CYBLE

Manufacturing Sectoral Report

July 2023

Table of Contents

Executive Summary

The Critical Manufacturing Sector is a vital part of the National Economy. Organizations within this sector process raw materials and produce highly specialized parts and equipment that are essential to primary operations in other Critical Infrastructure (CI) sectors. The sector comprises several industries that serve as the sector's core, including Primary Metals Manufacturing, Machinery Manufacturing, Electrical Equipment, Transportation Equipment, Appliance, Component Manufacturing, etc.

The Critical Manufacturing sector holds the utmost value among other CI sectors as the products developed within this sector are further employed for the economic benefit of an institution or a Nation. For example, in situations such as war or a pandemic, the exportation of machinery/equipment used in Defense Weapons and Pharmaceutical medicines offers exporters a significant global strategic edge.

Safeguarding the production and distribution processes becomes paramount to maintaining uninterrupted operations. Hence, this industry faces the crucial task of addressing various threats, including physical, human, and cyber risks, to ensure the security of their supply chains.

Cyber-attacks in this industry can have a catastrophic impact on the victim organization as well as the state, depending upon the assets/devices exploited.

Example:

1. If an attacker can manipulate Industrial Control System (ICS) assets, they may disrupt operations at the site and even inflict physical harm to on-ground operators & assets. A similar scenario was observed the previous year in Iran When Gonjeshke Darand (Predatory Sparrow) took responsibility for launching a cyber attack on Iran's Steel Industry. This incident highlights "How close TAs can reach ICS assets and inflict Physical Damage."
2. Ransomware attacks targeting organizations & vendors dealing in Critical Manufacturing from January 2023 are ramping up with each passing month. The recent ransomware campaign launched by CL0P by exploiting MoveIT emphasizes this issue.

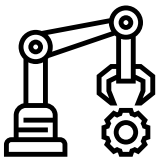
The examples above show that the convergence of Information Technology (IT), Operational Technology (OT), and Industrial Internet of Things (IIOT) assets within the Manufacturing sector provides a huge attack surface to Threat Actors (TAs), via which they can inflict desired damage to organizations.

Cyble Research & Intelligence Labs (CRIL) continuously monitor the emerging threat landscape in the Manufacturing sector to remain ahead of the risk curve.

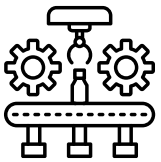
Process within Critical Manufacturing Sector

There are different types of manufacturing processes used in the Critical Manufacturing Sector. The following are the five types of manufacturing processes mentioned in the search results:

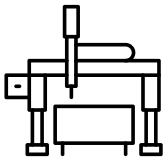
1. **Repetitive Manufacturing**
2. **Discrete Manufacturing**
3. **Job Shop Manufacturing**
4. **Continuous Process Manufacturing**
5. **Batch Process Manufacturing**



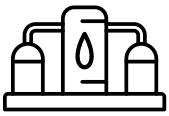
Repetitive Manufacturing:
This type of manufacturing involves creating the same product on an assembly line. It is used for products that are produced in large quantities and require minimal customization. Examples of industries that utilize this type of production process include electronic appliances.



Discrete Manufacturing:
In this type of process where a specified quantity of material moves as a unit between workstations, and each unit maintains its unique identity. Metal Stamping production is one of the examples of this process.

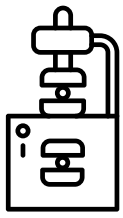


Job Shop Manufacturing:
Job shop manufacturing involves creating custom products that are made to order. This type of manufacturing is used for products that require a high degree of customization and are produced in small quantities. Examples of industries that utilize this type of production process include machine shops, commercial printing shops, and woodworking.



Continuous Process Manufacturing:
This type of manufacturing involves creating products that are produced continuously, such as chemicals or oil. The production process is not interrupted, and the product is created in a continuous flow.

Continuous processes are generally used to produce a large quantity of product per year. Examples of industries that utilize this type of production process include chemicals, fuels, and plastic.



Batch Process Manufacturing:
Batch process manufacturing involves creating products in batches. Some applications require specific quantities of raw material to be combined. Batch processes are generally used to produce a relatively low to immediate quantity of product per year. Examples of industries that utilize this type of production process include adhesives, beverages, and pharmaceuticals.

It is important to note that the specific manufacturing processes used in the Critical Manufacturing Sector may vary depending on the unique requirements of each industry or product, resulting in the utilization of varied software and hardware from multiple vendors.

Threat Landscape & Early Intelligence

Cyberattacks on the Manufacturing sector are increasingly becoming fast-paced. The more concerning issue is that the threat actors are quick to discover the security gaps and can develop exploits to target these loopholes more vigorously than ever before.

Vulnerabilities

Organizations dealing in the Critical Manufacturing sector work in conjunction with ICS & IT assets such as Programmable Logic Controllers (PLC), Human Machine Interface (HMI), SCADA, Industrial Routers, Networking devices, Conveyer Technologies, Monitoring Software, Remote Services, etc.

Due to the interoperability environment, the risk of cyber-attacks on an organization is multifold, and other factors, such as insider threats, misconfigurations, improper network segmentation, etc, further deteriorate the situation.

Below is the list of critical CVEs, affecting products widely used in the Manufacturing Sector.

Critical Severity Vulnerabilities in Manufacturing Sector

S. No	Vendor	Product	CVE
1	Advantech	R-SeeNet: versions 2.4.22 and prior	CVE-2023-2611
2	Advantech	WebAccess/SCADA: All versions before 9.1.4	CVE-2023-1437
3	Mitsubishi Electric Corporation	MELSEC Series CPU module	CVE-2023-1424
4	Johnson Controls Inc.	OpenBlue Enterprise Manager Data Collector: Firmware versions before 3.2.5.75	CVE-2023-2024
5	Teltonika	Teltonika's Remote Management System version 4.14.0	CVE-2023-2586
6	Rockwell Automation	Rockwell Automation Kinetix 5500 devices	CVE-2023-1834
7	Industrial Control Links	ScadaFlex II SCADA Controllers	CVE-2022-25359
8	Rockwell Automation	ThinManager ThinServer	CVE-2023-27855
9	AVEVA	AVEVA Plant SCADA and AVEVA Telemetry Server	CVE-2023-1256
10	Omron	CJ1M PLC	CVE-2023-0811
11	Mitsubishi Electric	MELSOFT iQ AppPortal	CVE-2023-31813
12	Siemens	COMOS	CVE-2023-24482
13	Siemens	Brownfield Connectivity Client: All versions before V2.15	CVE-2022-1292
14	Weintek	EasyBuilder Pro	CVE-2023-0104
15	Delta Electronics	DVW-W02W2-E2: Version 2.42	CVE-2022-42139
16	Delta Electronics	DX-2100-L1-CN: Version 1.5.0.10	CVE-2023-0432
17	SAUTER Controls	Nova 200–220 Series (PLC 6)	CVE-2023-0052
18	InHand Networks	InRouters	CVE-2023-22600

Security Alerts by Vendors in Manufacturing Sector

From January 2023 to June 2023 - Cybersecurity Infrastructure Security Agency (CISA) released **69 Critical Manufacturing-related advisories** highlighting the magnitude of vulnerabilities in this sector.

