SOCRadar®
Your Eyes Beyond

MANUFACTURING THREAT LANDSCAPE REPORT

"300% Increase in the Number of Dark Web References to Manufacturing Organizations"

socradar.io

SOCRadar®
Your Eyes Beyond

Table of Contents

www.socradar.io

Executive Summary

In this digitally-transformed era, the manufacturing industry has been reaping the benefits of advancements in technologies, such as Industrial Control Systems (ICS) and Operational Technology (OT). However, these developments have also introduced a new set of vulnerabilities, exposing the sector to an array of sophisticated cyber threats. Despite established concerns such as ransomware and phishing, a myriad of other threats have been increasingly causing significant disruptions in the manufacturing landscape.

This report synthesizes multiple reliable sources to provide an in-depth exploration of these key threats, ranging from intellectual property (IP) theft, supply chain attacks, nation-state attacks, to equipment sabotage, and internal breaches, with a particular focus on the rising threats to ICS and OT systems.

By comprehensively understanding these threats, it is our objective to guide manufacturers in strengthening their cybersecurity posture and building a resilient infrastructure that can withstand the evolving cyber threat landscape.

1. **Increased Threat Landscape:** As of 2023, the manufacturing sector has seen a sharp rise in cyber threats, as supported by a 300% increase in the number of dark web references to manufacturing organizations, revealing the sector's growing appeal to cybercriminals.

2. **Dominance of Ransomware:** Ransomware continues to pose a significant risk, with a substantial 28% of all ransomware attacks in 2023 targeting the manufacturing sector. This can be attributed to the industry's critical operational needs, which create an urgency to restore services, often leading to payment of demanded ransoms.

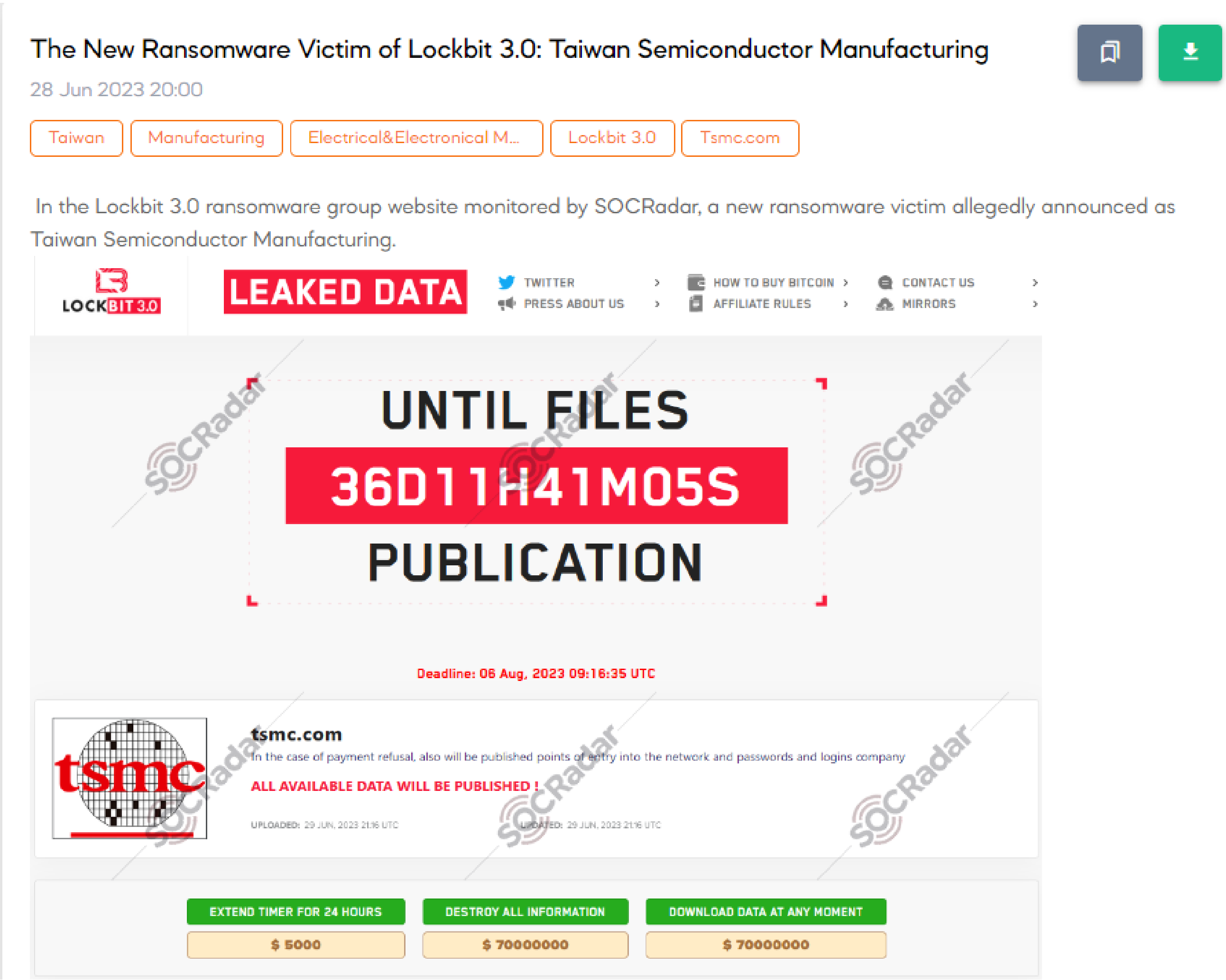
3. **Intellectual Property (IP) Theft:** IP theft has emerged as a major threat to manufacturers, given the value of their proprietary data. Hackers see this information as high-value loot, which can either be ransomed back to the companies or sold on the dark web.

4. **OT and ICS Vulnerabilities:** Operational Technology (OT) and Industrial Control Systems (ICS) attacks are increasingly becoming more sophisticated, with potentially devastating effects on manufacturing processes and product quality. An average of 39% of ICS computers in the manufacturing industry was attacked in H1 2022.

5. **Supply Chain Attacks:** Supply chain attacks are becoming more prevalent, exploiting multiple points of vulnerability across a manufacturing company's supplier network. This type of attack accounted for 40% of all cyber incidents involving manufacturers in the first half of 2023.

Cybersecurity Threats to the Manufacturing Industry: A Timeline

Cybersecurity in the manufacturing sector has become an issue of pressing concern over recent years. As manufacturers transition to digital operations, they present an enticing target to cybercriminals due to the complex networks they employ and the rich troves of valuable data they store. A prominent example of this escalating trend is the recent $70 million ransomware attack on Taiwan Semiconductor Manufacturing Company (TSMC), an Apple supplier, orchestrated by the Russian ransomware gang, LockBit.



The New Ransomware Victim of Lockbit 3.0: Taiwan Semiconductor Manufacturing

28 Jun 2023 20:00

Taiwan | Manufacturing | Electrical&Electronical M... | Lockbit 3.0 | Tsmc.com

In the Lockbit 3.0 ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as Taiwan Semiconductor Manufacturing.

UNTIL FILES
36D11H41M05S
PUBLICATION

Deadline: 06 Aug, 2023 09:16:35 UTC

tsmc.com

In the case of payment refusal, also will be published points of entry into the network and passwords and logins company

ALL AVAILABLE DATA WILL BE PUBLISHED !

