Ontinue

2023/Threat Intelligence Report

2023 End of Year Report

Executive Summary

In today's rapidly evolving threat landscape, understanding the specific threats that impact your industry is paramount. We are pleased to present our inaugural Threat Intelligence Report for 2023, authored by Ontinue's Advanced Threat Operations team.

Cyber attackers are becoming increasingly sophisticated, using advanced techniques such as social engineering, ransomware, and supply chain attacks to breach organizations' defenses. As new threats and tactics are used, it's becoming more challenging for organizations to keep up with the latest threats and implement effective defenses.

The first-ever inaugural report from Ontinue is a moment of pride and accomplishment for the team. It marks a significant milestone in our journey toward enhancing cybersecurity intelligence and providing valuable insights to clients and stakeholders.

This report provides a comprehensive overview of industry-specific threats and emerging trends, including:

- **The proliferation of connected devices.** The Internet of Things (IoT) has led to a proliferation of connected devices, expanding the attack surface for cybercriminals. Each connected device represents a potential entry point for attackers to infiltrate an organization's network.
- **Cloud security concerns**. As more organizations migrate their data and applications to the cloud, ensuring the security of cloud-based environments becomes paramount. However, misconfigurations and inadequate security measures can expose sensitive data to unauthorized access.
- **Regulatory compliance.** Organizations are subject to an increasing number of cybersecurity regulations and compliance requirements. Failure to comply with these regulations can result in severe penalties and reputational damage.
- **Lack of security awareness**. Many cybersecurity breaches occur due to human error, such as clicking on malicious links or falling victim to phishing attacks. Improving security awareness among employees through training and education is essential for mitigating this risk.
- **Supply chain vulnerabilities**. Organizations are increasingly interconnected through complex supply chains, making them vulnerable to attacks targeting third-party vendors and suppliers. A breach in one part of the supply chain can have cascading effects on multiple organizations.
- **Emerging technologies**. The adoption of emerging technologies such as artificial intelligence, machine learning, and quantum computing introduces new security challenges and risks. Organizations must stay ahead of the curve to effectively secure these technologies against cyber threats.

Noteworthy Data Breaches 2023

The Average Cost of a Data Breach Reached a Record High of $4.45 Million

X (Formerly Twitter)

More than **220 million users' email addresses leaked** by a hacker named 'Ryushi'. The hacker demanded payment of $200,000 in exchange for the stolen information. However, after a week and no payment the hacker put the data up for sale on a hacking forum. Although it appears that no personal information beyond email addresses was compromised, the incident poses significant privacy risks. For instance, **many people can be easily identified by their email address** – particularly if they use their name or the name of their business. This could be particularly troublesome for celebrities and other high-profile figures.

T-Mobile and AT&T

Both telecoms' organizations suffered data breaches resulting in **millions of user's personal information** being **exposed**. This included full names, addresses, DOB, Account numbers, social security numbers and more. T-Mobile has now fallen victim to nine data breaches since 2018.

TIGO

Reports emerged in July that one of China's most popular online messaging platforms Tigo leaked more than **700,000 people's personal data** online. The information contained people's names, usernames, gender, email addresses and IP addresses. It also included photos that users had uploaded to users' accounts as well as private messages. However, according to 'Have I Been Pwned', more than **100 million records were compromised in total.**

UK Electoral Commission

On 8 August, the Electoral commission issued a public notification of what it called a "complex cyber-attack" in which "hostile actors" **gained access to the UK's electoral registers**, which contain an estimated **40 million people's personal information**. However, a whistleblower reported to the BBC that the Commission had failed a Cyber Essentials audit around the time the attackers breached its systems. This was later backed by security researcher and cyber expert Kevin Beaumont who explained the that the Commission was known to have been **running an unpatched version of Microsoft Exchange Server** that was vulnerable to **ProxyNotShell** attacks at the time of the incident.