Vendor	Count
Schneider Electric	2
Mitsubishi Electric	11
SpiderControl	1
Advantech	4
SUBNET Solutions Inc	1
Rockwell Automation	6
Sensormatic Electronics, a subsidiary of Johnson Controls, Inc.	1
Atlas Copco	1
Delta Electronics	5
Horner Automation	2
Carlo Gavazzi	1
Johnson Controls Inc.	3
Rockwell	1
Teltonika	1
Omron	2
Datakit	1

Vendor	Count
FANUC	1
JTEKT ELECTRONICS CORPORATION	2
Industrial Control Links	1
SAUTER	2
ABB	2
RoboDK	1
AVEVA	1
Autodesk	1
B&R Industrial Automation	1
Rittal	1
Siemens	8
Weintek	1
SnapOne	1
XINJE	1
InHand Networks	1
RONDS	1

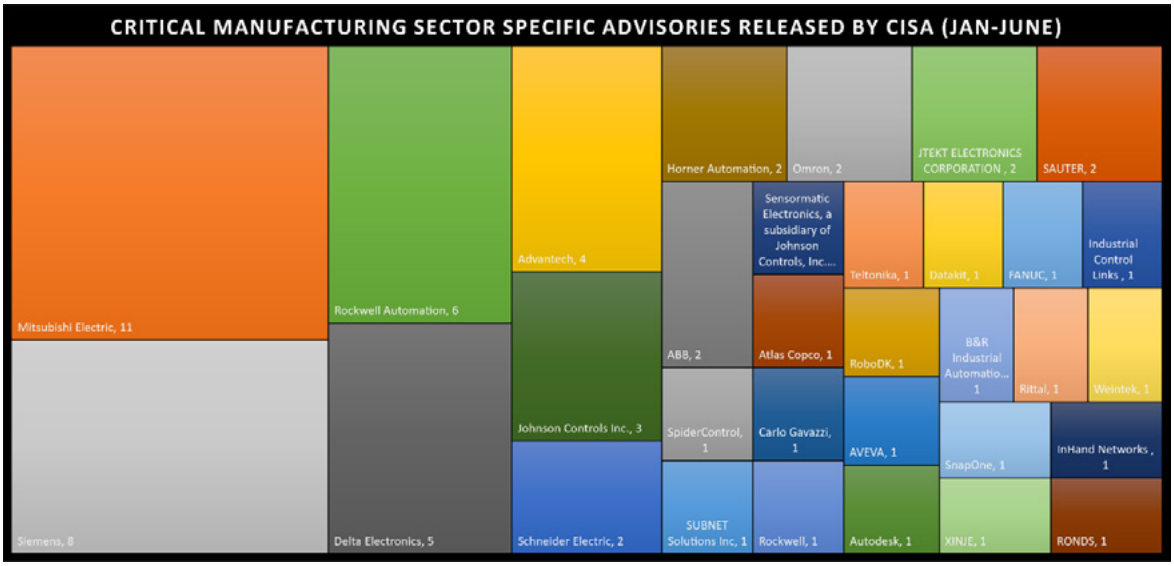


Figure 1: Graph representing vendors that released advisories for Jan 2023 - June 2023

Vulnerable Products within Manufacturing Sector

Most security advisories that CISA released in H1-2023 fall under 'Critical' & 'High' severity category.

The image below provides insights into these vulnerable products in their respective categories.

Cyble Global Sensor Intelligence – Manufacturing Sector

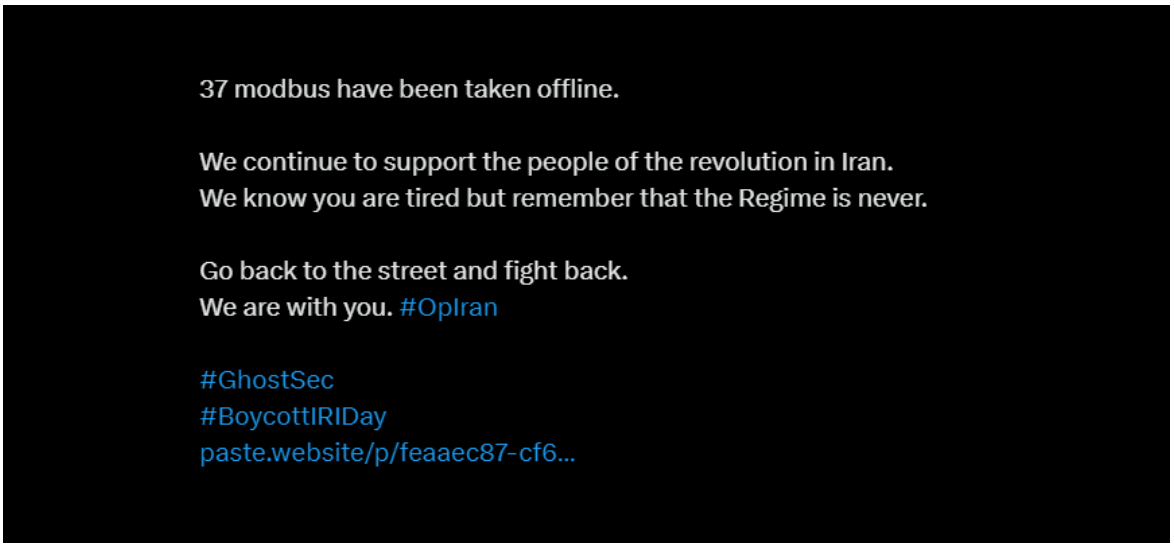
Cyble actively monitors exploitation attempts towards the Manufacturing Sector via The Cyble Global Sensor Intelligence (CGSI) network. We have recently picked up early intelligence about these exploitation attempts through our CGSI network towards Industrial Control System (ICS) protocols used in the Manufacturing sector, such as Modbus, S7Comm, and EtherNet/IP.

Modbus

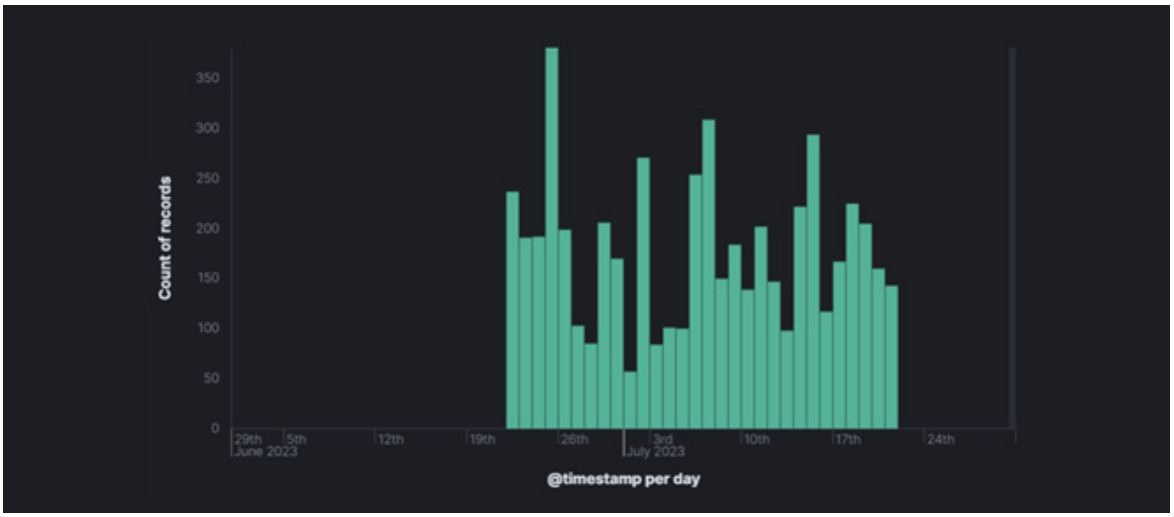
In the Critical Manufacturing sector, Modbus plays a crucial role in connecting various critical components such as Programmable Logic Controllers (PLCs), Supervisory Control and Data Acquisition (SCADA) systems, and Human-Machine Interfaces (HMIs). It enables real-time monitoring of essential manufacturing parameters, such as temperature, pressure, and flow rates.

For instance, in a pharmaceutical manufacturing plant, Modbus enables seamless communication between PLCs controlling the production equipment and SCADA systems supervising the entire manufacturing process. Its straightforward implementation and support for multiple physical layers make it a popular choice in many critical manufacturing applications.

With multiple Proof of Concepts, custom scripts, command line tools, and high exposure of ICS devices over the internet, TAs & Hacktivist groups have made several claims about exploiting ICS protocols in the past few months. One such claim was seen around Operation Iran by GhostSec, where they claimed to have targeted Modbus.