UPLOADED: 29 JUN, 2023 21:16 UTC UPDATED: 29 JUN, 2023 21:16 UTC

EXTEND TIMER FOR 24 HOURS	DESTROY ALL INFORMATION	DOWNLOAD DATA AT ANY MOMENT
$ 5000	$ 70000000	$ 70000000

This section presents a timeline of significant cyber incidents from 2018 to 2022 that have affected manufacturing companies. Since more than two-thirds (68%) of ransomware attacks against the manufacturing sector resulted in successful encryption of data according to the recent The State of Ransomware in Manufacturing and Production 2023 report of Sophos, this section aims to remind the escalating cybersecurity threats facing the sector and shows the importance of robust defense measures and practices to guard against these digital threats.

Cybersecurity Threats to the Manufacturing Industry: A Timeline

2018

In August 2018, TSMC, a major manufacturer of Qualcomm and a supplier of Apple's SoC components, fell victim to a new variant of the WannaCry ransomware. The cyberattack infected the company's plants during a software installation and caused errors during a new tool's installation process. As a result, TSMC experienced shipment delays and had to bear an approximate cost of USD 250 million.

2019

In February 2019, a U.S. manufacturing company discovered a new variant of BitPaymer ransomware that infected their systems via PsExec. The attackers compromised an account with administrator privileges to initiate the attack

In June 2019, ASCO, a large airplane part manufacturing company, underwent a significant ransomware attack. This cyberattack led to extended downtime, infecting most IT systems, and crippling production in factories across four countries, including the United States, Belgium, Germany, and Canada.

2020

In 2020, the automotive manufacturer conglomerate Renault-Nissan suffered a cyberattack involving the WannaCry ransomware. This attack halted production at five plants and caused losses believed to be as high as $4 billion.

The international aluminum manufacturer, Norsk Hydro, also experienced an attack by the LockerGoga ransomware in 2020. The attack forced the company to close multiple plants and damaged IT systems in various business functions, including in Norway, Qatar, and Brazil. The estimated cost of the attack was around $75 million.

2021

In April 2021, a high-profile ransomware attack was successfully conducted against Brenntag, a renowned chemical distribution company. The hacker group DarkSide targeted the North American side of the company business, encrypted the company network, and stole 150GB of data, including sensitive information about the company’s employees.

The same month, Quanta, a supplier to tech giants like Dell, Apple, Lenovo, Microsoft, and Cisco, acknowledged a crippling ransomware attack. REvil, the cybercriminal group behind the attack, attempted to extort $50 million from Quanta.

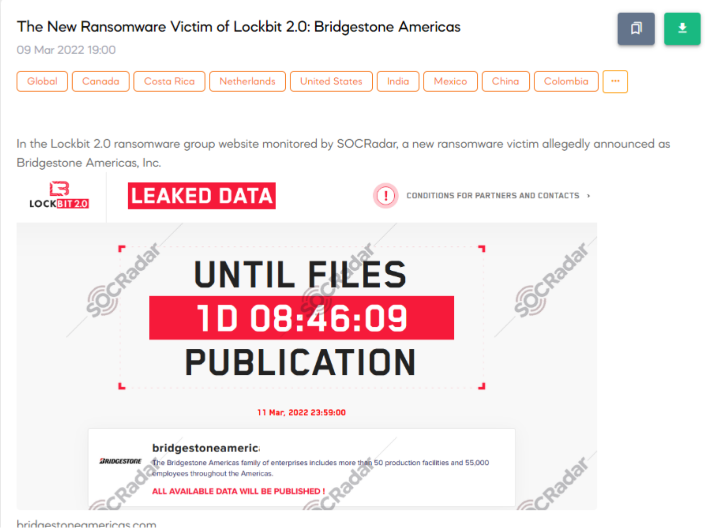
Another significant attack in 2021 was against the Colonial Pipeline, which led to the halting of production while the organization worked to respond to the threat. The attack caused significant disruption in production, resulting in the cancellation of flights and fuel shortages.

By the end of 2021, nearly a quarter (23%) of all attacks remediated by IBM X-Force were directed towards manufacturing companies, up from 18% in 2020.

Cybersecurity Threats to the Manufacturing Industry: A Timeline

2022

In February 2022, Bridgestone Americas, a tire producer, experienced a cyberattack by the LockBit ransomware group.



The New Ransomware Victim of Lockbit 2.0: Bridgestone Americas

09 Mar 2022 19:00

Global | Canada | Costa Rica | Netherlands | United States | India | Mexico | China | Colombia | ···

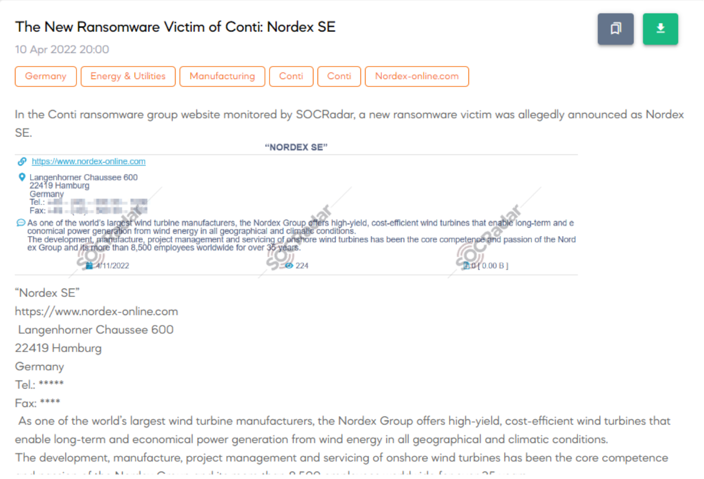
In the Lockbit 2.0 ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as Bridgestone Americas, Inc.

The Bridgestone Americas family of enterprises includes more than 50 production facilities and 55,000 employees throughout the Americas.

ALL AVAILABLE DATA WILL BE PUBLISHED !

bridgestoneamericas.com

In April 2022, Nordex, a major producer of wind turbines, suffered a Conti ransomware cyberattack, which caused several systems across their branches to go offline.



The New Ransomware Victim of Conti: Nordex SE

10 Apr 2022 20:00

Germany | Energy & Utilities | Manufacturing | Conti | Conti | Nordex-online.com

In the Conti ransomware group website monitored by SOCRadar, a new ransomware victim was allegedly announced as Nordex SE.

"NORDEX SE"

https://www.nordex-online.com

Langenhorner Chaussee 600
22419 Hamburg
Germany
Tel.: [redacted]
Fax: [redacted]

As one of the world's largest wind turbine manufacturers, the Nordex Group offers high-yield, cost-efficient wind turbines that enable long-term and economical power generation from wind energy in all geographical and climatic conditions.
The development, manufacture, project management and servicing of onshore wind turbines has been the core competence and passion of the Nordex Group and its more than 8,500 employees worldwide for over 35 years.

