The world is how we shape it

sopra steria

STATE OF CYBER SECURITY 2025

Contents

Executive Summary 03

Introduction 05

Insight : Digital Defence Directives 06

01. Cybercrime and Methods

Stages of Compromise 09

Tools and Techniques 10

Infrastructure 12

Insight : Remote Monitoring and Management 13

02. Initial Compromise 15

Phishing 15

Observed Phishing Trends in 2024 15

Social Media 19

Inside the Inbox 19

Vulnerabilities 23

Focus on virtual private network 25

Weaponization of Vulnerabilities 26

Targeting Application Programming Interface 27

Insight : OT Cybersecurity in 2024 28

03. After The Compromise 30

Malware and Stealers 31

Inside the Systems 32

Observed and Blocked 33

Insight : Repository Poisoning Ransomware Ecosystem 36

Ransomware ecosystem 38

04. Threat Landscape 39

Volatility of ransomware group 40

Key observations 41

Insight : Artificial Intelligence 42

05. Recommendations or Defenders 44

Phishing 45

Vulnerabilities 46

Malware 46

Pen-tester perspective 47

Outlook 2025 49

How Can Sopra Steria Help You 51

Executive Summary

The "State of Cyber Security 2025" report provides a comprehensive analysis of the current cybersecurity landscape, highlighting key trends, threats, and regulatory developments. The purpose of this report is to inform decision-makers about the evolving cybersecurity environment and to provide actionable recommendations to enhance organisational security.

Norway is set to introduce its first cross-sectoral regulatory framework for digital security, driven by the EU's NIS1 and elements of the NIS2 Directive. The Digital Security Act and DORA (Digital Operational Resilience Act) are pivotal in shaping the cybersecurity landscape, with DORA focusing on the financial sector's resilience against advanced threats. These frameworks aim to compel businesses to take cybersecurity seriously and integrate resilience into their core operations.

In 2024, cybercriminals employed diverse tactics, including the use of Remote Monitoring and Management (RMM) tools and legitimate software for malicious purposes. Specialization among cybercriminal groups and the exploitation of hybrid environments were notable trends. Cybercriminals used methods such as phishing, exploitation of valid accounts, and exploitation of public vulnerabilities to gain initial access.

Data collection techniques and destructive objectives like data encryption and system recovery inhibition were prevalent.

The increasing use of legitimate administration tools, malware, data theft tools, and network evasion tools by cybercriminals poses challenges to detection and mitigation efforts. The report highlights the sophistication of these tools and the need for advanced detection and response strategies.

Significant vulnerabilities were identified in Virtual Private Networks (VPNs), application programming interfaces (APIs), and other critical infrastructure components. The weaponization of vulnerabilities and the exploitation of tunnelling services for data exfiltration are key concerns. The time-to-exploit (TTE), which measures the average time taken to exploit a vulnerability after its disclosure, has significantly decreased in recent years, now being down to five days. To mitigate these risks, organizations must prioritize regular patching and updates.

Phishing remains a primary attack vector, with multi-channel phishing attacks, Adversary-in-the-middle (AiTM) attacks, and the rise of Phishing-as-a-Service (PhaaS) platforms being significant trends. The report provides detailed observations on phishing tactics and mitigation strategies, emphasizing the importance of Multi-Factor Authentication (MFA) and user awareness training.

The resurgence of malware, particularly infostealers like Lumma Stealer, highlights the role of malware in initial access operations and the challenges posed for the defenders by attackers utilizing living-off-the-land techniques. This report underscores the need for robust Endpoint Detection and Response (EDR) solutions to combat these threats.

The evolution of the Ransomware-as-a—Service (RaaS) model and the volatility of ransomware groups are examined, highlighting the significant increase in ransomware attacks and the use of advanced techniques by operators. The report recommends proactive measures, such as network segmentation and real-time threat detection, to mitigate ransomware risks.

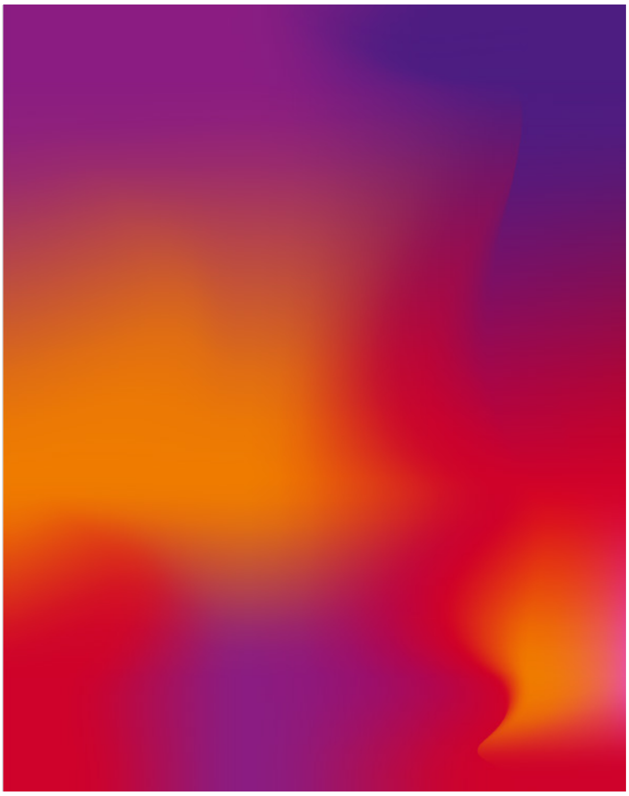
Generative AI's impact on cybersecurity includes the generation of deepfake content, social engineering, and malware development. The risks associated with shadow AI and the use of virtual agents for automated attacks are also discussed. Organisations are advised to implement safeguards to prevent the misuse of AI technologies.

Introduction

This report is structured to serve a broad audience, including security leaders, practitioners, and those with a vested interest in cybersecurity.

In an era where headlines about state threat actors and emerging vulnerabilities are a daily occurrence, determining which threats deserves attention is increasingly complex. The report compiles Sopra Steria real-world data from a wide range of organisations spanning various sectors. Readers have the opportunity to explore analyses of threat actors' methodologies, their actions post-access, and practical suggestions from incident responders aimed at protecting against such breaches. Although cybersecurity often feels like an endless struggle, this report underscores the belief that with intelligence, insight, and preparation, defenders can maintain a strategic advantage.

