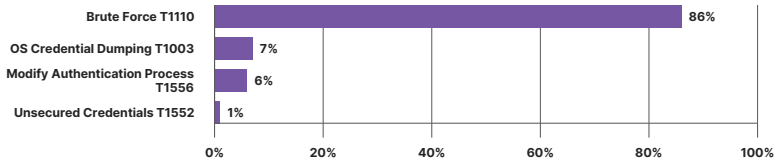

Figure 8: Credential access techniques used by attackers of manufacturing

Credential access techniques observed in the attacks relied mostly on brute-force attempts and generic brute-force attacks (86%). We also observed OS credential dumping attempts using CrackMapExec and Mimikatz (7%) and authentication process modification (6%).

Lateral Movement Techniques

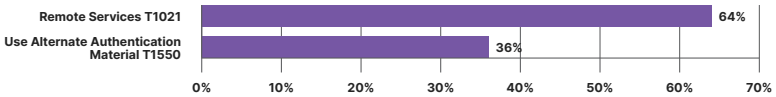

Figure 9: Lateral movement techniques used by attackers of manufacturing

To move laterally within manufacturing organizations, attackers relied mostly on Remote Services (64%), specifically Remote Desktop Protocol (RDP) and Use of Alternate Authentication Material (36%).

Crown Equipment Confirms a Cyberattack Disrupted Manufacturing

June 2024, **Bleeping Computer**

Conclusion & Key Takeaways

Conclusion

As the manufacturing sector continues to evolve, so too do the complexities and threats associated with its cybersecurity. The increasing convergence of IT and OT systems, along with the growing reliance on interconnected technologies such as IIoT and cloud-based platforms, has expanded the attack surface, leaving manufacturers vulnerable to a wide range of cyber threats. The findings of this report highlight the persistent and diverse nature of these risks, from ransomware attacks and credential theft to the critical impact of cyberattacks on physical operations and worker safety.

Manufacturers must recognize that the consequences of a breach extend far beyond financial losses. Data theft, production disruptions, and damage to brand reputation are just the beginning; compromised OT systems can lead to real-world safety hazards, putting workers and critical infrastructure at risk. Moreover, the reliance on legacy systems, lack of visibility into OT environments, and cultural gaps in prioritizing cybersecurity create significant challenges that need immediate attention.

To effectively mitigate these risks, manufacturers must adopt a proactive, multi-layered cybersecurity strategy that includes robust monitoring of both IT and OT systems, investment in modern technologies, and fostering a culture of cybersecurity awareness across all levels of the organization. By implementing the insights and recommendations provided in this report, manufacturers can better defend against evolving threats and ensure the safety and continuity of their operations in an increasingly digital world.

Key Takeaways:

- **IT/OT Convergence Risks:** The convergence of IT and OT systems expands the attack surface and introduces complex risks. OT systems, often legacy and lacking robust security, become vulnerable entry points.
- **Legacy Systems:** Many manufacturers rely on outdated systems that lack modern security features, making them susceptible to brute-force attacks and exploitation of known vulnerabilities.
- **Increased Connectivity:** The rise of IIoT and cloud-based platforms increases connectivity and creates new entry points for malicious actors.
- **Physical Damage:** Cyberattacks can result in direct physical damage to critical infrastructure, production lines, and employee safety. Compromised industrial control systems could lead to equipment malfunctions or hazardous material releases.
- **Lack of Visibility and Control:** Many manufacturers lack the capabilities to secure their OT systems, with 73% of OT devices being unmanaged.
- **Cultural Mindset Gap:** A cultural gap exists between IT and OT environments, with a greater emphasis on physical safety than cybersecurity, leading to an underestimation of digital risks.
- **Ransomware Attacks:** Ransomware is a significant and growing threat to manufacturers, with groups like Play and Ransomhub being particularly active. The US is the most targeted country for ransomware attacks in the manufacturing sector.

Manufacturers must prioritize cybersecurity to protect operations, ensure business continuity, and safeguard worker safety. This requires a proactive approach that includes comprehensive risk management, robust security measures, and a culture of cybersecurity awareness.


Trustwave®