"Nordex SE"
https://www.nordex-online.com
 Langenhorner Chaussee 600
22419 Hamburg
Germany
Tel.: *****
Fax: ****

As one of the world's largest wind turbine manufacturers, the Nordex Group offers high-yield, cost-efficient wind turbines that enable long-term and economical power generation from wind energy in all geographical and climatic conditions.
The development, manufacture, project management and servicing of onshore wind turbines has been the core competence

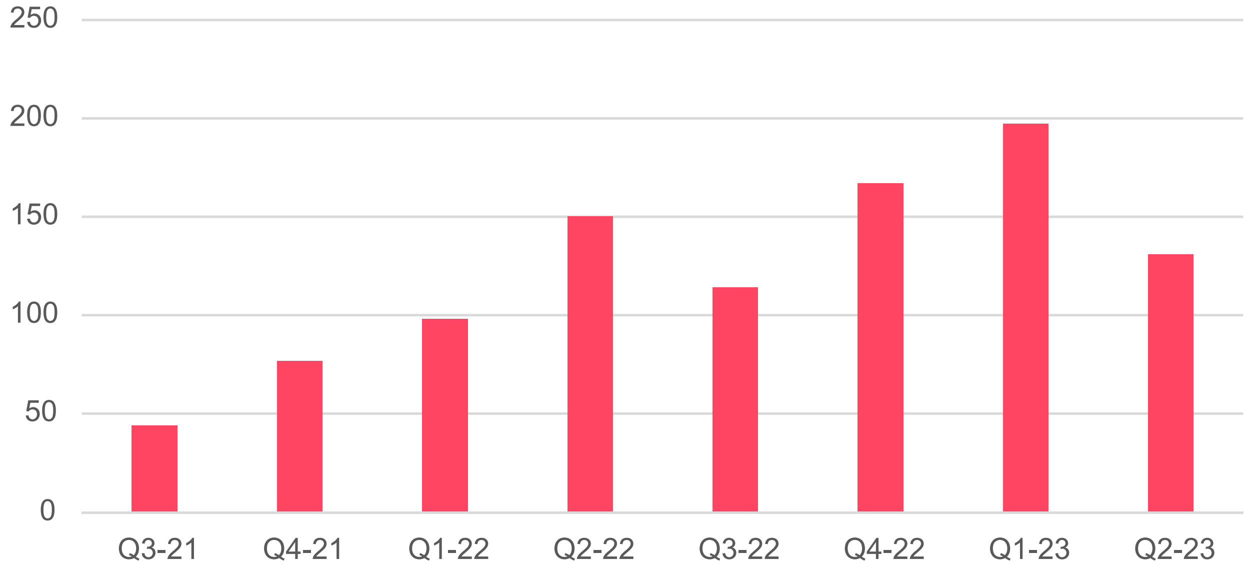
In June 2022, Iranian steel companies Hormozgan, Khouzestan, and Mobarakeh faced cyberattacks disrupting the industrial processes at Khouzestan Steelworks.

By the end of 2022, around 51 percent of manufacturing companies had experienced cyberattacks on their cloud infrastructure over the last year. These ongoing threats highlight the need for manufacturing companies to prioritize cybersecurity, adopt best practices, and seek dynamic solutions to prevent these types of cyberattacks. A critical element of this is patch management, as 44 percent of cyberattacks in the sector occurred because companies did not have their patch management in order.

Dark Web Radar: A Deep Dive into Recent Trends and Threats

Over the past two years, SOCRadar platform statistics have shown a sharp increase in Dark Web activity related to the manufacturing industry. From July 2021 to June 2023, there were 27,214 posts on the platform, with 978 of those posts mentioning the manufacturing industry. A closer look at this activity shows a rising trend in the number of these posts over time. In Q3 of 2021, only 4.50% of these (44) posts mentioned the manufacturing industry, but by Q1 of 2023, that number had risen to an alarming 20.14% (197 posts). Although there was a slight dip in the last quarter, it is evident from the bar graphic in the report that interest in the manufacturing sector on the Dark Web is growing.

Number of the Dark Web Posts Mentioning Manufacturing Industry



Geographically, the most targeted country, according to these posts, was the United States, representing a whopping 20.55% of the attacks. Other countries that were significantly targeted included India, the Russian Federation, Italy, Germany, and the United Kingdom, as can be seen on the table next page.

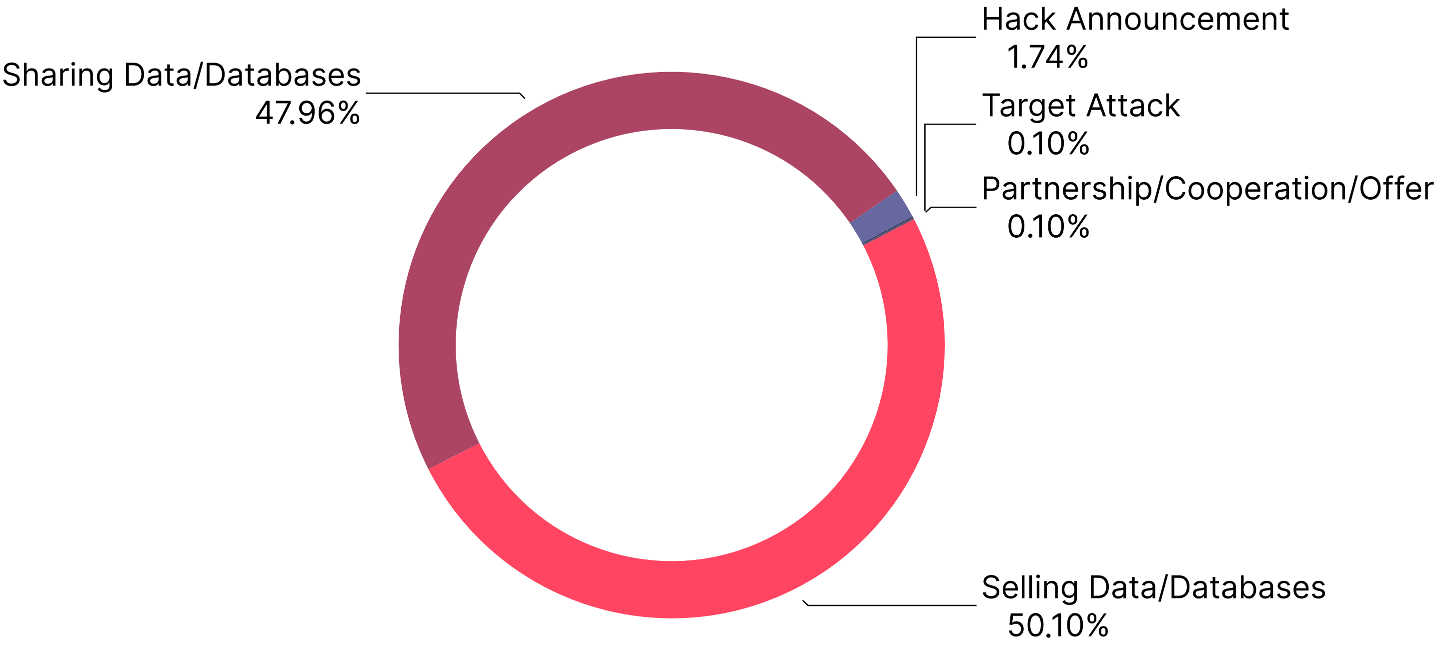
Dark Web Radar: A Deep Dive into Recent Trends and Threats

The Most Targeted Countries in the World in the Manufacturing Industry	
United States	20.55%
India	5.11%
Russian Federation	4.40%
Italy	3.68%
Germany	3.58%
United Kingdom	3.17%
China	3.07%
France	2.97%
Brazil	2.97%
Taiwan	2.04%
Thailand	2.04%
Canada	2.04%

Dark Web Radar: A Deep Dive into Recent Trends and Threats

When we break down the subject of these Dark Web posts, the statistics become even more alarming. A large majority of these posts (50.10%) revolved around selling data or databases related to the manufacturing industry. An almost equal percentage (47.96%) involved sharing of such data. Notably, posts related to hack announcements and target attacks represented only a small fraction of the posts. Interestingly, there was no interest in buying data or databases. This lack of buying interest can be attributed to the high saturation of sharing and selling posts on the Dark Web.