A statistical representation of perceived attacks by CGSI towards Modbus is as below:

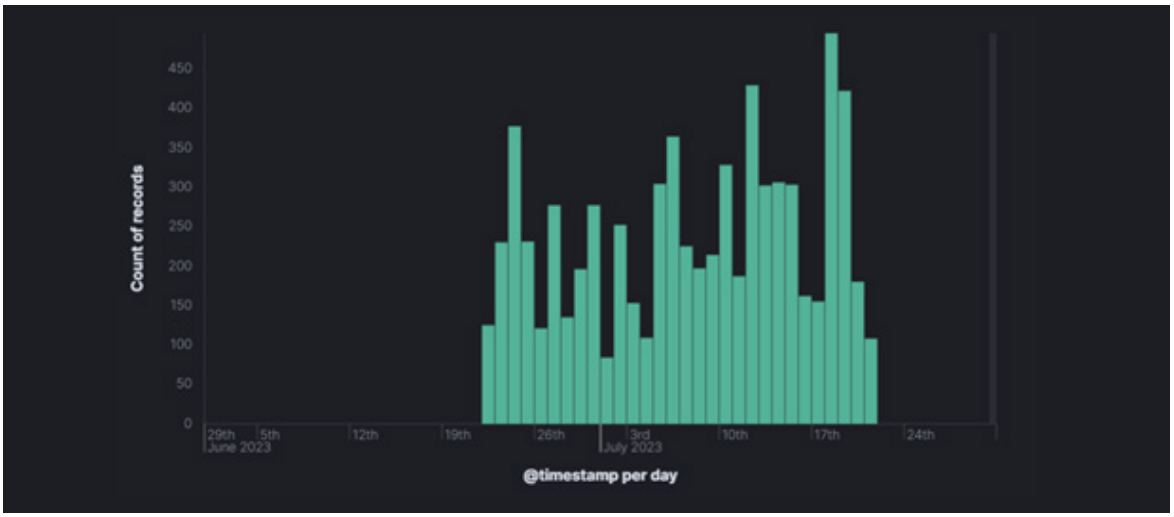


S7Comm

In the Critical Manufacturing sector context, Siemens' S7Comm protocol finds extensive use in large-scale industrial facilities where Siemens PLCs are prevalent. S7Comm ensures fast and secure data exchange between PLCs, HMIs, and engineering systems, enabling advanced automation and process control.

For instance, S7Comm facilitates efficient communication between PLCs controlling robotic arms and other automation equipment in an automotive manufacturing plant, allowing precise assembly and production operations. Its ability to handle complex data types and support for Siemens-specific features enhances its utility in sophisticated manufacturing processes.

A statistical representation of perceived attacks by CGSI towards S7Comm is as below:

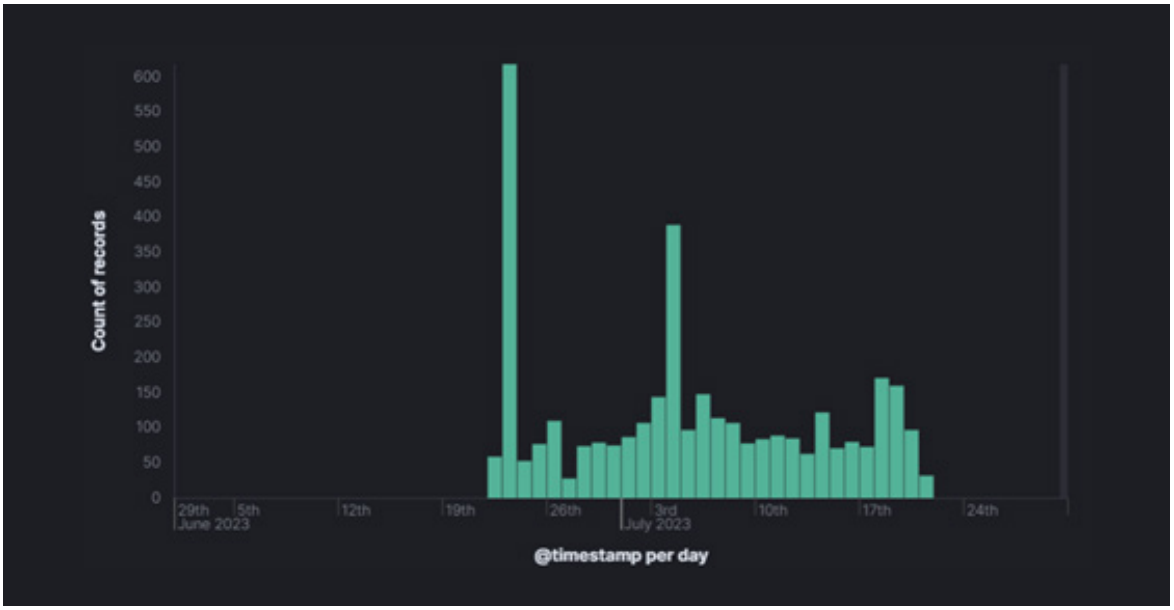


S7Comm

EtherNet/IP stands out in the Critical Manufacturing sector due to its robustness, scalability, and compatibility with standard Ethernet infrastructure. In manufacturing environments where diverse devices from different manufacturers need to communicate seamlessly, EtherNet/IP is a widely used open standard protocol.

For example, in a semiconductor fabrication facility, EtherNet/IP enables communication between various equipment, including wafer-handling robots, process chambers, and metrology tools, ensuring precise control and data exchange. Its support for both cyclic and acyclic communication allows for real-time control and efficient data exchange, making it a preferred choice for critical manufacturing applications.

A statistical representation of perceived attacks by CGSI towards EtherNet/IP is shown below:



CRIL Early Intelligence

1. Out of the given list of vulnerabilities, CISA has pointed out that Proof of Concepts (POCs) for exploiting vulnerabilities related to **Delta Electronics & Industrial Control Links** products are publicly available.
2. CRIL has observed internet-exposed instances of **Advantech R-SEENET**, a monitoring application that collects information from routers, processes it, and presents it to network administrators.

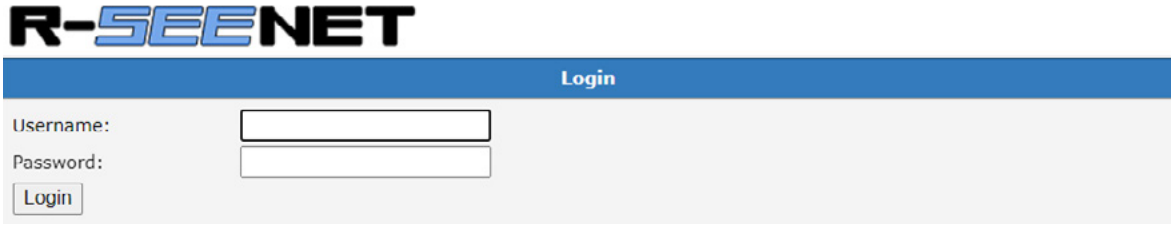


Figure 2: Internet exposed R-SEENET instance

Internet scanner results reflect that R-SEENET might be vulnerable to exploitation. Given below are versions exposed over the internet and are susceptible to attacks.