Ultimately, the reports aims to inform and enlighten stakeholders on a rapidly evolving threat landscape. By illuminating threats, developments and actions it can provide a strategic knowledge that can equip readers to better navigate the cybersecurity landscape.



— Ultimately, the report aims to inform and enlighten stakeholders on a rapidly evolving threat landscape.

Digital Defence Directives

"It is necessary to initiate work on the regulatory framework to ensure that the existing rules are better applied in practice and to provide a solid foundation for their renewal and further development (...),"

stated the National Strategy for Information Security in 2003.

For over two decades, Norwegian authorities have worked to highlight critical IT infrastructure. More than 20 years after the first strategy for information security, Norway is now on the verge of introducing its first cross-sectoral regulatory framework for digital security. The introduction of the Digital Security Act, which initially implements the NIS1 Directive and later the NIS2 Directive, is, however, driven by the EU. Overall, we see an increase in regulations governing cybersecurity, both nationally and regionally through EU directives. The purpose of these regulations, whether from national authorities in various countries or the EU, is to compel businesses to take cybersecurity seriously, as recommendations and voluntary measures have not been effective.

Regulatory frameworks often reflect an evolving understanding of the threat landscape, and the Digital Security Act/NIS2 is no exception. The increasing interconnectedness of critical infrastructures and reliance on digital systems have amplified vulnerabilities, making it essential to adopt frameworks that not only address existing risks but also prepare for future challenges. The Act's cross-sectoral focus represents a recognition that cybersecurity threats do not respect industry boundaries, requiring a unified approach to safeguard national infrastructure.

The year 2024 marks a turning point where the regulatory framework receives increased attention, and its impact becomes evident. DORA, which applies to the financial sector and comes into force in 2025, represents the first regulatory framework in Norway that truly addresses the complex threat landscape facing the financial sector. Among other measures, DORA introduces threat-based testing and strengthens requirements for incident response. These elements demonstrate a shift towards more robust mechanisms for identifying and mitigating risks in sectors with significant exposure to advanced threats.

Compared to the Digital Security Act, which will apply to a large proportion of Norwegian organisations across sectors, DORA is significantly more comprehensive in terms of digital operational resilience. The financial sector, given its systemic importance and susceptibility to cyberattacks, necessitates stricter regulations that emphasize not just prevention but also continuity and recovery. The detailed requirements outlined in DORA aim to ensure that financial institutions can maintain functionality even under adverse conditions, reducing the potential for widespread disruption.

The Digital Security Act, which has not yet come into force, primarily regulates fundamental security requirements. The Act requires a risk-based approach to security work within organisations. Although the framework does not explicitly mandate a threat-based approach, several elements suggest that organisations must consider the constantly evolving threat landscape in their security efforts. Firstly, the security level of organisations must be established based on an understanding of digital security as a foundation for their work. Secondly, an organisation's risk is closely linked to the threat actors it faces. Thirdly, risk-based risk management is not a static process but a dynamic approach that must adapt to changes in the threat landscape and new attack vectors.

By 2025, we can expect NIS2 to be implemented in Norwegian law. However, whether the framework will actually come into force by then remains uncertain. The framework, which is still under development, will place greater emphasis on both business continuity and incident handling. The exact scope and detail of these requirements remain to be seen. Nevertheless, the progression toward more detailed and actionable regulations indicates a broader trend of integrating cybersecurity into national strategies and frameworks.

What is crucial is that Norwegian organisations are required to adopt a holistic approach to security work, where non-compliance may result in accountability through administrative fines. The introduction of these frameworks highlights an overarching shift toward embedding resilience into the core operational structures of organisations, ensuring they are better equipped to face the challenges of a rapidly evolving digital landscape.

– Regulatory frameworks often reflect an evolving understanding of the threat landscape, and the Digital Security Act/ NIS2 is no exception. –

01 Cybercrime and methods

In 2024, cybercriminals employed a diverse array of tactics, techniques, and procedures (TTPs) spanning multiple stages of the Kill Chain. They exploited numerous tools, malware, and methods to advance their attacks, illustrating significant trends in the evolution of cyber threats. These trends highlight attackers' efforts to evade traditional detection systems and leverage the complexities of hybrid environments.

Notably, there has been an increased use of Remote Monitoring and Management (RMM) tools, which, due to their extensive capabilities and integration in some corporate environments, enable attackers to deploy a variety of techniques while camouflaging within legitimate traffic.

Analysis of prevalent tools and malware indicates a diversification in methods and an enhanced exploitation of legitimate software for malicious objectives.

The year 2024 saw a specialization among cybercriminal groups, with more groups focusing on one stage of the attack chain rather than the entire attack. For example, attackers specializing in initial access, vulnerability exploits or malware development.

Criminal actors innovate with evasion techniques and enhanced encryption to bypass security solutions. The persistence of these actors demonstrates the lucrative interest for cybercriminals in this method of extortion, especially through double extortion attacks.

Cybercriminals, increasingly adaptive, are focusing on network infrastructures and SaaS platforms, targeting the foundations of cloud environments and remote work. This transition not only illustrates their ability to exploit organisational weaknesses, such as patch management, but also their strategy to maximize impact in an interconnected world.

Stages of compromise

Initial Access

Sopra Steria's own observations has been that cybercriminals primarily exploited the following techniques in the MITRE ATT&CK framework[1] to gain access to systems throughout 2024 :

- Phishing (T1566) : Cyber threats continue to show innovation in phishing campaigns.
- Valid Accounts (T1078) : The prevalence of stealers in 2024 significantly influenced how threat actors obtained their initial access to target systems.
- Exploitation of Public Vulnerabilities (T1190) : Exploiting vulnerabilities in internet-exposed systems remains a method marginally used by the cybercriminal sphere.

The methods used by cybercriminals to gain initial access to compromised systems increasingly involve using valid accounts previously acquired by threat actors. Through an initial compromise by a stealer, RDP, SSH, or other, credentials are purchased on the darknet and then repurposed for other uses.