Subject of Dark Web Posts



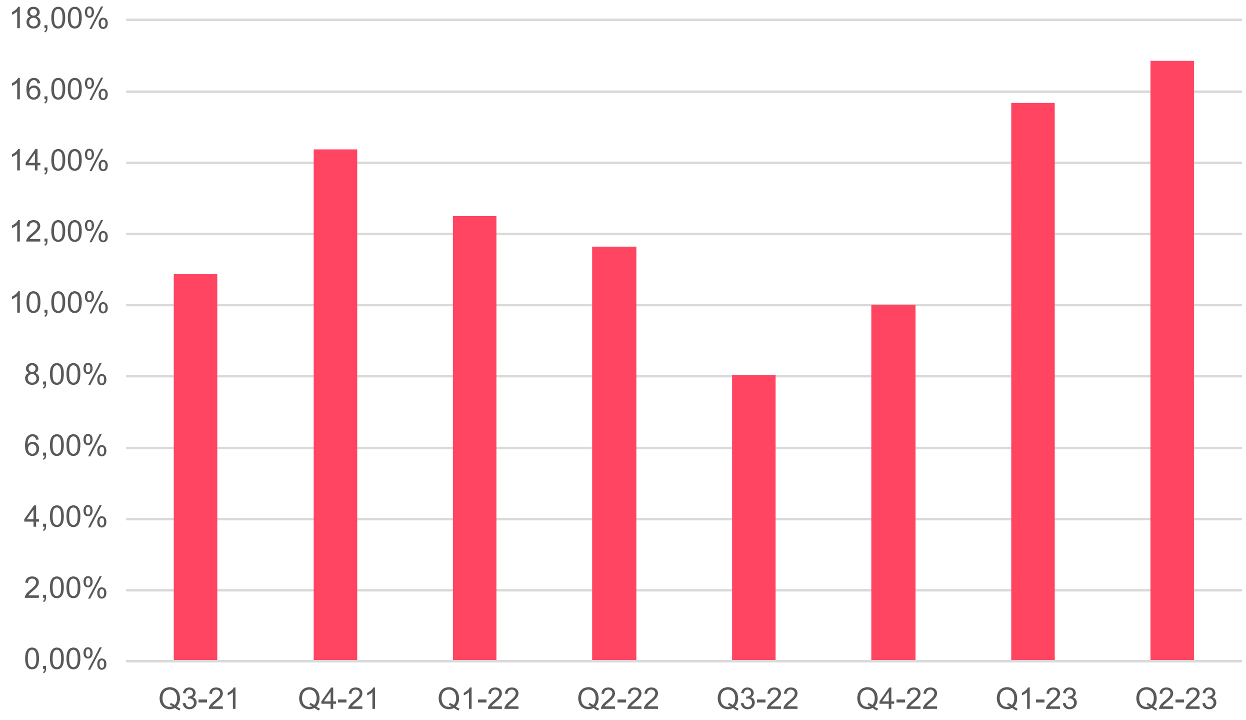
The type of data being shared and sold also includes access into victim systems such as Remote Desktop Protocol (RDP) and Virtual Private Network (VPN) accesses. Credentials for administrative panels and Citrix were also available. Customer databases were particularly popular, while posts about credit card information were significantly fewer compared to the finance industry.

This rising trend of Dark Web activities related to the manufacturing industry shows the need for robust security measures and continuous monitoring of cyber threats. It is more critical now than ever for manufacturing companies to take proactive steps to safeguard their data and systems against the growing threat from cybercriminals active on the Dark Web.

Ransomware Threats: Manufacturing Industry Under Siege

Over the last two years (July 2021-June 2023), manufacturing industries have significantly come under the radar of various ransomware groups. These industries are witnessing a sharp spike in cyber threats, representing 19.2% of the total shares (1168 out of 6081) over this period.

Percentage of Ransomware Shares Targeting Manufacturing Industry



A trend analysis depicted in the bar graphic in the report shows a concerning escalation in ransomware threats to the manufacturing industry over the quarters. The highest rise was observed in the second quarter of 2023 with 16.87% of the attacks, a stark contrast to 10.87% in the third quarter of 2021.

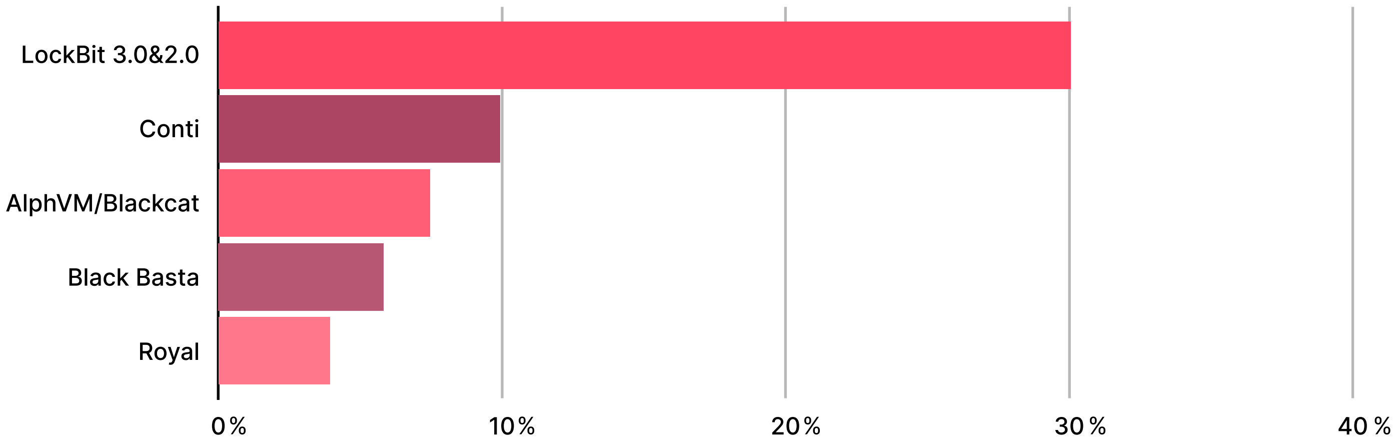
Ransomware Threats: Manufacturing Industry Under Siege

Ransomware Threats in the Manufacturing Industry	
United States	36.82%
Germany	5.99%
Italy	4.54%
United Kingdom	4.20%
Canada	3.34%
France	2.83%
Taiwan	2.40%
Japan	2.31%
China	1.97%
India	1.97%
Switzerland	1.71%
Spain	1.71%

A geographical assessment of these attacks reveals that the United States was the prime target, suffering 36.82% of the total attacks. Other major victims were Germany (5.99%), Italy (4.54%), and the United Kingdom (4.20%). Interestingly, Russia, which was highly prevalent in dark web posts, surprisingly had only 0.17% recorded attacks over two years.