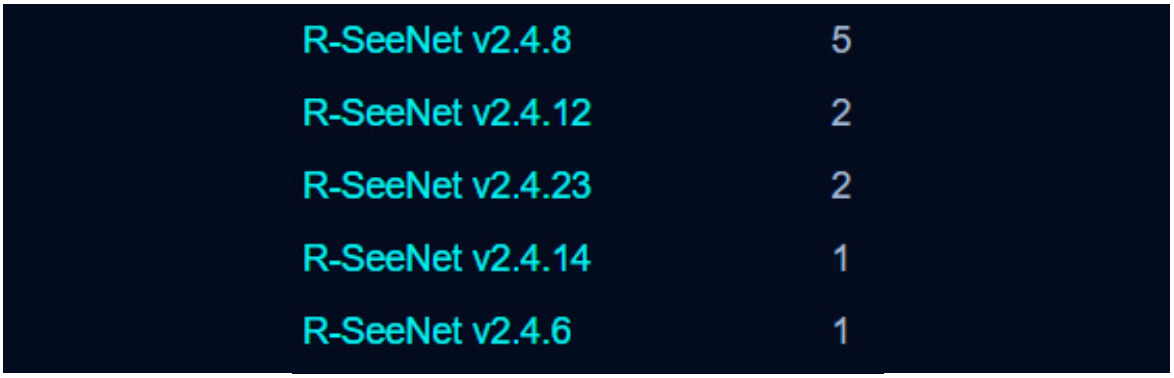


Figure 3: R-SEENET Versions exposed over the Internet

3. During the investigation, multiple **Advantech WebAccess** were also observed to be exposed over the internet. Advantech WebAccess is a software solution that serves as the core of Advantech's IoT solutions. It is a complete browser-based software package for Human Machine Interface (HMI) and Data Acquisition and Supervisory Control (SCADA). Vulnerabilities such as RCE, SQL, and Directory Traversal exist in older product versions.

Figure 4: Internet exposed Advantech WebAccess/SCADA [1]

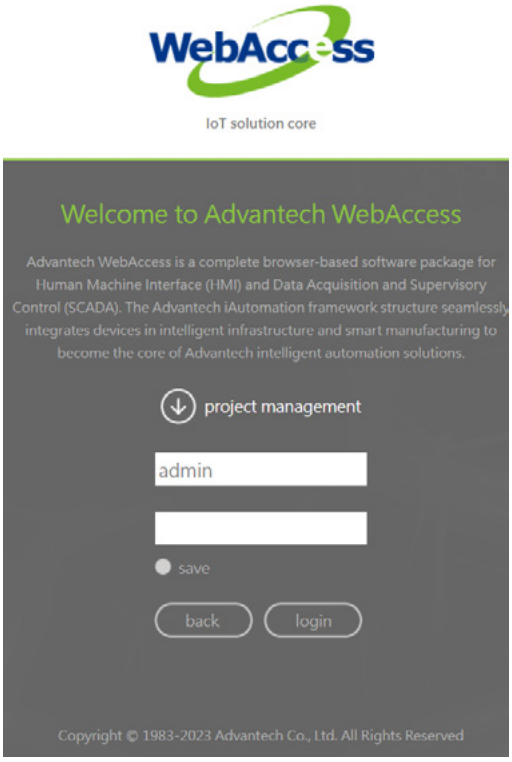


Figure 5: Internet exposed Advantech WebAccess/SCADA [2]

4. Organizations dealing in Critical Manufacturing rely on Programmable Logic Controllers (PLC) to operate heavy machinery. The given below chart shows the internet exposure of **Mitsubishi Programmable** Controllers.

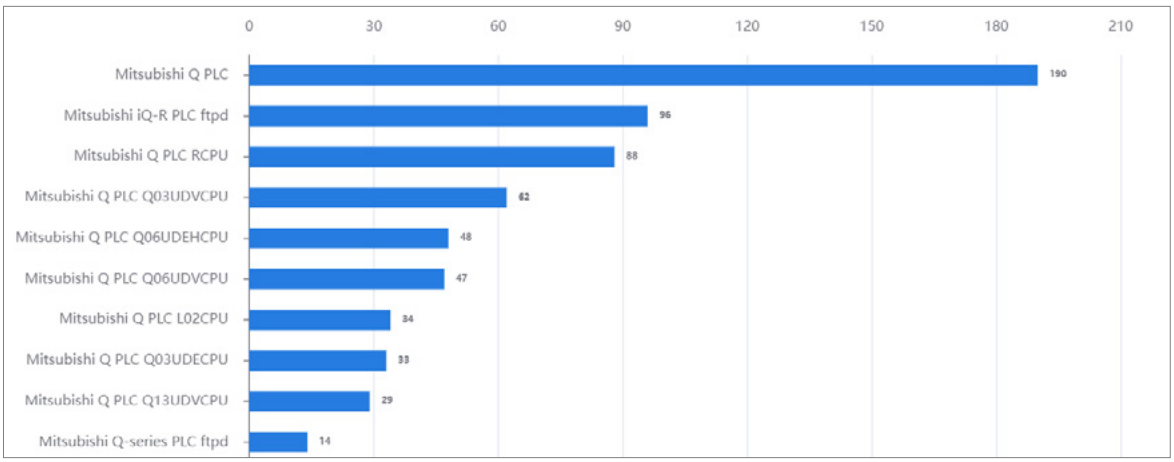


Figure 6: Internet exposure of Mitsubishi Q-PLC range

As Programmable Controllers can be controlled by Ethernet and FTP (File Transfer Protocol), if PLCs are left exposed over the internet. If these controllers rely on default/ factory configurations, the threat actors may utilize the same communication channels to send malicious commands to these controllers.

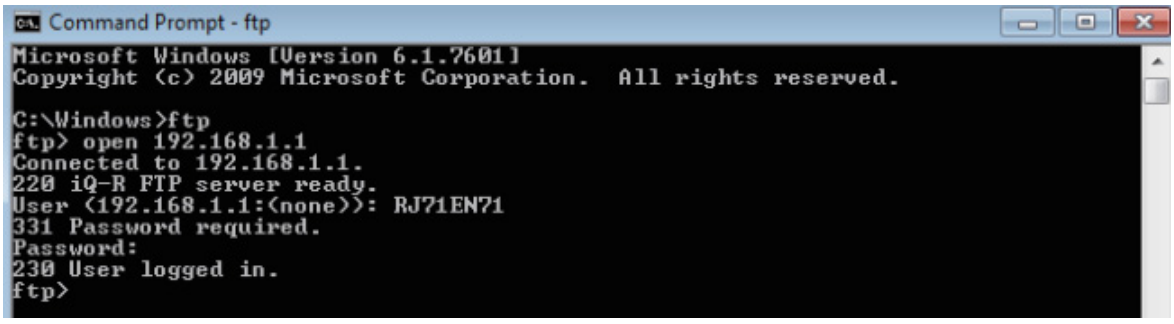


Figure 7: FTP and logging into the Ethernet-equipped module [Source: Link]

5. Human Machine Interface (HMI) is a technology that enables communication between humans and machines. Operations within manufacturing facilities include conveyer belt movement, mixing raw materials, processing raw materials, etc. Researchers observed that multiple **Weintek cMT Series HMI** are exposed over the internet.

Figure 8: Internet exposure of Weintek cMT Series

The image below enunciates the Top 5 countries with the highest number of Weintek cMT Series HMI exposures.

Figure 9: Top 5 Countries with the highest exposure to Weintek cMT Series

6. The ControlLogix EtherNet/IP (ENIP) communication module is a component used in industrial systems for communication purposes. These products are used in multiple industrial verticals, including but not limited to, manufacturing, electric, oil and gas, and liquified natural gas. There are vulnerabilities in communication modules, including Remote Code Execution (RCE) & Denial Of Service (DOS), which were recently targeted by Advanced Persistence Threat (APT) actors.

   CRIL observed that the Rockwell Automation communication modules have significant internet exposure in the United States (US) region.