Data Collection

Attackers have diversified and intensified their search for sensitive information on compromised systems. This explains the presence of the following techniques in the top techniques of 2024 :

- OS Credential Dumping (T1003) :
- Data from Local System (T1005) :
- Exfiltration Over C2 Channel (T1041) :

Impact and Destructive Objectives

- Data Encryption (T1486) : Primarily used in ransomware attacks to make data inaccessible to victims.
- Inhibit System Recovery (T1490) : Prevents victims from restoring systems from backups, exacerbating the attack's impact.

These methods indicate a destructive end goal alongside significant impacts on target systems.

[1] https://attack.mitre.org/techniques/enterprise/

Tools and Techniques

The increasing use of legitimate services and platforms by cybercriminals marks a significant shift in their tactics. No longer confined to traditional malicious tools, they now adopt a “Living off the Land” approach, using existing tools already installed on the target system.

This evolution reflects their advanced experience and deep understanding of the environments they target, showcasing a new level of technological maturity.

Increased use of legitimate administration tools :

Tools like ADExplorer, AnyDesk, Advanced IP Scanner, and PsExec are often repurposed for use in intrusions into corporate systems. These tools allow attackers to explore infrastructure, maintain persistent access, and extend their attacks while reducing detection risk by appearing as legitimate operations.

For example, AnyDesk and TeamViewer facilitate remote control, while ADExplorer and PowerShell commands allow mapping of Active Directory.

Proliferation of Malware and Data Theft Tools

Data theft tools like Mimikatz, LaZagne, and others, as well as targeted malware such as Lumma Stealer, Redline and Raccoon Stealer, have been widely used to extract credentials.

These tools enable attackers to exfiltrate passwords and sensitive information, facilitating unauthorized access and lateral movement within enterprise networks.

Cybercriminals frequently update their tools to avoid detection. For instance, Lumma Stealer gets weekly updates to its code and servers, making it harder to detect and more appealing to criminals. This rapid update cycle helps it stay ahead of web browser security features. Similarly, Latrodectus, the successor of IcedID, removes features in its updates to evade detection.

Exploitation of Tunneling Services and Network Evasion Tools

Cybercriminals use tunneling services like Ngrok and Cloudflare Tunnel to, bypassing security measures. These tools make it harder to detect and stop malicious connections, showing attackers' growing sophistication in evading network defences.

Use of Vulnerability Exploitation Tools

Tools and techniques such as Metasploit, Nmap, and Kerberoasting are used to identify and exploit vulnerabilities within network systems and authentication services. By uncovering security misconfigurations, these approaches enable attackers to infiltrate and potentially compromise entire infrastructures.

Evasion and Persistence Tools

Attackers use tools like SystemBC and SocGholish to hide their presence and maintain access to infected systems. They also use BITSAdmin and PowerShell to automate malicious tasks. This hybridization of legitimate tools and advanced malware makes their actions harder to detect and more effective.

Use of Legitimate Services for Data Exfiltration

Cybercriminals use file-sharing platforms like Dropbox and MEGA to secretly exfiltrate stolen data. By leveraging trusted services, they make detection harder for security teams, showing their skill in bypassing traditional defences and exploiting weaknesses in external services.

Multiple C2 Channels to Avoid Detection

Attackers use channels like Discord, Telegram, IRC, and SMTP to communicate with infected machines. This variety shows their technical skill in maintaining flexible and resilient command and control (C2) systems. By using multiple services, they reduce the risk of disruption if one channel is blocked, demonstrating their adaptability.

Infrastructure

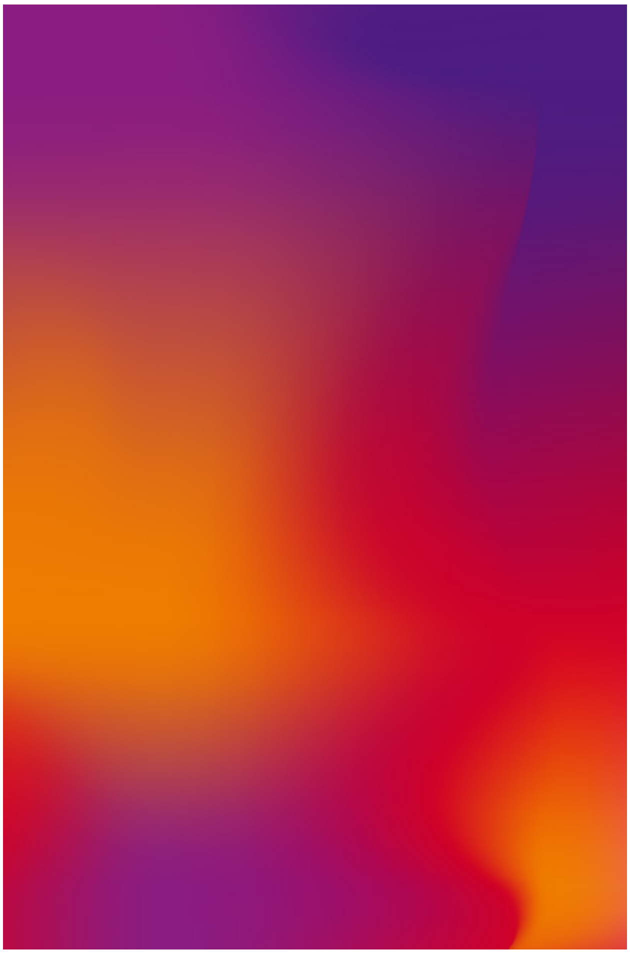
Exploitation of APIs and Streaming Technologies

Attackers use APIs from services like GitHub, GitLab, GoFile, and Vimeo to integrate these platforms into their C2 processes. This automation enhances their operations' resilience and efficiency.

Using technologies like WebSockets and WatsonTCP shows their expertise in advanced communication protocols.

Obfuscation via Randomly Generated Destination Algorithms

By employing algorithms that generate random destinations for data transfer, cybercriminals complicate the detection of exfiltration flows. This obfuscation technique demonstrates an understanding of network traffic analysis methods and ways to circumvent detection measures based on behavioral models.



Use of Public Cloud Solutions

Attackers use services like CloudFlare, Amazon Web Services and Firebase to hide their activities behind legitimate cloud infrastructure. This makes it harder for security analysts to distinguish between normal and malicious traffic, showing attackers' maturity and knowledge of cloud security practices.