MoveIT & GoAnywhere (FTP services)

MOVEit breach continues to claim victims, among which the most significant – at least in terms of the number of individual victims – was Better Outcomes Registry & Network, which discovered that personal health information of approximately 3.4 million people was compromised. The number of affected **organisations** is **over 2,000** and the number of **individual victims over 60 million.**

A vulnerability in the file transfer service GoAnywhere enabled cyber criminals to exploit dozens of organisations that use the tech, with some reports estimating that as many as 130 organisations were targeted. The attacks have been attributed to the Clop ransomware gang, but the TTPs have not been consistent with their normal methods. In this case, Clop, were stealing data rather than encrypting it

Disrupted Cyber Operations

2023 Operations Shut Down by Authorities

Big Wins for the Good Guys

2023 saw multiple law enforcement agencies aimed at disrupting ransomware operators and threat actors. Multiple collaborative efforts led to the take down of known assets of these gangs, dismantling of operations and arrests.

In January 2023, an FBI-led operation with cooperation from the Department of Justice, saw the **Hive ransomware group**, who had been on a rampage of extorting over $100m from 1,500 organisations in 18 months, being **hacked and assets seized**. The FBI obtained decryption keys for the Hive strain and distributed it to the victims. The servers were taken down and the Hive group were no more.

Ref: https://www.justice.gov/

2023 THREAT INTELLIGENCE REPORT

2023 Cyberthreat Trends

Threat Landscape

Trends Throughout 2023

Rise in Nation-State Cyber Operations

Throughout 2023, nation-state actors have exhibited a **significant increase in cyber operations, targeting both governmental and private sectors**. These advanced threat actors have displayed sophisticated tactics, techniques, and procedures (TTPs) to achieve their objectives, including **espionage, disruption of critical infrastructure, and intellectual property theft**. Attribution of these attacks remains challenging, heightening the need for improved defences and international cooperation.

Accelerated Adoption of Internet of Things (IoT) Devices

The proliferation of IoT devices continued to grow exponentially in 2023, introducing new attack vectors and amplifying the overall threat landscape. Poorly secured connected devices have increasingly become targets for **botnet exploitation**, **distributed denial-of-service (DDoS)** attacks, and unauthorized access. Organizations must prioritize IoT security to prevent potential breaches and protect consumer data.

Escalation of Ransomware Attacks

Ransomware attacks have reached new heights in 2023, with threat actors employing more sophisticated techniques, targeting organizations of all sizes and industries. These attacks have resulted in significant financial losses, operational disruptions, and compromised sensitive data. Threat actors have increasingly adopted double-extortion tactics, threatening to leak stolen data if the ransom is not paid, amplifying the impact on victim organizations. Robust backup strategies, employee training, and security awareness programs are critical defences against ransomware attacks.

Exploitation of Artificial Intelligence (AI) and Machine Learning (ML)

As AI and ML technologies continue to advance, **threat actors have begun leveraging them for malicious purposes**. From generating convincing deepfake content to evading traditional security measures through adversarial attacks, AI and ML have become a double-edged sword. Protecting AI and ML systems from exploitation requires a combination of algorithmic defences, robust training data, and ongoing security research.

Supply Chain Attacks and Third-Party Risks

Supply chain attacks have emerged as a significant concern in 2023, with threat actors exploiting vulnerabilities in software dependencies and **compromising trusted vendors** to gain unauthorized access to target organizations. Organizations must strengthen their supply chain security by conducting **thorough vendor assessments, implementing secure development practices, and adopting continuous monitoring mechanisms.**

Increased Sophistication of Social Engineering Attacks

Social engineering attacks, including phishing, spear-phishing, and business email compromise (BEC), have become increasingly sophisticated and deceptive. Threat actors **exploit human vulnerabilities**, leveraging psychological manipulation techniques to deceive individuals and gain unauthorized access to sensitive information and systems. Organizations should **prioritize employee education, implement multi-factor authentication, and deploy advanced email security solutions to mitigate the risks associated with social engineering attacks.**

In the Spotlight: QR Phishing

AKA "Quishing"