Ransomware Threats: Manufacturing Industry Under Siege

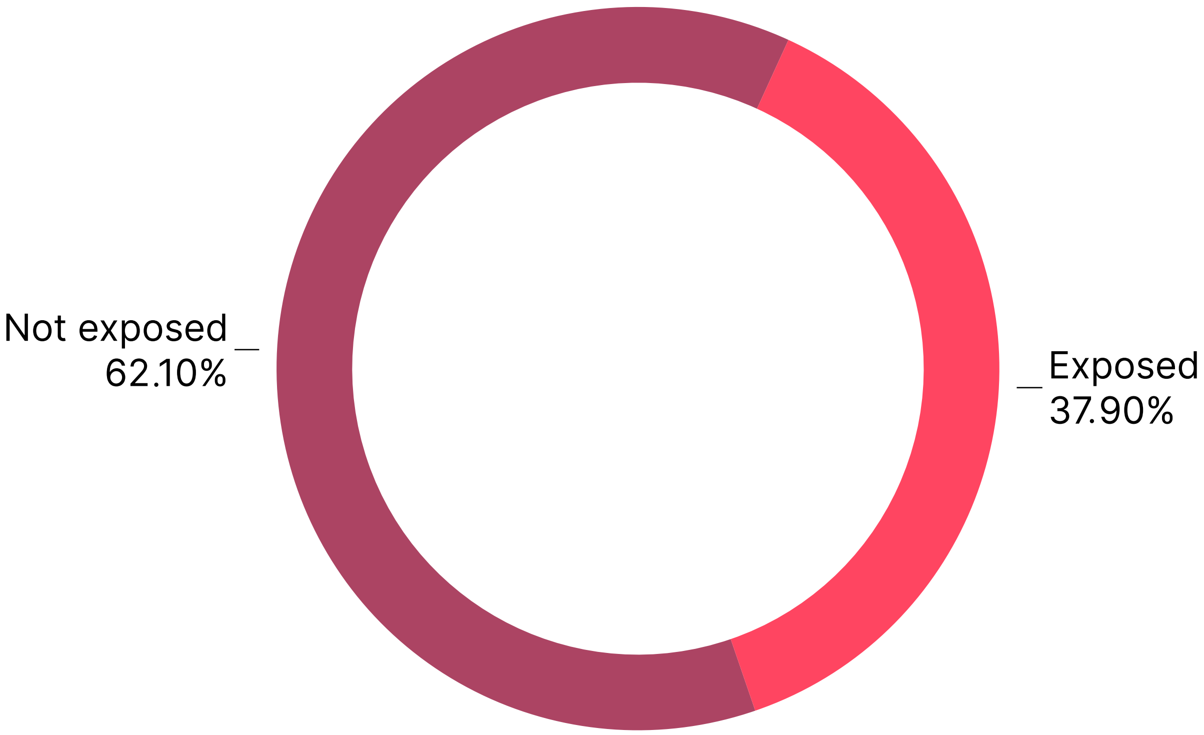
Top Ransomware Groups in the Manufactoring Industry



Amongst ransomware groups, LockBit stood out as the most active, accountable for a staggering 30.05% of these attacks. Other prominent threat actors were Conti (9.93%), AlphVM Blackcat (7.45%), and Black Basta (5.82%). In total, around 70 different active groups were involved in carrying out these attacks.

Ransomware Threats: Manufacturing Industry Under Siege

Ransomware Groups` Shares of Exposing Data and Databases



A closer look at the nature of these shares further clarifies the grim picture. Of the 1168 recorded attacks, 321 involved data exposure, while 847 were victim announcements. This implies that up to 37.9% of victims had their data exposed as a result of these attacks. Worryingly, it can be deduced that as high as 62.1% of the victims likely reached an agreement with the ransomware gangs, which often involves paying a full or partial ransom.

As ransomware continues to evolve and diversify, these findings underscore the critical need for the manufacturing sector to prioritize cybersecurity measures and invest in robust defenses against these emerging threats.

Multifaceted Threats in the Manufacturing Industry

As digital transformation permeates the manufacturing industry, the potential cyber threats facing manufacturers have become increasingly diverse and complex. This is accentuated by the growing interconnection between Information Technology (IT), Operational Technology (OT), and Industrial Control Systems (ICS), expanding the potential attack surface for malicious actors.

With the manufacturing sector being the most attacked Operational Technology (OT)-related industry, the IBM 2023 X-Force Threat Intelligence Index report reveals that attacks on manufacturers constitute more than 50% of all incidents against OT organizations. High-profile ransomware attacks such as those against Bridgestone, AGCO, and Kojima Industries often impact production systems either through network proliferation or by forcing precautionary shutdowns of physical systems. These shutdowns can cost more than the actual ransom paid to regain IT access. Direct attacks on OT systems pose even greater risks as they can harm equipment, the environment, and human life.

The cyber attack on Honda in 2020 and the LockerGoga ransomware attack on Norsk Hydro in 2019 both exemplify the escalating danger faced by manufacturers. These incidents involved sophisticated software designed to compromise industrial facilities such as factories and power plants. The 2019 attack on Norsk Hydro resulted in a temporary production halt and a financial loss of $52 million. Similarly, the 2020 attack on Honda disrupted their global operations and highlighted the vulnerability of manufacturing companies to cyber threats

Underreporting of cyber attacks is a significant concern in the manufacturing industry due to fewer compliance reporting requirements. Supply chain threats can also disrupt internal systems, as demonstrated by the Microsoft Exchange email server vulnerability exploits in February 2021 and the SolarWinds software compromise in December 2020. The threat landscape includes organized hacker groups like Allanite, APT33, Dragonfly, Dragonfly 2.0, Hexane, Lazarus Group, Leafminer, Oilrig, Sandworm, and Xenotime.

There is an array of cyber threats that manufacturers must prepare for, beyond the widely recognized threats such as phishing and ransomware (which is detailed in the previous section). The following five cyber threats stand out in their potential to impact the manufacturing sector significantly:

IP Theft: The Intellectual Property (IP) of a manufacturer, such as trade secrets, blueprints, and patented techniques, represents a significant competitive advantage. The theft of this sensitive information can have disastrous consequences, from the emergence of competitor products to the devaluation of the company's assets. For example, Ryan Hernandez, a hacker from Seattle, illegally breached the security of Nintendo's servers, illicitly obtaining sensitive data pertaining to gaming consoles and video games.