Remote monitoring and management

A Remote Monitoring and Management (RMM) tool is a type of software designed to help managed service providers (MSPs) and IT professionals remotely monitor and manage client endpoints, networks, and computers when physical access is limited. These tools typically offer a range of features, such as remote access, monitoring, automation, alerting, reporting and security management.

While designed for legitimate purposes, they are increasingly exploited by attackers for their extensive capabilities. Cybercriminals use RMM tools to remotely control victim computers, conduct reconnaissance, deploy malware, and maintain persistent access, often bypassing traditional security measures due to their legitimate nature. This was seen in a campaign in August 2024, where attackers used social engineering, such as phishing and phone calls, to trick victims into installing the RMM software AnyDesk. Both state-sponsored threat actors and ransomware groups use RMM tools for unauthorized access, persistence, command execution, and data exfiltration. Notably, ransomware attacks between July and August 2024 involved AnyDesk and altered RDP settings to deploy ransomware and exfiltrate data.

Adversaries often use social engineering, like threatening pop-ups, phishing, or targeted calls, to trick victims into installing RMM software.

As examples, two campaigns from August 2024 convinced victims to install AnyDesk, a legitimate RMM :

Initial access :

- Email bombs and persuasive phone call.
- Impersonated UK banks, utilizing spoofed websites and phishing methods.

Post-installation :

- Delivering various payloads, such as System BC malware and reverse SSH tunnels, to elevate privileges and execute malicious activities on compromised systems.
- Gained access to victims' bank accounts and exfiltrated data.

RMM tools are often used by ransomware groups because they can establish persistence and remote control, but they can also aid in the deployment of ransomware and the exfiltration of data. As examples, ransomware attacks, conducted between July and August 2024, leveraged AnyDesk or altered Remote Desktop Protocol (RDP) settings :

Initial access :

- Play exploited internet-facing systems and compromised credentials to access exposed RDP and Exchange server systems.

- INC Ransomware used Gootloader infections for a campaign targeting US hospitals.

- Mad Liberator targeted victims who were already using AnyDesk, sending unsolicited connection requests to gain unauthorized access.

- Akira exploited an unpatched Veeam backup server via CVE-2023- 27532.

Post-installation :

- RMM tools are used to maintain persistence, exfiltrate data and ultimately deploy the ransomware.

- Disable user input.

Protect your organisation from Remote Monitoring and Management threats.

To be able to detect malicious RMM activity involves a combination of technical measures and analysis, such as :

- Endpoint Detection and Response (EDR) : Implement EDR solutions that monitor endpoint activities and detect suspicious behaviours. EDR tools can identify unauthorized RMM tools based on their behaviour and communication patterns.

- Regular Audits : Conduct regular security audits and vulnerability assessments to identify and mitigate potential risks. Audits can help uncover unauthorized software installations and configurations.

- Application Whitelisting : Implement application whitelisting to ensure only approved software can run on your network. This can prevent unauthorized RMM tools from being installed and executed.

02 Initial compromise

Initial compromise is the phase where adversaries try to gain their first foothold within a network. In 2024, Sopra Steria observed that cybercriminals primarily relied on three techniques to infiltrate systems : phishing, the use of valid accounts, and exploiting public vulnerabilities. This section will offer an analysis of the 2024 phishing trends, alongside observed vulnerabilities for the same year.

Phishing

Phishing has transformed from a mere nuisance into a cornerstone of modern cybercrime, exploiting both human and technical vulnerabilities. It stands as the leading initial attack vector, with both the frequency of attacks and the sophistication of tactics escalating each year. In 2024, Sopra Steria observed that 59.9% of all incidents within their customers' networks were phishing related.

The increase in phishing incidents noted by Sopra Steria in 2023 has persisted throughout 2024.

Observed phishing trends in 2024

Phishing trends in 2024 show similarities to previous years but have evolved, with new techniques emerging to adapt to changing environments. This section provides an analysis of the most prevalent phishing tactics observed by Sopra Steria throughout the year of 2024.

Credential Harvesting

One of the most significant and continually increasing trends is credential harvesting. Beyond immediate exploitation, these credentials are often sold or traded for use in follow-up attacks such as account takeovers, financial fraud, and identity theft.

As such, credential theft fuels a large thriving underground market for stolen credentials.

Multi-Channel Phishing Attacks

In 2024, multi-channel phishing attacks have increased, with threat actors using SMS, phone calls, and messaging apps alongside email. Actors often pose as IT support staff to deceive target users into downloading malicious software or granting access. According to telecommunications providers in Norway [2], spoofing filters have been introduced that are more effective at blocking fake calls. This has led to threat actors increasingly using Danish and Swedish numbers to bypass defences.

[2] https://www.telenor.no/bedrift/aktuelt/sikkerhet/spoofing-filter/

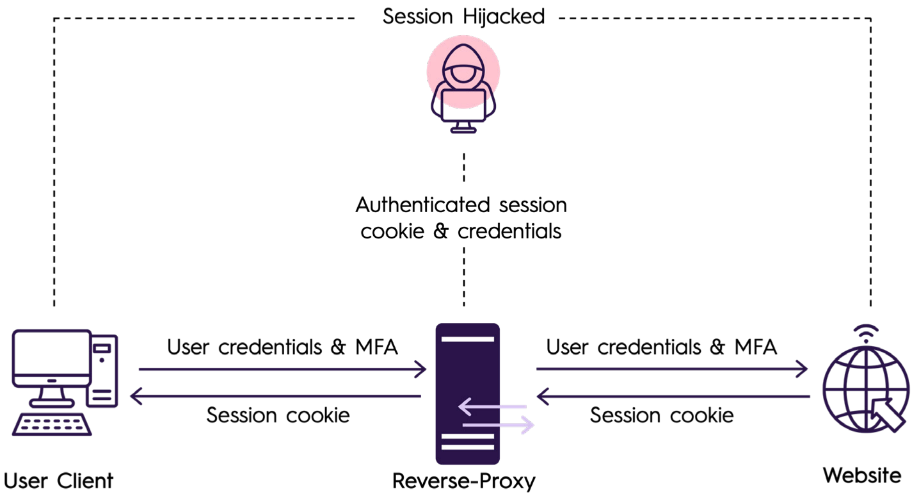
Adversary-in-the-Middle

Sopra Steria has observed a high prevalence of AiTM attacks in our customer base throughout 2024.