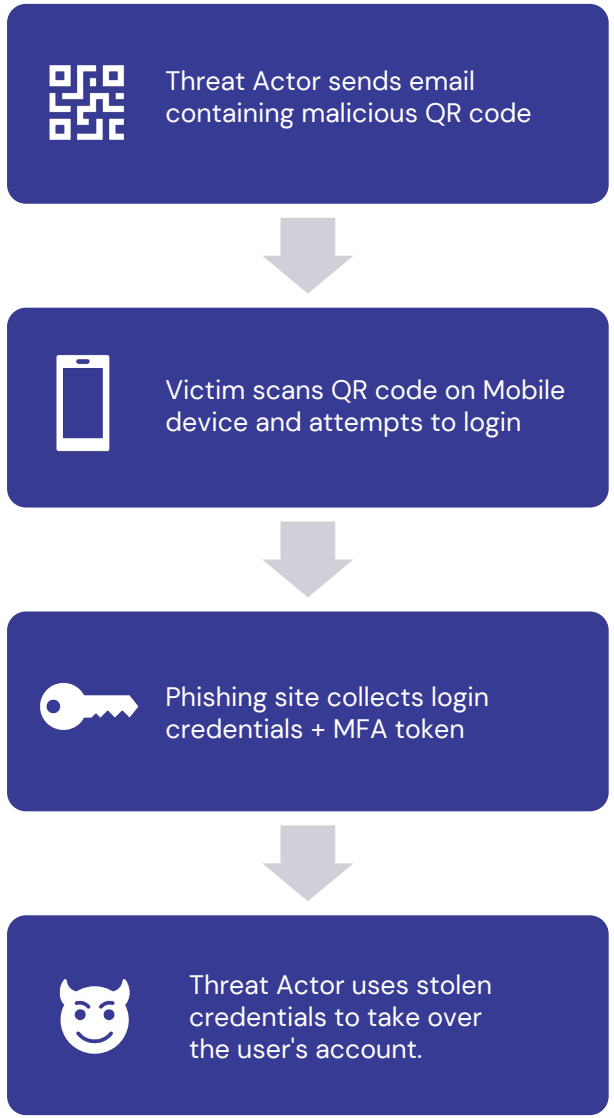
In 2023, we saw the rise of the QR phishing email. A **simple yet effective method** to bypass common security controls. The email could be as simple as a single image, designed to look like the Microsoft authentication MFA message that we see all the time.

Victims are scanning the codes on their mobile devices (which often sit outside of an organisation's security controls), leading them to an imitation Microsoft login screen to enter their credentials.

The reason this was so effective in bypassing common security controls was the simplicity of the email contents. Typically, Microsoft Defender for Office 365 scans attachments and links within emails to detect phishing attempts or malicious software. However, the QR code effectively bypasses this layer of security because the **malicious link is embedded within the QR code image**

How do we protect against this?

Educating users continues to be the best defence against all forms of social engineering. Relying solely on automated defences is not reliable. As we saw this year, threat actors will continue to adapt their techniques to bypass these defences. However, there are now detection and prevention rules in place to combat this attack vector. Additional protection can also include MDE – Mobile threat defence on mobile devices, implement continuous access evaluation. As an Ontinue customer, we now look for suspicious user activity when an email has been received, QR code scanned, and credentials used.