Multifaceted Threats in the Manufacturing Industry

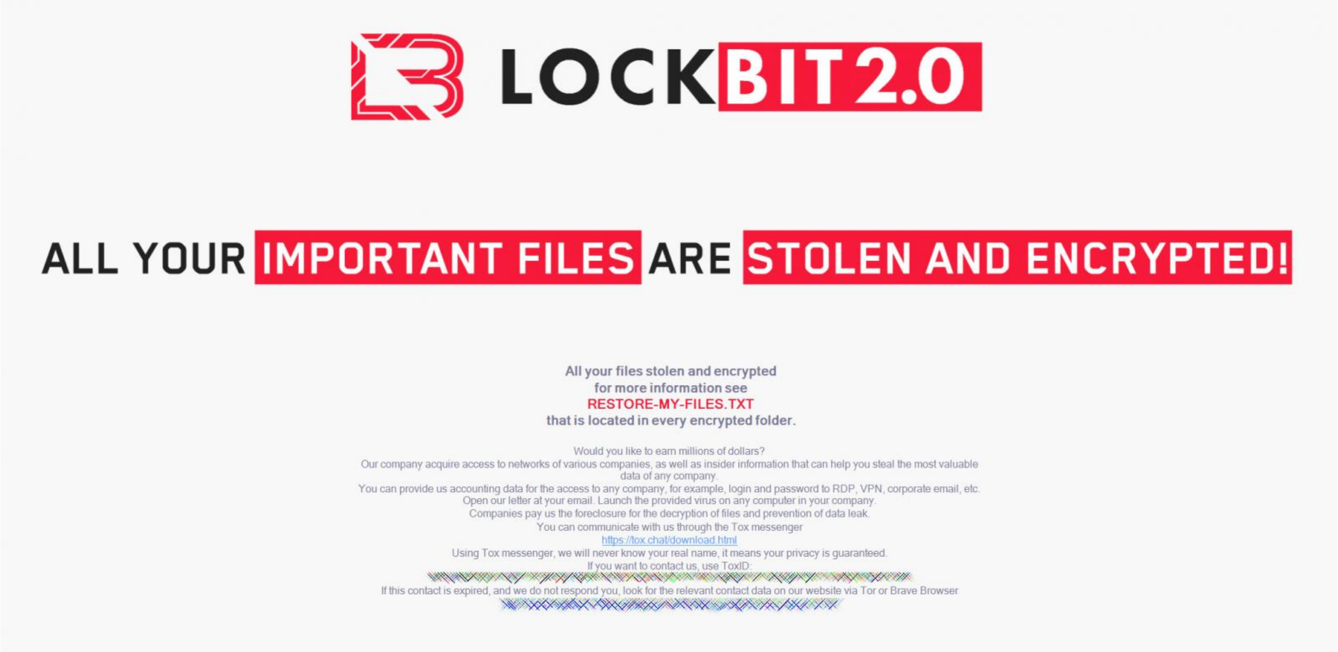
Supply Chain Attacks: Supply chain attacks target a company’s business partners or suppliers. These can cause significant disruptions, especially in an industry like manufacturing that relies heavily on its supply chain. The NotPetya malware, resulted in massive losses for multiple companies, showing the potential extent of damage from such attacks.

Nation-State Attacks: These attacks, often highly sophisticated, can be motivated by economic or military objectives. Manufacturing industries, particularly those related to defense and critical infrastructure, are prime targets. As an example, a recently identified ICS-focused threat group called Chernovite emerged in 2022, suspected to have backing from a nation-state according to cybersecurity firm Dragos. This group utilized an advanced ICS hacking toolkit called PIPEDREAM, specifically designed to exploit technologies supported by various third-party vendors.

Equipment Sabotage: While OT (Operational Technology) devices have been around for some time, their integration into modern communication systems is a recent development. Unlike in the past, these devices now rely on external linking technologies, exposing them to potential threats from the outside. Unfortunately, many manufacturing companies continue to utilize these devices without implementing adequate security measures. This lack of security practices leaves them vulnerable to malicious external attacks. Prominent examples of malware that exploit this vulnerability include Stuxnet and Triton.

Internal Breaches: Internal breaches, which account for nearly 30% of cyberattacks, involve employees or personnel with access to a company's systems. While external hackers are often financially motivated, internal attacks can stem from financial incentives as well as feelings of anger or dissatisfaction among employees or former employees.

Multifaceted Threats in the Manufacturing Industry



LOCKBIT 2.0

ALL YOUR IMPORTANT FILES ARE STOLEN AND ENCRYPTED!

All your files stolen and encrypted
for more information see
RESTORE-MY-FILES.TXT
that is located in every encrypted folder.

Would you like to earn millions of dollars?
Our company acquire access to networks of various companies, as well as insider information that can help you steal the most valuable data of any company.
You can provide us accounting data for the access to any company, for example, login and password to RDP, VPN, corporate email, etc.
Open our letter at your email. Launch the provided virus on any computer in your company.
Companies pay us the foreclosure for the decryption of files and prevention of data leak.
You can communicate with us through the Tox messenger
https://tox.chat/download.html
Using Tox messenger, we will never know your real name, it means your privacy is guaranteed.
If you want to contact us, use ToxID:
[redacted]
If this contact is expired, and we do not respond you, look for the relevant contact data on our website via Tor or Brave Browser
[redacted]

LockBit2.0 trying to recruit employees using the wallpaper ransomware note

Unlike external hackers, internal threat actors do not need to breach network security measures. They can exploit their existing knowledge or credentials to gain access to sensitive data, making it easier for them to carry out threats without detection.This can include planting logic bombs - code intentionally inserted into a software system that will set off a malicious function when specified conditions are met. Unfortunately, even former employees can potentially exploit this access if passwords or entry methods are not changed to mitigate the risk of such attacks.

The shift to remote work and the use of personal devices have created opportunities for unintended internal breaches. Companies, unprepared for the security challenges, especially during the pandemic, lacked the necessary infrastructure to maintain consistent security measures for all employees. This blurred the lines between personal and work environments, enabling hackers to exploit home networks and devices with limited security.

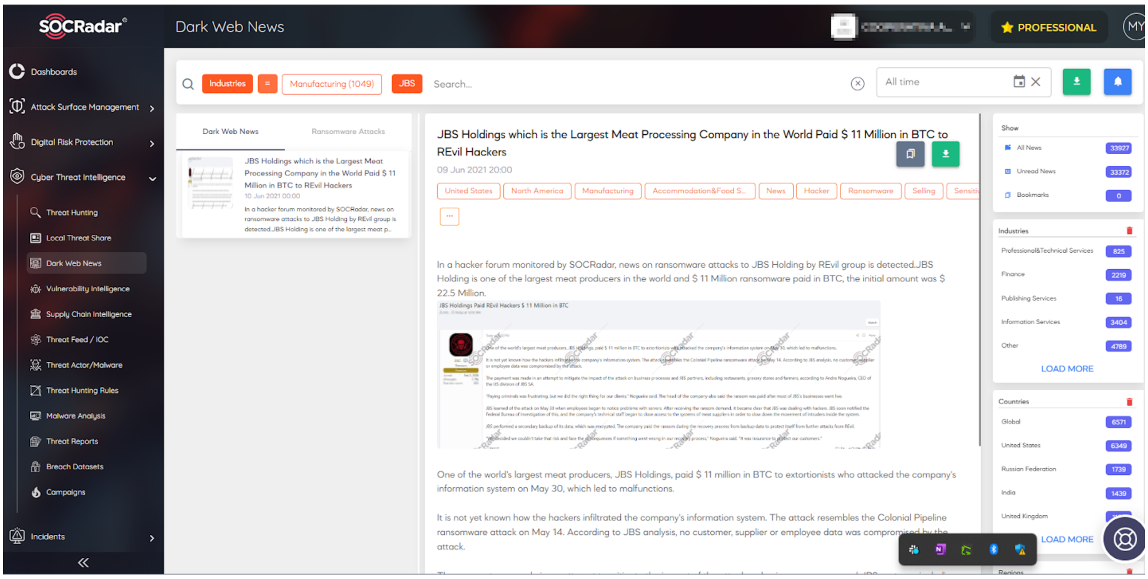
In facing these multifaceted threats, manufacturers must adopt an equally comprehensive approach to cybersecurity, prioritizing not only IT systems but also the security of OT and ICS. Understanding these threats is the first step towards implementing effective countermeasures and ensuring the ongoing safety and stability of the manufacturing industry.