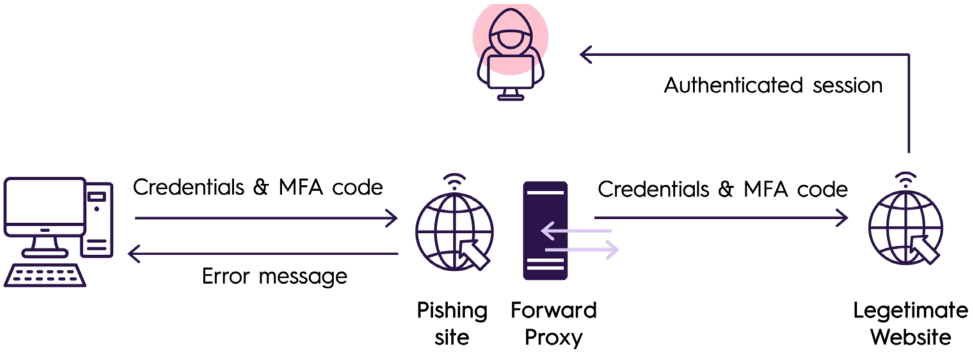
The availability of PhaaS platforms like Tycoon and Evilginx has contributed to the growing popularity of AiTM attacks, making them easily accessible to threat actors regardless of their technical ability. These attacks use proxies to intercept communication between users and legitimate websites, capturing credentials and session cookies to bypass multi-factor authentication (MFA).

Observed techniques include reverse-proxy AiTM attacks, which target specific accounts by intercepting traffic to legitimate sites, and forward-proxy AiTM attacks, which mimic sign-in pages to steal credentials and MFA tokens without directly proxying traffic.

Reverse-Proxy AiTM



Forward-Proxy AiTM



Example

On April 18, 2024, the UK's Metropolitan Police Service, along with international law enforcement and private industry partners, successfully took down LabHost, a PhaaS provider. LabHost, also known as LabRat, emerged in late 2021 and offered various phishing services targeting banks and other organisations, primarily in Canada, the US, and the UK.

At the time of the takedown, LabHost had over 2,000 criminal users who deployed more than 40,000 fraudulent sites, affecting hundreds of thousands of victims worldwide. The platform provided tools for obtaining two-factor authentication codes, customizable phishing templates, and a popular SMS smishing component.

Example

Sopra Steria has observed several incidents involving the use of Tycoon and Evilginx. After the initial foothold, these incidents often involve adding additional authentication devices to the user account for persistence, querying for sensitive documents, and adding inbox rules to mailboxes.

Phishing-as-a-Service

PhaaS has become a significant force in the global phishing landscape by offering turnkey solutions that simplify and streamline phishing operations. In 2024, the majority of phishing emails originated from these platforms. By providing ready-made phishing kits, counterfeit domains, and comprehensive support services, PhaaS lowers the barrier to entry for cybercriminals, enabling more widespread and sophisticated phishing attacks.

Platforms like "Darcula," "Tycoon," and "Caffeine" (now "ONNX") enable even low-skilled attackers to launch sophisticated campaigns, often targeting Sopra Steria has observed several MFA-protected accounts through built-in AiTM capabilities. The adaptability of PhaaS platforms, which included tactics like embedding phishing URLs in HTML, PDFs, or ZIP files to bypass detection, led to a notable increase in credential harvesting in 2024. During that year, major PhaaS providers sent millions of phishing emails each month, significantly amplifying their impact.

Social media

The use of social media and fake profiles in phishing attacks has grown significantly in 2024. Threat actors monitor platforms like LinkedIn in real time, exploiting updates such as job titles to launch social engineering attacks soon after changes are made. Sopra Steria has observed cases where this tactic was used to gain initial access to victims' systems.

Additionally, state actors have been observed conducting phishing campaigns that involve actors impersonating recruiters or job seekers.

Using AI tools, they craft convincing profiles and resumes to lure targets into fake meetings, direct them to malware-laden portals, or compromise credentials via bogus skills assessments. In some cases, attackers secure remote work positions to abuse legitimate access, stealing data, intellectual property, and funds.

Attachments

Sopra Steria's analysis of customer data reveals that the most common file types found in quarantine folders, excluding image and text files, are RAR, HTML, ZIP, PDF, and DOCX. This aligns with global patterns of commonly used file types in phishing and other cyberattacks. Globally we have observed intriguing global phishing techniques. Examples include SVG files, OneNote documents with embedded malicious URLs, and RDP files as attachments. These instances are relatively rare in our customer data, likely due to our proactive measures in blocking these attachments and the fact that such methods are often employed by smaller, specialized groups with specific targets.

Inside the inbox

In 2024, Sopra Steria saw a total of 824 million email events across the customer base, with each inbox email averaging 4.6 URLs and 1.7 attachments. This prevalence of embedded links and files underscores the challenge of distinguishing legitimate emails from potential threats, increasing the risk of phishing attacks. This section will specifically discuss our observations on quarantined emails, attachments, and domain-related threats within Sopra Steria's customer base.

Quarantined emails

An analysis of Sopra Steria's customer data from 2024 revealed that over 29 million emails— ~3,6% of all emails—were either quarantined or marked as junk. While not all quarantined and junk emails are phishing attempts, they often indicate suspicious patterns, making them valuable for threat analysis.

Top five file types found in quarantined folder

8.2 % RAR

RAR files are frequently exploited in phishing campaigns due to their ability to bundle multiple malicious components. Encrypted or password-protected RAR files can bypass email filters, hiding their contents from automated scans, and delivering malware such as ransomware or Trojans.

6.1 % HTML

HTML files are commonly used in phishing attacks due to their versatility. They often contain URLs that lead to phishing sites or connect to attacker-controlled servers to deploy phishing content. To evade detection, HTML files are frequently embedded within ZIP archives, Microsoft Office documents, or other file types. Techniques like HTML smuggling, where malicious code is hidden within the HTML, allow attackers to bypass security filters and deliver malware or credential phishing schemes.