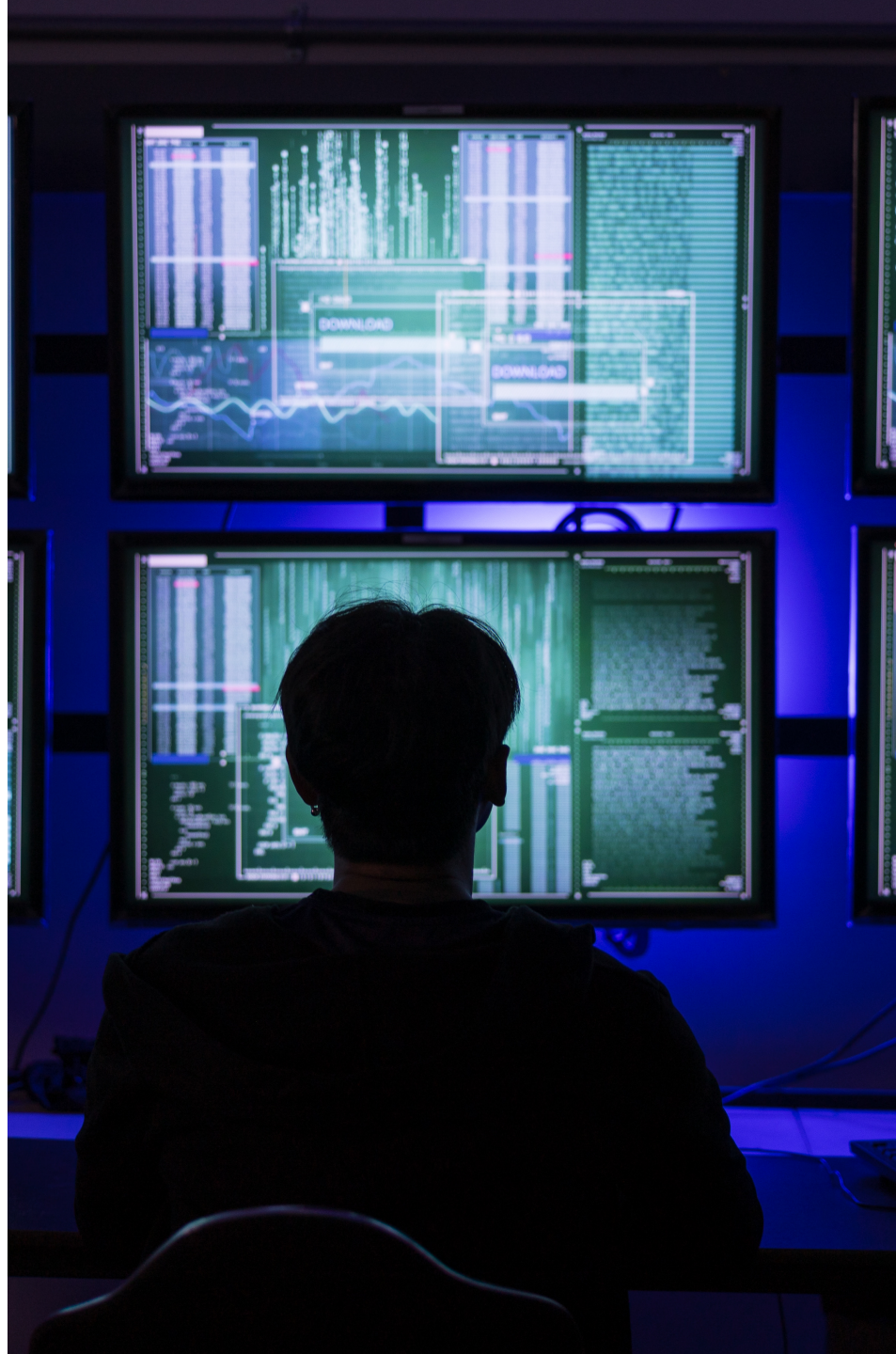


In the Spotlight: Adversary-in-the-Middle (AiTM) Phishing Attacks

In 2023, the cybersecurity landscape was transformed by the advent of Adversary-in-the-Middle (AiTM) phishing attacks. These sophisticated threats exploit real-time communications to bypass multifactor authentication (MFA), posing a significant challenge to traditional security measures.
AiTM phishing operates through deceptive tactics, where cybercriminals interpose themselves between the user and legitimate online services. The attack usually starts with a phishing email, directing the victim to a fake login page designed to mirror well-known platforms. The crux of these attacks lies in the use of a simple proxy with a sophisticated ability to intercept and manipulate sensitive data, by stealing session cookies, enabling unauthorized access to user accounts.

How do we protect against this?

Elevating user understanding through education and awareness initiatives is crucial in recognizing and avoiding phishing attempts, significantly reducing susceptibility to such attacks. Deploying sophisticated detection systems is essential for spotting irregular login activities or patterns that signal AiTM attempts, including monitoring for logins from new devices or unusual locations. Strengthening multifactor authentication (MFA) with technologies like biometric verification or physical security keys enhances resistance to interception. Furthermore, implementing vigilant monitoring for abnormal behaviors indicative of a security breach is vital, ensuring immediate action is taken to curtail unauthorized access. Together, these strategies form a comprehensive defense against sophisticated cyber threats, safeguarding digital assets and user trust.