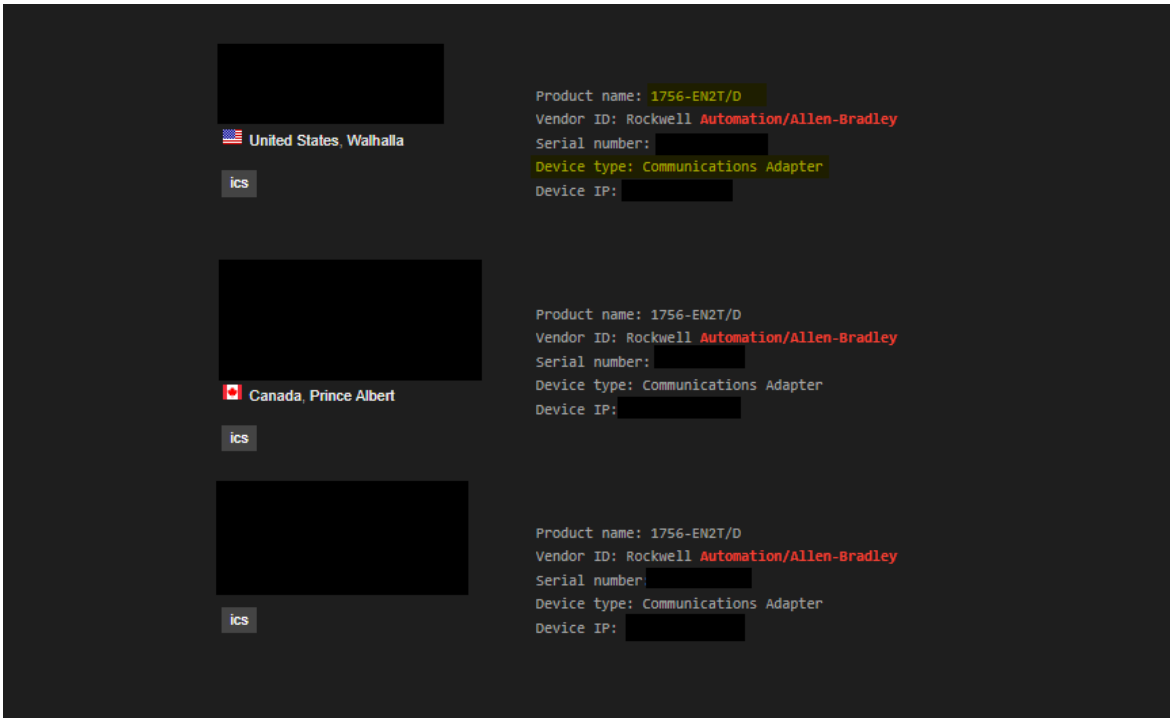


Figure 10: Internet exposed of Rockwell Communication Modules

7. **The PowerMonitor 1000** is a compact and cost-effective electric power and energy metering device designed for industrial control applications used in critical manufacturing.

   The device is intended for use in industrial control applications, where it can be used for load profiling, cost allocation, energy control, and power management. Researchers observed that PowerMonitor 1000 has internet exposure. Given below is the screenshot from one of the internet-exposed instances.

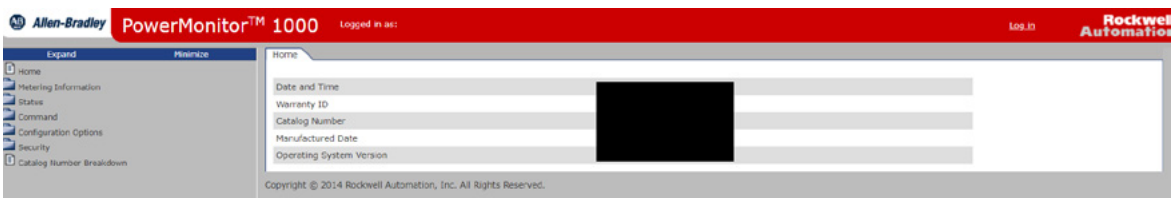


Figure 11: Internet exposed PowerMonitor 1000

8. Teltonika RMS (Remote Management System), a product of Teltonika Networks, is a remote management platform designed to monitor and manage networking devices. Recently CISA released a security advisory for multiple vulnerabilities in RMS and RUT model routers.

   The advisory states, "Successful exploitation of these vulnerabilities could expose sensitive device information and device credentials, enable remote code execution, expose connected devices managed on the network, and allow impersonation of legitimate devices."

   CRIL observed that there is high exposure of Teltonika RUT routers. Even though not all the exposed assets need to be vulnerable, the high exposure instead provides a wider attack surface to the TAs.

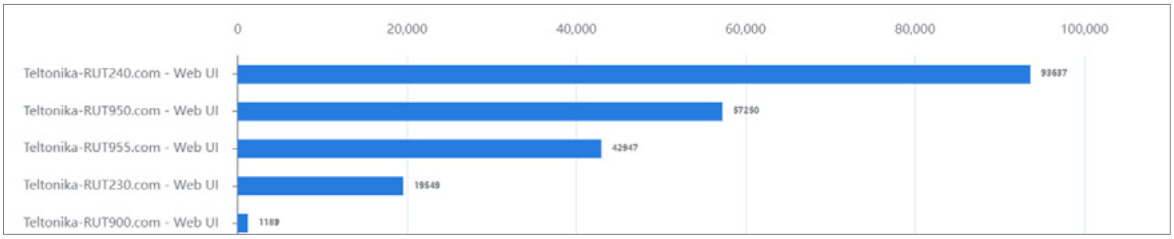


Figure 12: Statics of Internet-exposed Teltonika RUT range

9. Streamlining of warehouse processes is imperative to supply-chain management in the Critical Manufacturing sector. Inventory Management Systems play a crucial role in this management. However, being web-based, they need to be updated with the latest security patches. If these systems are not updated or misconfigured, a cyber-attack via these systems can disrupt operations in a warehouse.

   CRIL observed multiple misconfigured Warehouse Management Solutions exposed over the internet.

   The figure below highlights the criticality of such instances.

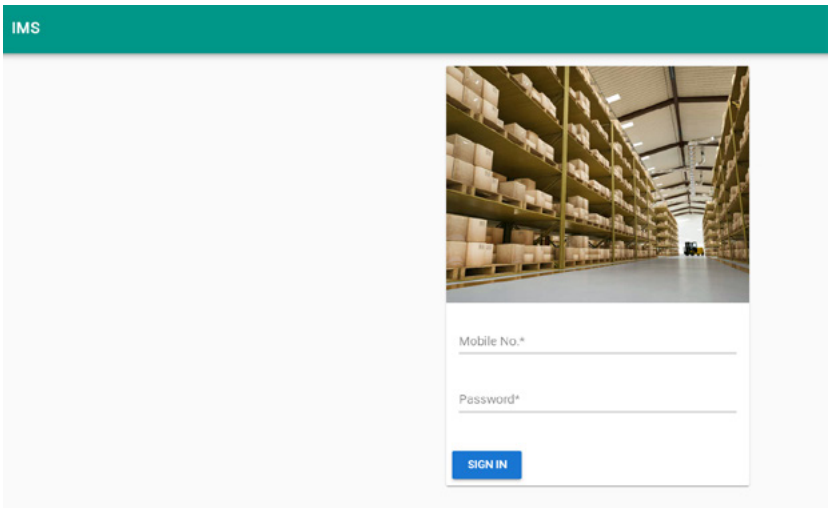


Figure 13: Internet exposed Inventory Management System [1]