6,1 % ZIP

ZIP files are a common phishing tool due to their ability to compress and hide malicious payloads. Attackers use them to bundle harmful components and bypass security filters, especially when encrypted or password—protected.

RAR files, however, are often favored over ZIP because they can bundle more complex structures, making them more effective in sophisticated phishing campaigns.

6.0 % PDF

PDF files remain a popular phishing vector, often containing URLS that lead to phishing sites through multi-step redirections. These may involve legitimate services, CAPTCHA challenges, or direct links to phishing domains. Attackers often hide PDFs within layers of other file types, like ZIP files, or host them on legitimate platforms to evade detection. This approach mirrors HTML phishing tactics and underscores attackers' adaptability in using trusted formats for malicious purposes.

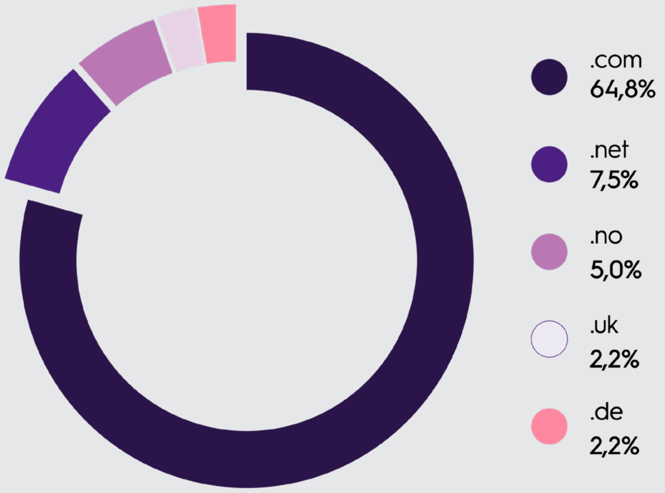
3.4 % DOCX

DOCX files, despite a low quarantine rate, still pose a threat. Although macros are blocked by default in modern Office installations, attackers use alternative exploitation methods such as template injection. In 2024, a notable trend involves using corrupted DOCX files in phishing campaigns. These damaged files can bypass security filters, and when recipients open them, Word's recovery feature restores the document, prompting interaction with embedded malicious content.

Domains

The top-level domains (TLD) most frequently identified in quarantine folders across Sopra Steria's customer base in 2024 were .com, .net, .no, .uk, and .de. Notably, a portion of all TLDs in these folders originates from .ru (Russia) and .cn (China). These TLDs are rarely associated with legitimate email communications for our customers, making their presence especially interesting.

Top five TLDs found in quarantined emails



The top five TLDs found in quarantined emails reflect a mix of trusted global and regional domains. While expected in Sopra Steria's networks, their widespread use and credibility make them prime targets for abuse. Phishing campaigns often exploit popular TLDs like .com, .net, and region-specific domains such as .no, .uk, and .de to appear legitimate. These domains are frequently paired with bulletproof hosting services that resist take-downs and legal action, providing attackers with stable infrastructure for malicious activities.

Attackers increasingly integrate these TLDs with cloud platforms like AWS and Google Cloud to host phishing pages, blending malicious traffic with legitimate use. Trusted services such as Dropbox and OneDrive are also used to host payloads, while free certificates (e.g., Let's Encrypt) enable the creation of convincing, HTTPS-secured phishing sites.

Phishing URLs combine these elements with tactics like typosquatting, redirect chains, and encoded parameters, masking their intent while mimicking trusted brands.

Business Email Compromise (BEC) is a sophisticated form of cybercrime where attackers use email to deceive businesses into transferring money or sensitive information. These attackers often impersonate high-ranking executives or trusted partners, using tactics like fake invoices or urgent requests to manipulate their targets. The goal is to exploit the trust and authority associated with the impersonated email accounts to carry out fraudulent activities.

Business Email Compromise (BEC) has evolved with the integration of generative AI tools, leading to more sophisticated and harder-to-detect attacks. Traditional cybersecurity measures are struggling to keep up, necessitating multilayered defence strategies.

BEC scams can involve spoofing email accounts, spear phishing, and using malware to infiltrate networks and time fraudulent requests. Attackers often manipulate inbox rules to hide their activities, move laterally within organisations, hijack conversations, and tamper with multi-factor authentication to maintain access. They also exploit legitimate applications for mailbox exfiltration and conduct low-profile attacks to evade detection.

In 2024, Sopra Steria managed several significant Business Email Compromise (BEC) cases. One observed tactic involved using compromised accounts within external organizations in the same sector. These accounts were used to send phishing emails, which successfully bypassed the target company's email filters due to their origin from known external vendors or partner organizations.

This strategy also exploited the inherent trust of the target recipients. In some incidents observed by Sopra Steria, the attackers use compromised accounts to send additional phishing emails, further spreading the attack within the organisation. After initial access of user accounts, attackers typically search for sensitive documents like financial data, set up inbox rules, and use the compromised accounts to send phishing emails internally and to external organisations.

> — Business Email Compromise (BEC) has evolved with the integration of generative AI tools, leading to more sophisticated and harder-to-detect attacks.

Vulnerabilities

The year 2024 saw significant developments in the landscape of cybersecurity vulnerabilities. Various sources [3] [4] reported a notable increase in the total number of vulnerabilities discovered compared to 2023. Additionally, the number of exploited vulnerabilities rose by approximately 20 percent [5].

Among the most notable vulnerabilities categories were Cross-Site Scripting (XSS), classified as the most critical software vulnerability of 2024 by MITRE and the Cybersecurity and Infrastructure Security Agency (CISA), surpassing 2023 by 10.2%.

Out-of-Bounds Write and SQL Injection also continued to dominate the threat landscape. These categories, identified in the MITRE 2024 CWE Top 25 list, highlighted persistent weaknesses in software systems that adversaries frequently exploited to compromise data and disrupt services.