Initial Access Methods

Used by Ransomware Operators

Phishing Emails

Threat actors commonly use phishing emails to trick individuals into revealing sensitive information or downloading malicious attachments.

Exploiting RDP Vulnerabilities

Threat actors take advantage of vulnerabilities in RDP, a protocol that allows remote access to systems, to gain unauthorized access to targeted networks.

Exploiting Software Vulnerabilities

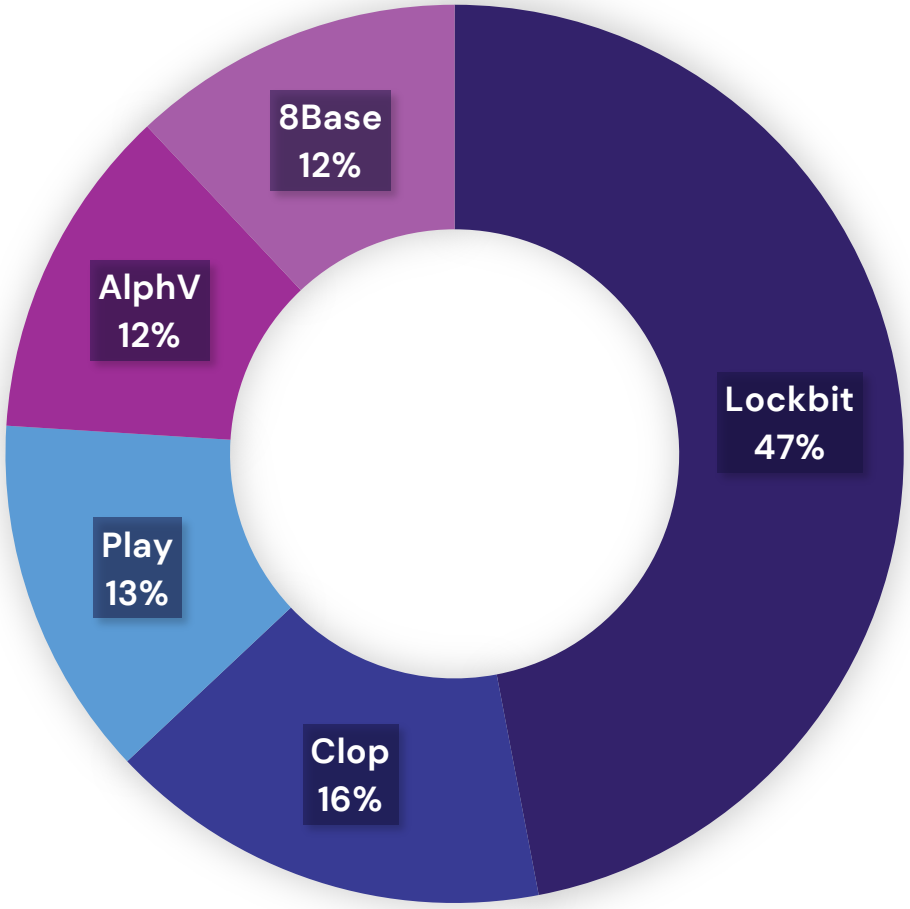
Threat actors exploit known vulnerabilities in software, such as Citrix Bleed or WinRAR vulnerabilities, to gain unauthorized access to systems.

Social Engineering

Threat actors employ social engineering techniques, such as impersonation or manipulation, to deceive individuals into providing sensitive information or granting access to systems.