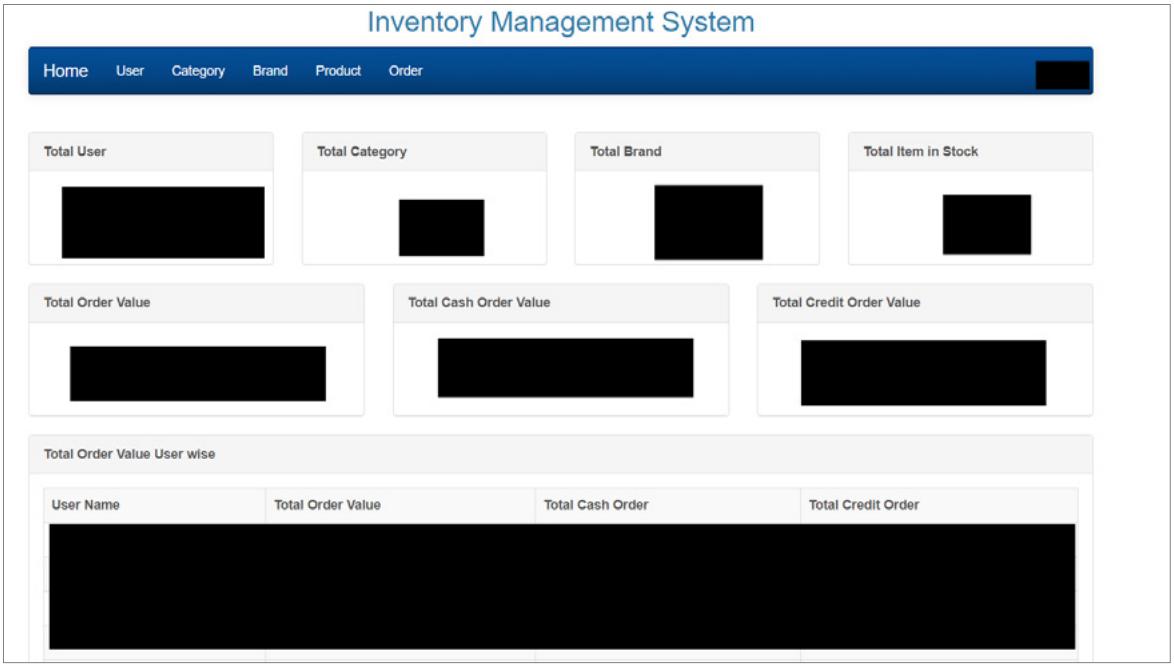


Figure 14: Internet exposed Misconfigured Inventory Management System [2]

Figure 15: Internet exposed Inventory Management System [3]

10. Virtual Network Computing (VNC) is a remote desktop protocol that allows users to access and control a computer's graphical desktop environment over a network connection. VNC is commonly used by system administrators to remotely control a system for maintenance or to use shared resources.

    However, if VNC endpoints are not properly secured with a password, they can serve as entry points for unauthorized users, including threat actors with malicious intentions.

Hacktivist groups generally target internet-exposed VNCs to target ICS environments. A recent example of the same is Team1919 targeting VNC exposures in Sweden.

CRIL observed that ICS assets connected via VNC are generally sold & distributed over Darkweb Markets. Below is a screenshot where a TA sells a list of IPs connected via VNC.

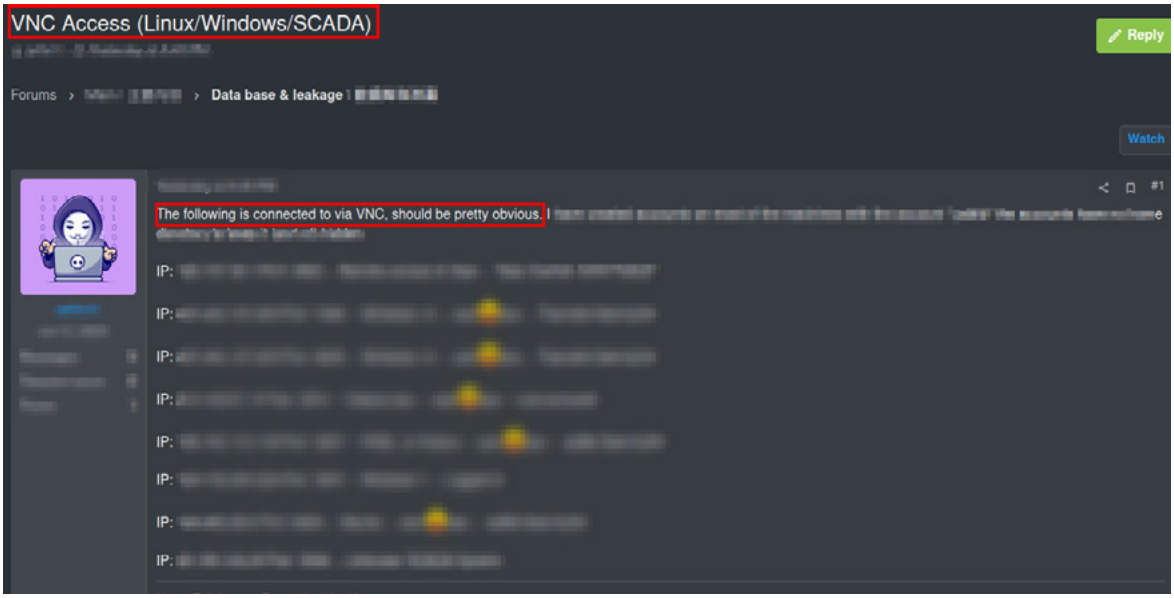


Figure 16: TA selling VNC Access over Darkweb

Further, the particular threat actor was also providing access to SAW Control System. Given below is a screenshot for the same.

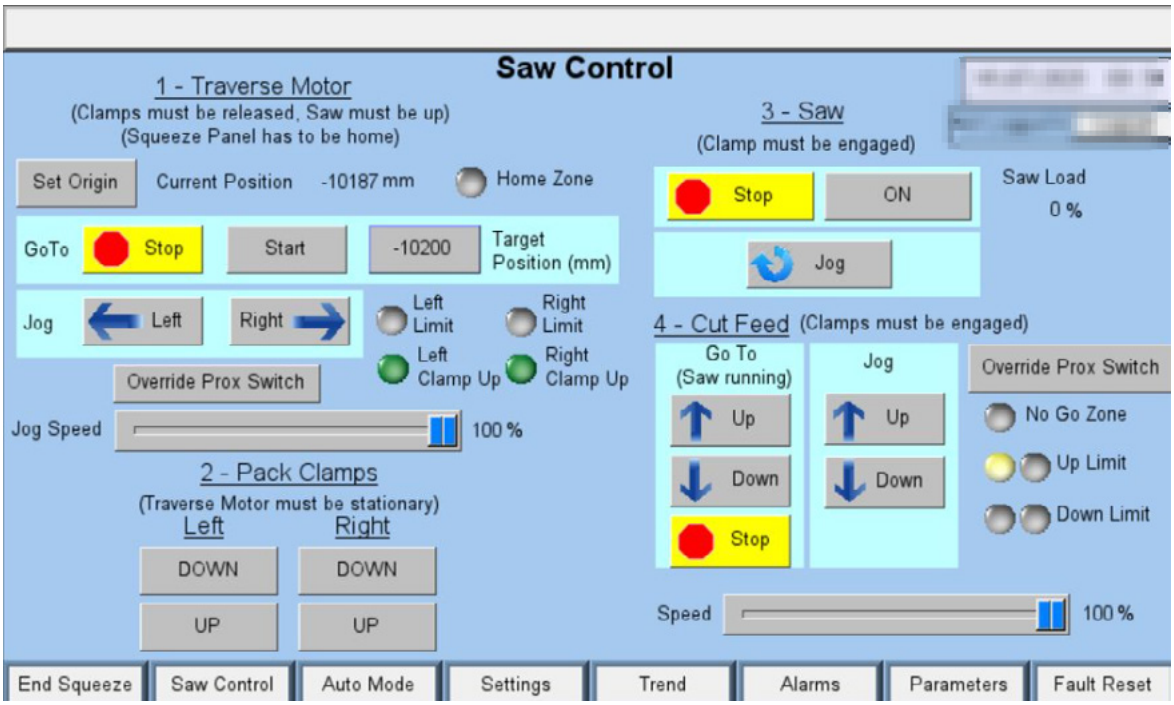
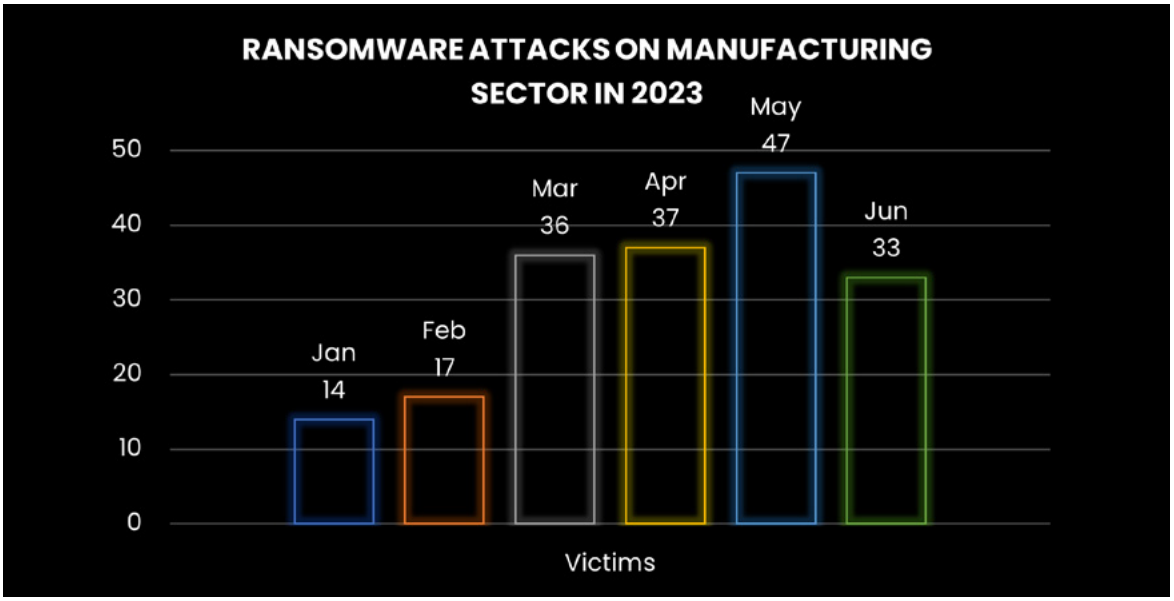