[3] https://www.statista.com/statistics/500755/worldwide-common-vulnerabilities-and-exposures/

[4] https://www.secpod.com/blog/the-cybersecurity-landscape-of-2024-key-insights-from-the-annual-vulnerability-report/

[5] https://vulncheck.com/blog/2024-exploitation-trends

Number of vulnerability alerts created by Sopra Steria SOC

January

GitLabEE/CE
Cisco Unified Communications
Ivanti
Citrix Netscaler
Jenkins

February

Ivanti
Fortnet

March

Cisco Secure Client

April

xz/liblzma
Palo Alto
GlobalProtect
Oracle
Cisco
ArcaneDoor

May

Check Point Security Gateway

June

MOVEit Gateway/Transfer
GitLab pipeline

July

Cisco Smart software
Oracle
Cisco Email Gateway
OpenSSH
Git cloning repositories
Cisco Nexus Switch
Citrix Netscaler
GitLab

August

Windows TCP IP
Apache HTTP Server

September

GitLab CEÆE
VMware Vcenter
SolarWinds
GitLab
Cisco Smart Licensing
Veeam
Linux CUPS

October

Firefox
WhatsUp Gold
WatchGuard
GitLab
Junos
Cisco ASA, FMC & FTD

November

Palo Alto
FortiOS SSLVPN
Citrix Virtual Apps & Desktops
Ivanti

December

Apache Struts
Cisco ASA
Ivanti Cloud Services Application
Privileged Remote Access (PRA) and Remote Support (RS) products
Palo Alto PAN-OS
Apache MINA framework

Regularly addressing Windows vulnerabilities through Microsoft's Patch Tuesday releases is beneficial, as it shortens the lifespan of these vulnerabilities. Consequently, companies that schedule their Windows system updates based on these releases are less affected by vulnerabilities in Microsoft products. However, vulnerabilities in platforms outside of Microsoft's scheduled release, like Fortinet, Cisco, Citrix, and VMware etc have become attractive targets for malicious entities, with several high-profile state-sponsored and criminal groups utilizing these exploits for ransomware attacks and espionage operations.

Focus on virtual private network

Ransomware operators maintained their focus on VPN solutions during 2024, both for exploit and as an access point for using breached credentials. The focus of ransomware attacks shifted towards exploiting vulnerabilities in network perimeter technologies, such as VPNs and virtual desktop infrastructure, often due to missing or unenforced multi-factor authentication. Heavily targeted were VPN solutions that use Secure Socket Layer/Transport Layer Security (SSL/TLS), often known as SSLVPN, WebVPN, or clientless VPN.

These solutions are frequently targeted by threat actors because of their high exposure on the public internet, which makes them visible and accessible to attackers.

The reliance on outdated security practices and algorithms further worsened the situation, making these solutions susceptible to brute-force and other forms of attacks. Additionally, generic implementations of these solutions often lack robust authentication, often relying on single-factor authentication that can easily be compromised.

This has caused many countries' security authorities, including NCSC in Norway, to recommend replacing remote access solutions that use SSL/TLS with more secure alternatives.

Example

Notable vulnerabilities, like those exploiting Windows SmartScreen, gained particular attention due to their recurring exploitation by threat actors aiming to bypass security measures integral to Windows Defender. Specifically, CVE-2023-36025 was leveraged by cybercriminal groups like TA544 to deploy the Remcos remote access Trojan in sophisticated attacks primarily targeting institutions in Europe.

The Windows SmartScreen security feature bypass vulnerability (CVE-2024-21351) was actively exploited by numerous hacking groups who used it to infiltrate financial institutions and deploy malware such as DarkGate and Phemedrone Stealer.

Example

Ivanti's Connect Secure and Policy Secure products received significant attention due to several critical vulnerabilities detected, which were exploited by various cyber threat actors, including sophisticated state-sponsored groups.

" The focus of ransomware attacks shifted towards exploiting vulnerabilities in network perimeter technologies, such as VPNs and virtual desktop infrastructure, often due to missing or unenforced multi-factor authentication. "

Weaponization of vulnerabilites

Throughout the year, ransomware groups continued their long-standing focus on exploiting system vulnerabilities, a trend observed consistently over the past years. A notable shift occurred with the disruption of established players like LockBit, leading to the emergence of new ransomware strains such as RansomHub, Fog, and 3AM. Unlike their predecessors, these new strains exploit vulnerabilities at the execution level, rather than at the network or application level. This shift has been accompanied by advanced anti-detection measures, including the use of passwords to block access to embedded configurations, which protect their payloads and complicate reverse-engineering efforts. Consequently, these measures have significantly hindered detection and mitigation efforts.

A significant area of vulnerability exploitation was seen in the evolution of evasion techniques used by infostealers, trojans, and loaders. Malware like Raspberry Robin exploited emulator and sandbox vulnerabilities by using virtual dynamic-link libraries (VDLLs).

By identifying and responding to sandbox environment vulnerabilities, this malware effectively evaded detection. Similarly, RedLine took advantage of vulnerabilities related to the analysis of less-common programming languages, such as Lua, evading traditional malware detection systems not equipped to parse such languages.

Another trend observed during 2024 was a shift towards exploiting simpler, more accessible vulnerabilities. Command Injection and Improper Authentication issues were frequently targeted, reflecting a broader trend of threat actors favouring low-complexity, high-impact exploits.

An example of this was the authentication bypass vulnerability in Palo Alto Networks PAN-OS management web interface (CVE-2024-0012). This shift was also evident in the increased exploitation of Command Injection (CWE-77) vulnerabilities, such as the vulnerability in the Cisco NX-OS Software (CVE-2024-20399) with a CVSS score of 6.7. This has led to an increase in successful attacks and a higher risk of data breaches and system disruptions.

Targeting application programming interface

Application Programming Interface (API) adoption has surged, essential for microservices, AI proliferation, and container-driven architectures, making them attractive for innovation. This rapid adoption has also expanded the attack surface for malicious actors, evidenced by a notable 80% increase in API-related data breaches within the past year. These breaches have exposed over 1.6 billion records, underscoring the urgency of fortifying API security[6].

APIs are vulnerable to a wide array of threats, often compounded by their openness. These risks include data breaches and unauthorized access because of misconfigurations or insufficient perimeter validation. The ease of exploiting APIs has grown, particularly with advancements in AI API calling capabilities, which democratizes access, allowing attackers, regardless of their expertise, to probe APIs extensively and efficiently.