Most Active Ransomware Groups

Top 5 Groups 2023



Source: https://cybernews.com/ransomlooker/

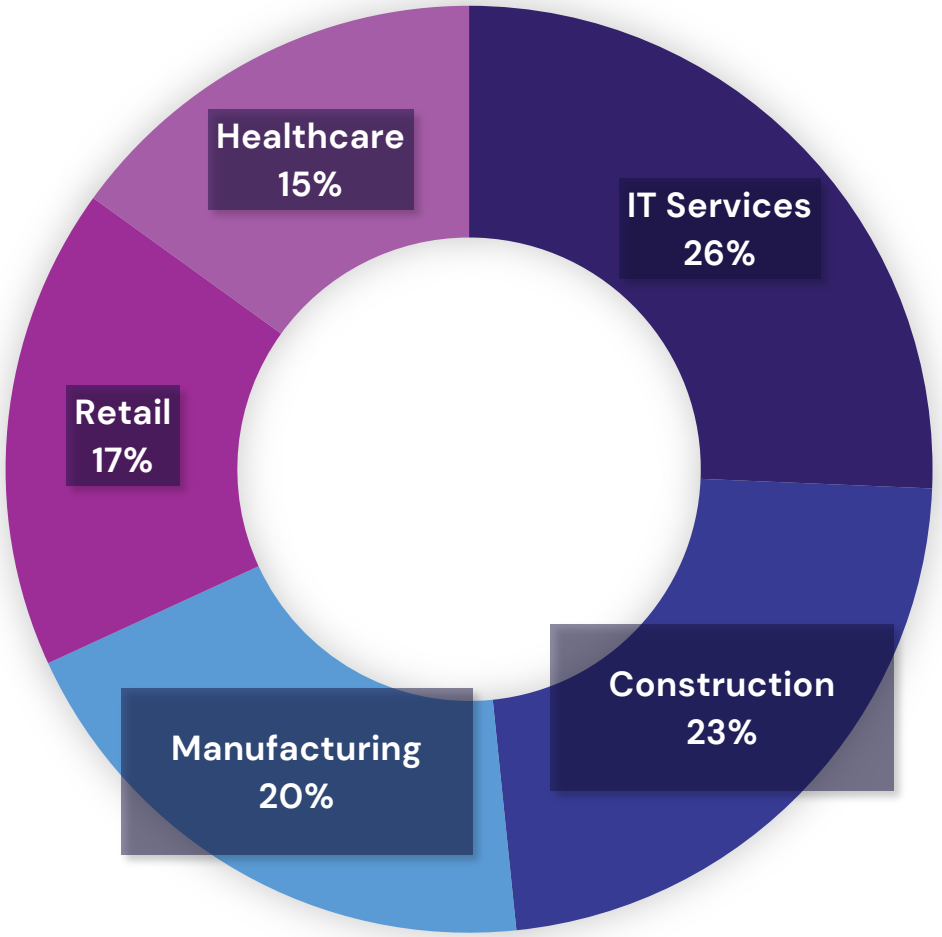
In 2023, **LockBit** emerged as the most active ransomware group, engaging in numerous high-profile attacks throughout the year. With its "name and shame" technique, LockBit threatened to leak stolen data from its victims if the ransom demands were not met. Despite efforts from law enforcement and cybersecurity firms, LockBit maintains its position as one of the most active and dangerous ransomware groups.

Lesser known **8Base** ransomware group emerged in March 2022 and has been **highly active since June 2023**, with a significant spike in their activities observed. Mainly **attacking small- and medium-sized businesses in the United States, Brazil, and the United Kingdom.**

Most Targeted Industries

By Ransomware Groups

The **information technology** and **construction** sectors were the most impacted by **ransomware** operations throughout 2023, accounting for almost 50% of all attacks. These industries are likely targeted more than others due to the large attack surfaces and the financially rich environments of these sectors.



Source: https://cybernews.com/ransomlooker/

Most Exploited Vulnerabilities

Patching is Paramount to Avoid Being Exploited

CVE-2023-38831 (RARLAB WinRAR)	A vulnerability in WinRAR software that allows remote attackers to execute arbitrary code by tricking users into opening a maliciously crafted archive file.
CVE-2023-4966 (Citrix Bleed vulnerability)	A vulnerability in Citrix NetScaler ADC and NetScaler Gateway that allows sensitive information disclosure when configured as a Gateway or AAA virtual server.
CVE-2023-34362 (Progress Software MOVEit Transfer)	A SQL injection vulnerability in Progress Software's MOVEit Transfer file transfer solution that can lead to unauthorized access and data exfiltration.
CVE-2023-36025 (Microsoft Windows SmartScreen)	A vulnerability in Microsoft Windows SmartScreen protection mechanism that allows remote attackers to bypass the protection and execute malicious code.
CVE-2023-36033 (Microsoft Windows Desktop Window Manager)	A vulnerability in Microsoft Windows Desktop Window Manager that allows remote attackers to execute arbitrary code by convincing users to open a specially crafted file or visit a malicious website.