Figure 17: VNC sold over dark web points to SAW Control system

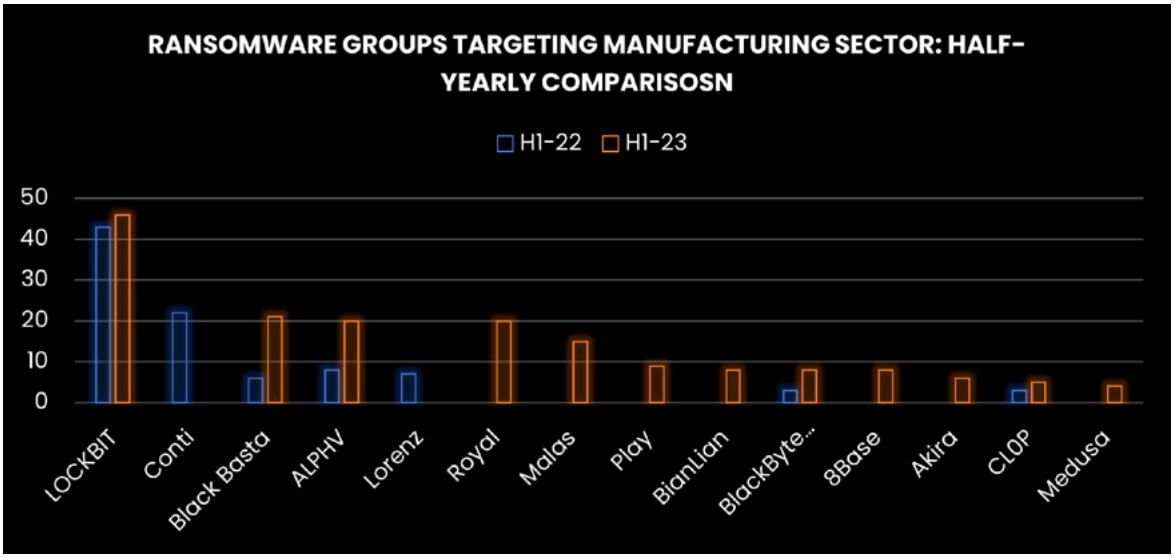
Ransomware Attacks & Threat Groups

The Manufacturing sector has been among the most affected due to ransomware attacks since the beginning of 2023. CRIL witnessed an over **140% Quarter-over-Quarter (Q-o-Q) increase in ransomware attacks on the Manufacturing sector in Q2-2023 (47 victims) viz-a-viz Q1-2023 (117 victims)**. CRIL observed a 40% increase in ransomware attacks from January-June 2023 compared to the same period in 2022. There were 131 publicly disclosed victim organizations in the Manufacturing sector in 2022 compared to 184 in H1-2023.

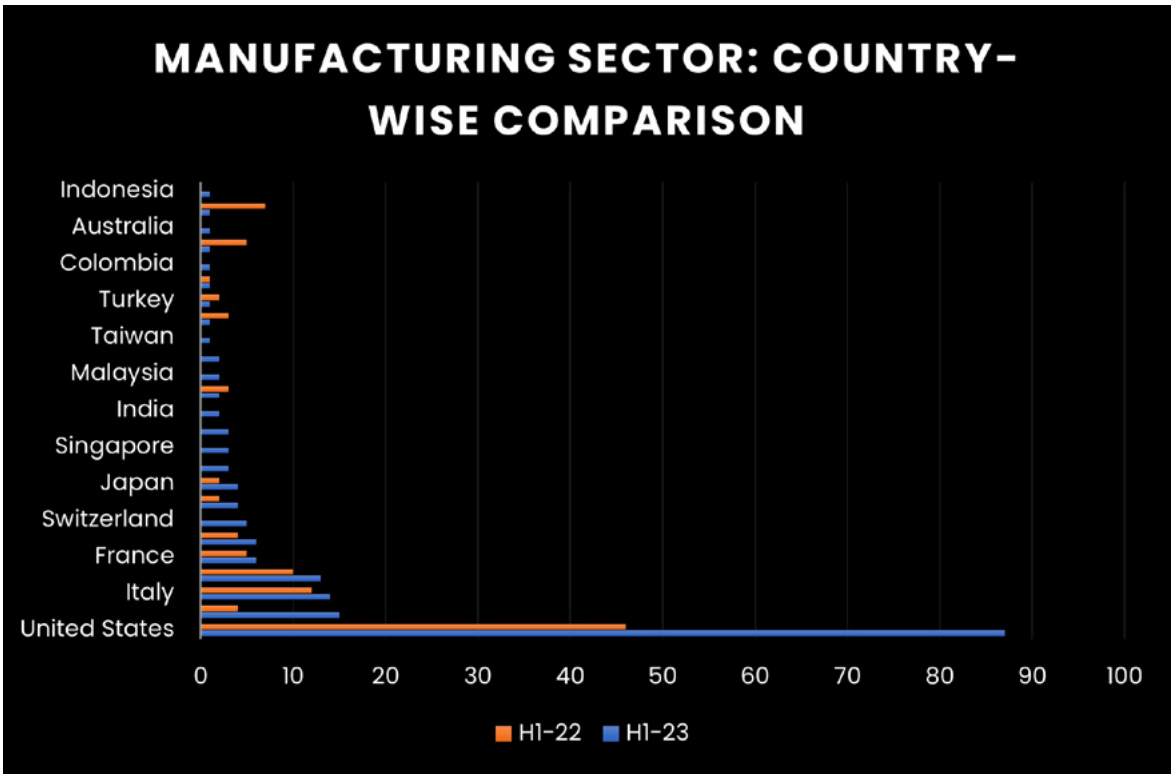


LOCKBIT ransomware group was the most aggressive group in targeting the Manufacturing sector in H1-2023. Previously, in H1-2022, Conti was the most nefarious group targeting this sector.