Lessons Learned from Cyber Attacks in the Manufacturing Industry

Based on our comprehensive study and findings, several lessons have been learned that can significantly inform the cybersecurity strategy for the manufacturing industry:

1. **Increasing Cyber Threats:** The manufacturing sector is increasingly becoming a high-priority target for cybercriminals. Regardless of the industry not being frequently highlighted in mainstream media, the threat statistics clearly indicate an escalating trend of attacks, especially ones involving state-sponsored actors. SOCradar's threat intelligence platform can help by providing real-time alerts on potential threats, enabling swift response actions.

2. **Growing Relevance of Darknet:** The darknet has become a hub for threat actors to coordinate and launch attacks. Constant monitoring and usage of threat intelligence platforms like SOCradar that track darknet activities can provide valuable insights to prevent potential cyberattacks.



JBS Holdings which is the Largest Meat Processing Company in the World Paid $ 11 Million in BTC to REvil Hackers

10 Jun 2021 00:00

In a hacker forum monitored by SOCRadar, news on ransomware attacks to JBS Holding by REvil group is detected.JBS Holding is one of the largest meat p...

JBS Holdings which is the Largest Meat Processing Company in the World Paid $ 11 Million in BTC to REvil Hackers

09 Jun 2021 20:00

In a hacker forum monitored by SOCRadar, news on ransomware attacks to JBS Holding by REvil group is detected.JBS Holding is one of the largest meat producers in the world and $ 11 Million ransomware paid in BTC, the initial amount was $ 22.5 Million.

JBS Holdings Paid REvil Hackers $ 11 Million in BTC

One of the world's largest meat producers, JBS Holdings, paid $ 11 million in BTC to extortionists who attacked the company's information system on May 30, which led to malfunctions.

It is not yet known how the hackers infiltrated the company's information system. The attack resembles the Colonial Pipeline ransomware attack on May 14. According to JBS analysis, no customer, supplier or employee data was compromised by the attack.

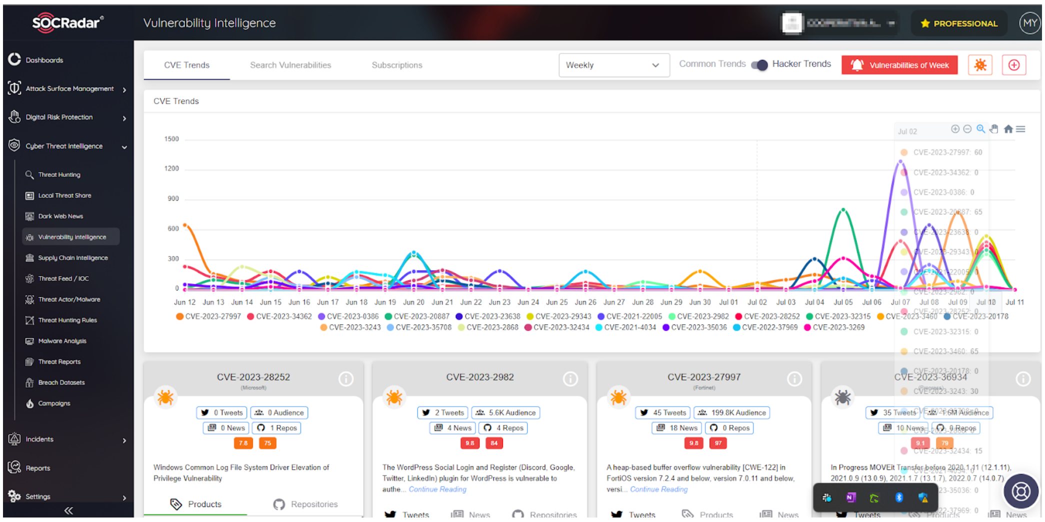
Stay ahead of cyber threats lurking in the Dark Web with SOCRadar's Threat Intelligence module. Gain valuable insights and proactively monitor potential risks. Enhance your security strategy and protect your organization from emerging threats.

3. **Critical Role of OT and ICS Security:** Operational Technology (OT) and Industrial Control Systems (ICS) are pivotal to the manufacturing sector and, therefore, are major targets for cybercriminals. SOCradar's capabilities can ensure their security by providing comprehensive visibility and actionable intelligence on OT and ICS threats.

4. **Rise of Sophisticated Cyber Attacks:** Cyber attacks have grown more sophisticated, incorporating AI and Machine Learning to bypass traditional security measures. SOCradar's advanced threat detection technology, informed by Machine Learning, can match the complexity of these threats and help to identify them in the early stages.

Lessons Learned from Cyber Attacks in the Manufacturing Industry

5. **Significance of Proactive Measures:** The need for proactive cybersecurity measures over reactive ones is evident. This includes conducting regular cyber risk assessments, implementing robust cybersecurity protocols, and continuous employee training. SOCradar's proactive threat hunting capabilities enable organizations to stay one step ahead of potential cyber threats.



Windows Common Log File System Driver Elevation of Privilege Vulnerability

The WordPress Social Login and Register (Discord, Google, Twitter, LinkedIn) plugin for WordPress is vulnerable to authe... Continue Reading

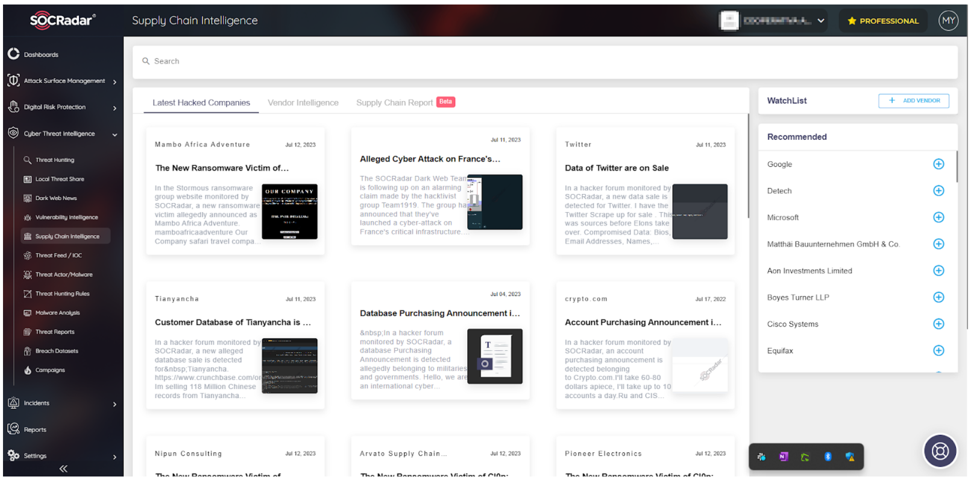
A heap-based buffer overflow vulnerability [CWE-122] in FortiOS version 7.2.4 and below, version 7.0.11 and below, versi... Continue Reading

In Progress MOVEit Transfer before 2020.1.11 (12.1.11), 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7),

Empower your defenses with SOCradar's Vulnerability Intelligence Module. Stay one step ahead of potential threats by proactively identifying and addressing vulnerabilities.

6. **IP Protection:** Protecting Intellectual Property (IP) is crucial as its theft can have disastrous implications for manufacturing businesses, potentially enabling competitors to gain a competitive advantage. SOCradar can assist by identifying potential IP-related risks and threats on the internet and dark web.

7. **Importance of Comprehensive Supply Chain Security:** With supply chains becoming a target for cybercriminals to gain access to critical business systems, it's vital to ensure comprehensive supply chain security. SOCradar can provide critical insights into the cybersecurity posture of third-party vendors, helping to safeguard the supply chain.