2023 THREAT INTELLIGENCE REPORT

Threats by Industry

Common Threats

Between All Industries

The 3 most common threats across all industries are **Phishing**, **Social Engineering** and **Vulnerability Exploitation**. Threat actors can replicate these attack vectors with automated scripts and cast a wide net with broad scanning.

Industries that are compromised by these attack vectors are likely not targeted specifically. However, after the attacker receives a response from a scan, indicating a vulnerable host, or a user falls victim to a social engineering website or phishing email, threat groups can take action to engage a second level of attack or compromise.

Staff training and awareness remains the best defense against Phishing and Social engineering whereas **regular patching, vulnerability scanning, and network assessments** should be frequent. Do not rely solely on a fixed patching schedule

Phishing Emails

Social Engineering

Vulnerability Exploitation

Top Threats by Industry

Overview by Industry Vertical

Chemicals	Consulting/Business Services	Education	Engineering	Financial Services	Government
•Phishing emails and social engineering techniques targeting employees. •Supply chain attacks, exploiting vulnerabilities in manufacturing processes or compromising critical infrastructure. •Exploiting vulnerabilities in software or hardware used in chemical manufacturing processes.	•Targeted spear-phishing emails impersonating high-profile clients or executives. •Exploiting weak network security protocols and misconfigured systems. •Leveraging social engineering techniques to trick employees into revealing login credentials or granting unauthorized access.	•Social engineering attacks targeting students or staff. •Exploiting vulnerabilities in educational software or learning management systems. •Phishing campaigns targeting students, faculty, or staff.	•Exploiting vulnerabilities in engineering software or hardware. •Spear-phishing attacks targeting engineers. •Leveraging insider threats or compromised third-party contractors.	•Credential stuffing attacks using leaked login credentials. •Social engineering attacks targeting financial services employees. •Exploiting vulnerabilities in online banking systems or payment gateways.	•Advanced persistent threats (APTs) targeting government officials' email accounts or systems. •Exploiting vulnerabilities in government websites or portals. •Social engineering attacks targeting government employees.

Top Threats by Industry

Overview by Industry Vertical

Healthcare	Hospitality	Industrial Supplies	Insurance	Manufacturing	Media and Entertainment
• Ransomware attacks targeting healthcare organizations' networks. • Phishing campaigns targeting healthcare workers. • Exploiting vulnerabilities in medical devices or healthcare software.	• Point-of-sale (POS) system attacks to steal credit card information. • Social engineering attacks targeting hotel or hospitality staff. • Exploiting vulnerabilities in hotel or hospitality booking systems.	• Phishing emails targeting employees in the industrial supplies sector. • Leveraging insider threats or compromised third-party vendors. • Exploiting vulnerabilities in supply chain management systems.	• Spear-phishing campaigns targeting insurance employees. • Exploiting vulnerabilities in insurance company websites or portals. • Social engineering attacks targeting insurance agents or brokers.	• Ransomware attacks targeting manufacturing companies' networks. • Exploiting vulnerabilities in industrial control systems or manufacturing software. • Phishing campaigns targeting manufacturing employees.	• Credential stuffing attacks targeting media streaming platforms or subscription-based services. • Social engineering attacks targeting media and entertainment industry professionals. • Exploiting vulnerabilities in content management systems or streaming platforms.

Top Threats by Industry

Overview by Industry Vertical

NGO	Retail	Shipping and Logistics	Technology	Utilities
• Phishing campaigns targeting NGO employees or volunteers. • Exploiting vulnerabilities in NGO websites or portals. • Social engineering attacks targeting NGO staff.	• Point-of-sale (POS) system attacks to steal credit card information. • Phishing campaigns targeting retail employees. • Exploiting vulnerabilities in e-commerce platforms or online payment gateways.	• Phishing campaigns targeting shipping and logistics employees. • Exploiting vulnerabilities in logistics management software or supply chain systems. • Social engineering attacks targeting shipping or cargo personnel.	• Exploiting vulnerabilities in software or hardware used in technology companies. • Phishing campaigns targeting technology industry professionals. • Social engineering attacks targeting IT administrators or developers.	• Exploiting vulnerabilities in critical infrastructure systems used in utilities. • Phishing campaigns targeting utility employees or contractors. • Leveraging insider threats or compromised third-party vendors.