Several new ransomware groups, such as Royal, Play, BianLian, 8 Base, and Medusa, emerged in 2023 and aggressively targeted the Manufacturing sector.



The geographical distribution of ransomware attacks in H1-2023 was more concentrated toward the West. The United States Manufacturing companies were targeted the most, with an increase of 87% in attacks compared to the same time in 2022. Further, the United Kingdom, Italy, Germany, and France Manufacturing corporations, too, witnessed an exponential rise in ransomware attacks.

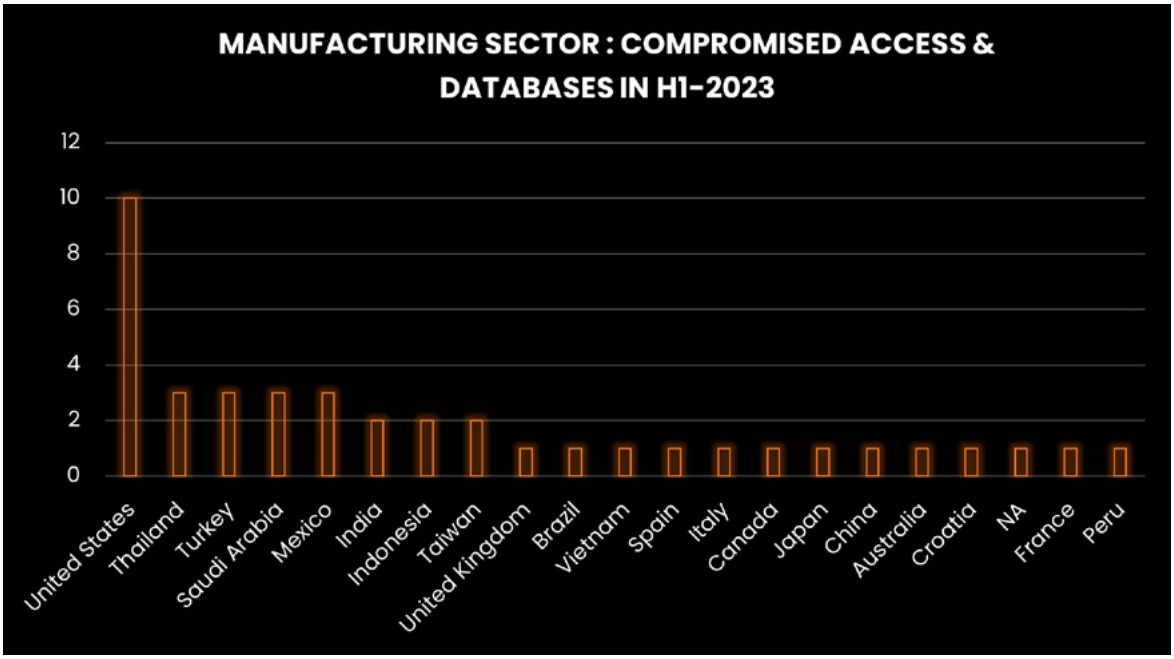


Impact of Compromised Accesses & Database Leaks on Darkweb

Compromised accesses and database leaks can significantly impact the Manufacturing sector. Due to the intellectual property and sensitive information held by these companies, the Manufacturing sector is a treasure trove for threat actors. Therefore, the threat actors leverage historical data leaks and compromise access to reconnoiter around and exploit their targets. Threat actors can further utilize these to launch supply-chain attacks on the sector.

The effect of such attacks could be far-reaching if threat actors utilize the compromised information combined with unpatched vulnerabilities to target critical systems in these industries to disrupt their operations.

In H1-2023, we observed that United States (US) entities from the Manufacturing sector were adversely affected due to the sale of compromised data and accesses on the darkweb. The same could also be assimilated from the ransomware attacks carried out on companies from this sector in the US.



Conclusion

The Manufacturing sector threat landscape is quite dynamic and complex, owing to the magnitude of products and vendors catering to this sector. The increased use of Industrial IoT devices in this sector to scale the demand and economy of efforts has led to increased security risks.

As the adoption of these components increases in the sector, so is the adeptness of the threat actors in leveraging commercially available tools to target these systems. Besides APTs and ransomware groups, Hacktivist groups have also started targeting these critical components to satiate their ideological aspirations.

Furthermore, the Manufacturing sector faces a critical business operations challenge due to the use of components nearing their obsolescence. Replacing these components is an ardent task because it increases the cost of operations, training the manpower, and maintaining them, especially during ongoing economic turbulence.

Moreover, their vendors do not adequately maintain this obsolete equipment due to ongoing development in automation and robotics. Hence, product manufacturers and users must adopt a proactive approach when it comes to identifying and securing these security gaps to prevent disruption of manufacturing operations.

Recommendations

- Robust Cybersecurity Measures: Implement comprehensive cybersecurity protocols to safeguard critical manufacturing sector assets from cyber threats. This includes regular vulnerability assessments, penetration testing, and employee cybersecurity training.

- Redundancy and Backup Systems: Ensure redundancy in critical systems and establish robust backup mechanisms to minimize downtime and maintain production continuity during unforeseen events or system failures.

- Supply Chain Resilience: Strengthen supply chain resilience by diversifying suppliers and fostering partnerships with reliable vendors to mitigate disruptions and reduce dependency on single sources.

- Risk Assessment and Management: Conduct regular risk assessments to identify potential vulnerabilities and develop effective risk management strategies to address them proactively.

- Physical Security Enhancements: Enhance physical security measures to protect manufacturing facilities, sensitive equipment, and personnel from unauthorized access and potential threats.

- Real-time Monitoring and Response: Implement advanced monitoring systems that provide real-time insights into operational processes and promptly respond to anomalies or potential security breaches.

- Employee Training and Awareness: Conduct comprehensive training sessions for employees to raise awareness about cybersecurity best practices, potential threats, and the importance of adhering to security protocols.

- Regular Security Audits: Conduct regular security audits, both internally and through third-party assessments, to identify and address any potential vulnerabilities in the manufacturing sector's infrastructure and systems.

Recommendations

— Secure Communication Channels: Utilize encrypted communication channels and secure data transmission methods to protect sensitive information from unauthorized access during data exchanges.

— Compliance with Industry Standards: Comply with relevant industry regulations, standards, and best practices to maintain a high level of security and quality in critical manufacturing processes.

— Incident Response Planning: Develop a well-defined incident response plan that outlines the steps to be taken in case of a security breach, ensuring a coordinated and efficient response to minimize the impact.

— Collaboration and Information Sharing: Foster collaboration with other critical manufacturing sector entities, government agencies, and cybersecurity experts to share threat intelligence and stay informed about emerging risks and mitigation strategies.

— Zero Trust Architecture: Implement a Zero Trust architecture to enhance cybersecurity by treating every user, device, or system as untrusted until proven otherwise. This approach requires strict authentication, authorization, and continuous monitoring of all network activities, regardless of whether they originate from within or outside the organization. By adopting the Zero Trust model, the critical manufacturing sector can significantly reduce the attack surface and minimize the risk of unauthorized access or lateral movement by potential threats.

— Regular Firmware Updates: Ensure regular firmware updates for all connected devices and industrial control systems (ICS) within the critical manufacturing sector. Firmware updates often include security patches and enhancements that address known vulnerabilities. By keeping the firmware up-to-date, the sector can mitigate the risk of exploitation through known weaknesses and ensure that critical devices operate with the latest security measures.

About Cyble

Cyble is a global threat intelligence SaaS provider that helps enterprises protect themselves from cybercrimes and exposure in the Darkweb. Its prime focus is to provide organizations with real-time visibility to their digital risk footprint. Backed by Y Combinator as part of the 2022 winter cohort, Cyble has also been recognized by Forbes as one of the top 20 Best Cybersecurity Startups to Watch In 2020. Headquartered in Alpharetta, Georgia, and with offices in Australia, Singapore, and India, Cyble has a global presence. To learn more about Cyble, visit www.cyble.com