Mambo Africa Adventure Jul 12, 2023
The New Ransomware Victim of...
In the Stormous ransomware group website monitored by SOCRadar, a new ransomware victim allegedly announced as Mambo Africa Adventure. mamboafricaadventure Our Company safari travel compa...

Jul 11, 2023
Alleged Cyber Attack on France's...
The SOCRadar Dark Web Team is following up on an alarming claim made by the hacktivist group Team1919. The group has announced that they've launched a cyber-attack on France's critical infrastructure...

Twitter Jul 11, 2023
Data of Twitter are on Sale
In a hacker forum monitored by SOCRadar, a new data sale is detected for Twitter. I have the Twitter Scrape up for sale . This was sources before Elons take over. Compromised Data: Bios, Email Addresses, Names,...

Tianyancha Jul 11, 2023
Customer Database of Tianyancha is ...
In a hacker forum monitored by SOCRadar, a new alleged database sale is detected for Tianyancha. https://www.crunchbase.com/or... Im selling 118 Million Chinese records from Tianyancha...

Jul 04, 2023
Database Purchasing Announcement i...
 In a hacker forum monitored by SOCRadar, a database Purchasing Announcement is detected allegedly belonging to militaries and governments. Hello, we are an international cyber...

crypto.com Jul 17, 2022
Account Purchasing Announcement i...
In a hacker forum monitored by SOCRadar, an account purchasing announcement is detected belonging to Crypto.com I'll take 60-80 dollars apiece, I'll take up to 10 accounts a day Ru and CIS...

Nipun Consulting Jul 12, 2023
The New Ransomware Victim of...

Arvato Supply Chain... Jul 12, 2023
The New Ransomware Victim of Cl0p:

Pioneer Electronics Jul 12, 2023
The New Ransomware Victim of Cl0p:

Gain valuable insights into cyber incidents impacting your business partners with SOCRadar's Supply Chain Intelligence. Gain comprehensive visibility and stay informed about the cybersecurity landscape of the companies you collaborate with.

Recommendations For CISOs

In our pivotal roles as gatekeepers of our respective organizations' cyber defenses, we have the distinct challenge and privilege of navigating the ever-evolving landscape of cyber threats. SOCRadar analysis marks our ongoing commitment to providing actionable intelligence, aimed at not only defending our organizations against potential cyber threats but also ensuring a shared understanding within the cybersecurity community. Through our continuous monitoring, research, and reporting, SOCRadar aim to equip you with the latest knowledge and effective tools necessary for reinforcing your cybersecurity measures.

The manufacturing industry, while not always the centerpiece of conversations in cybersecurity circles, consistently ranks high in lists of industries most targeted by cyber attacks. One likely factor contributing to this high level of threat activity is the involvement of state-sponsored actors. Unlike the more commonly seen cybercriminals primarily motivated by financial gains, these actors often have more complex motives such as causing disruptions to key industries, Intellectual Property theft, and asserting geopolitical power. As such, their strategies and tactics often involve a wider range of threats and more advanced techniques than typically encountered.

The manufacturing sector is not just a crucial pillar of our economies, but also a key component of our societies. It's an industry that transforms raw materials into the products we all rely on daily, and consequently, any disruption can have far-reaching impacts.

SOCRadar’s report provides an encompassing view of the current cyber threat landscape, highlighting particular threats that deserve our attention. While ransomware and phishing attacks continue to pose significant risks, this report goes beyond these to explore the substantial risks posed by Intellectual Property theft, data spillages, supply chain attacks, and equipment sabotage.

SOCRadar’s analysis shows that the manufacturing industry is no longer a peripheral target but a central focus of sophisticated cybercriminals. The report identifies a range of threats, from the growing dark web marketplace for malicious software to the rise of nation-state attacks. However, the primary concern I want to emphasize is threats to Operational Technology (OT) and Industrial Control Systems (ICS) due to their critical roles in manufacturing operations.

Ransomware and phishing attacks continue to pose significant risks. However, this report offers a broader view, pointing out the substantial risk that Intellectual Property theft, internal breaches, supply chain attacks, and equipment sabotages. The pivot to remote work has presented new security challenges that need our attention. Protecting remote workers' devices and ensuring secure connections to our networks are essential. Remote workers should receive adequate training on best cybersecurity practices, and their devices should comply with the organization's security standards.

Recommendations For CISOs

The dark web has become an increasingly active platform for cybercriminals to exchange information and tools. To mitigate this, companies in this industry should enhance their efforts in dark web monitoring, spotting potential threats early, and taking appropriate action.

Here are some actionable recommendation for CISO's:

- **Prioritize OT and ICS Security:** Given the potential for disruption and damage, security protocols for OT and ICS should be as stringent as those for IT systems.
- **Review and Strengthen Security Infrastructure:** Implement advanced threat detection solutions, regular penetration testing, and security audits to identify and mitigate vulnerabilities.
- **Strengthen Supply Chain Security:** Conduct regular security audits of your suppliers and third-party partners to ensure they follow best cybersecurity practices.
- **Enhance Employee Training:** Regular cybersecurity awareness training for employees can help reduce the risks of phishing, data spillage, and other user-related vulnerabilities.
- **Dark Web Monitoring:** Tools such as SOCradar can help track threats specific to your organization on the dark web, enabling proactive response.
- **Develop Incident Response Plans:** Having a well-structured and practiced incident response plan helps minimize damage and recovery time from any potential cyber-attacks.

Who is SOCRadar®?

Your Eyes Beyond

As an Extended Threat Intelligence (XTI) platform and inventor of the concept, SOCRadar's approach effectively integrates Threat Intelligence, Digital Risk Protection, and External Attack Surface Management (EASM). Adapting proactive security with a hacker mindset, we aim to help security teams to detect blindspots before attackers.

The shortage of cybersecurity experts is a growing problem worldwide. All companies around the world must use resources efficiently to provide adequate cyber security with their limited resources. Automated security solutions offer precisely the opportunity that corporations are looking for. With its AI-powered automation technology. **With providing protection against threats for more than 6.000+ companies from 157 countries, SOCRadar has become an extension of SOC teams from every industry.**

SOCRadar provides extended cyber threat intelligence (XTI) that combines: **"Cyber Threat Intelligence, Digital Risk Protection, and External Attack Surface Management Services."** SOCRadar provides the actionable and timely intelligence context you need to manage the risks in the transformation era.

8.400
Free Users

Dark Web Monitoring: SOCRadar's fusion of its unique dark web recon technology with the human analyst eye further provides in-depth insights into financially-targeted APT groups and the threat landscape.

Protecting Customers' PII: Scan millions of data points on the surface, deep and dark web to accurately identify the leakage of your customers' Personally Identifiable Information (PII) in compliance with regulations.

Credit Card Monitoring: Enhance your fraud detection mechanisms with automation speed by identifying stolen credit card data on popular global black markets, carding forums, social channels, and chatters.

360-Degree Visibility: Achieve digital resilience by maintaining internet-facing digital asset inventory. Significantly accelerate this process by automated discovery, mapping, and continuous asset monitoring.

GET ACCESS 12 MONTHS FOR FREE

Gartner Peer Insights Customer First

Gartner Peer Insights™ 5/5 ★★★★★

Contact Us

✉ info@socradar.io

☎ +1 (571) 249-4598

651 N Broad St, Suite 205,
Middletown, DE 19709