2023 THREAT INTELLIGENCE REPORT

A Look Ahead: Forecasts for 2024

Threats and Targets in 2024

Breakdown

Artificial Intelligence

We will see more implementation of AI as a tool for good and for more nefarious purposes like social engineering and more advanced attack vectors. Additionally, as more organisations adopt biometric security, it is likely AI will be used as a method to bypass these controls.

Internet of Things

Organisations are relying more and more on IoT devices and 5G networks, this now creates a much larger attack surface for threat groups. Also, Mobile devices are being targeted as access points and credential harvesting and we expect this could be expanded for espionage and creating a DDoS network similar to webcam DDoS attacks in 2016.

Hacktivism & Hack-for-Hire

With conflicts such as the war in Ukraine and the Israel-Hamas conflict, individual hackers and hacking groups have aligned themselves to cause disruption against the opposing force. However, hack-for-hire operations are on the rise. These operators show no allegiance and will provide services for anyone willing to pay the price.

Supply chain Attacks

Supply chains will continue to be leveraged as the initial access method of choice. Organisations must adapt their security audit process to include assessment of all third-party assets.

Threats and Targets in 2024

Breakdown

Evolving ransomware operations

Payloads and attack methods will continue to evolve, and extortion tactics have expanded. We saw this with Alphv/blackcat towards the end of 2023. Telling the victim to pay up or they'll not only release the data, but they will also inform the governing body to impose fines on them. Literally reporting their attack to the police.

Business Email Compromise

BEC can generate large financial revenues for threat groups. It is highly likely that in 2024 we will see the trend of BEC continue and frequency increase. Already, in January 2024, Microsoft announced that its own executive's email accounts had been compromised.

CNI & NIS2

In times of conflict and global tension, it is highly likely that nation state-sponsored Advanced Persistent Threat groups (APTs) will attempt to disrupt or cripple Critical National Infrastructure (CNI) to limit impact foreign economies. To bolster the defensive strategy of CNI, the EU has developed the NIS2 Directive 2022/255535 to be in effect by October 2024. However, with this deadline, it is likely that we will see opportunistic threat groups targeting EU CNI prior to the implementation of this new security legislation.

Building a Stronger Security Maturity

Best Practices to Prevent Business Disruption

The following are cybersecurity best practices to help organizations develop a stronger security posture to reduce the risk of cyber threats and data breaches.

1. Regular Software Updates and Patch Management

Keeping all software, including operating systems, applications, and security tools, up to date is crucial. Regularly install patches and updates released by vendors to address vulnerabilities and protect against known threats.

2. Strong Access Controls and Authentication

Implement robust access controls to ensure that only authorized users have access to sensitive data and systems. Enforce the principle of least privilege, where users are granted only the minimum level of access required to perform their duties. Utilize multi-factor authentication (MFA) to add an extra layer of security beyond passwords.

3. Employee Training and Awareness

Invest in cybersecurity training and awareness programs to educate your employees regarding common threats such as phishing, social engineering, and malware. Encourage a culture of that embraces security consciousness and provide regular updates on emerging threats and best practices.

4. Regular Data Backups and Disaster Recovery Planning

Implement a comprehensive backup strategy to regularly back up critical data and systems. Ensure that backups are stored securely and can be easily restored in the event of data loss or a ransomware attack. Develop and regularly test a disaster recovery plan to minimize downtime and data loss in the event of a cyber incident.

5. Network Segmentation and Monitoring

Segment your network to isolate critical systems and sensitive data, limiting the potential impact of a security breach. Implement network monitoring tools to detect and respond to suspicious activity in real-time. Monitor network traffic, user behavior, and system logs for signs of unauthorized access or malicious activity.


Ontinue
AI-Powered MXDR