Example

Both malware loaders and ransomware capitalized on system defence vulnerabilities. Operations involving GuLoader and Remcos exploited vulnerabilities starting from phishing email vectors.

GuLoader used complex evasion techniques to manipulate and bypass system defences, while Remcos exploited system vulnerabilities to maintain remote control, enabling subsequent ransomware deployment.

Example

GitHub Repository Secret Spill, which leaked 13 million API secrets, demonstrate that attackers highly value API secrets for use in further compromises. This mirrors the patterns observed with regular user credentials.

[6] https://www.firetail.io/reports/the-state-of-api-security-2024

OT Cyber-security in 2024

In 2024, we saw a significant surge in interest in OT cybersecurity in the Nordics, driven by an increase in international incidents and heightened regulatory demands. Ransomware continues to dominate as the most prevalent threat, targeting industries across the board, from energy and manufacturing to public utilities. Meanwhile, the rising frequency of zero-day exploitations and the previous uncovering of advanced tools like PipeDream underscore the growing vulnerable state of industrial control systems (ICS), which are critical to modern infrastructure.

International developments, such as the ongoing fallout from the SolarWinds supply chain attack and the SEC's liability rulings, have further amplified the focus on supply chain security. Organisations are increasingly adopting measures like software bill of materials (SBOM) controls and inventory systems to address these risks and ensure compliance.

Regulatory pressures have also intensified. Updates to Norway's Digital Security Act, the NIS2 Directive, the Cyber Resilience Act (CRA), and various sector-specific regulations have driven stricter compliance requirements. Critical infrastructure operators now face greater scrutiny to implement robust security frameworks like IEC 62443, identify and manage cybersecurity risk for their OT-environment, and develop stronger resilience into their operations.

Amid these challenges, there is a growing movement toward proactive cyber-security strategies. Organisations are adopting measures such as network segmentation, real-time threat detection, SOC services tailored to include OT environments, and comprehensive employee training programs. The integration of these efforts with regulatory compliance is not just addressing immediate threats but is laying the groundwork for a stronger, more resilient approach to securing critical infrastructure against an increasingly sophisticated threat landscape.

That said, the journey toward appropriate protection and resilience, proportional to the potential consequences from incidents, for critical infrastructure is far from over. Many organisations are still in the early stages of implementing necessary security measures, and the road ahead will require sustained focus, investments, and innovation. Encouragingly, we see some of our clients setting a global standard in OT cyber-security, proving that world-class security is achievable. These pioneers offer a glimpse of what is possible, even as the broader landscape continues to evolve and adapt to emerging threats.

— Critical infrastructure operators now face greater scrutiny to implement robust security frameworks like IEC 62443, identify and manage cybersecurity risk for their OT- environment, and develop stronger resilience into their operations.

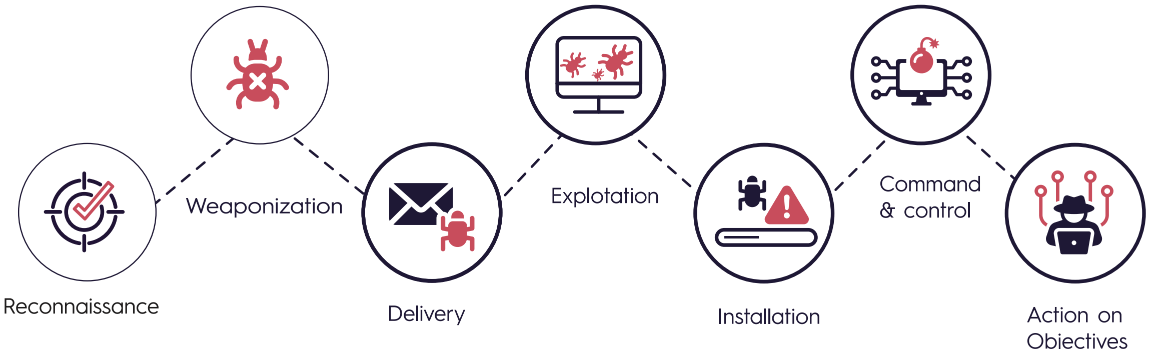
03

After the compromise

In 2024, cybercriminals continued to utilize a wide range of tools, malware, and techniques to carry out their attacks, revealing significant trends in the evolution of cyber threats. There has been a diversification of methods and an increased exploitation of legitimate software for malicious purposes. This section will cover 2024 trends related to malware, stealers, and hack tools. Sopra Steria observations show that malware has experienced a resurgence, especially through the use of infostealers.

This is also supported by other security services like ENISA (European Union Agency for CyberSecurity). Examples include RedLine, Raccoon Stealer, Vidar, Agent Tesla, FormBook, and Lumma stealer. Notably, Lumma Stealer has been vastly observed in Sopra Steria`s customer base throughout the second half of 2024.

> *"Another challenge for cybersecurity defences is the increased use of Living-of-the-Land Techniques, where actors use legitimate tools and functions of the infrastructure they are attacking, manipulating the functionality to fit their malicious need."*



Malware and stealers

Malware, including viruses, worms, and trojan horses, is software designed to cause damage to a computer, server, client, or computer network. It can enable control over systems (e.g., botnets), steal data, allow remote access (e.g., Remote Access Trojans), or install additional malicious software (e.g., downloaders), depending on the threat actor's goal.

Malicious actors create or access malware for cyber campaigns, evading defences and controlling assets. Unlike ransomware, malware is a distinct, persistent threat, with evolving tactics to challenge cybersecurity defences.

Another challenge for cybersecurity defences is the increased use of Living-of-the-Land Techniques, where actors use legitimate tools and functions of the infrastructure they are attacking, manipulating the functionality to fit their malicious need. Though not classified as malware, the attackers can misuse tools for malicious purposes, such as executing unauthorized commands, downloading malicious files, or evading security measures [7].

In the cyber kill chain, malware typically plays a crucial role in the "Delivery," "Exploitation," and "Installation" stages. During the delivery phase, malware is introduced to the target system, often through email attachments, malicious links, or other vectors. In the exploitation phase, it leverages vulnerabilities to execute its payload on the target.

The installation stage follows, where the malware is installed on the system to establish a foothold for further malicious activities. Depending on its capabilities, malware may also be involved in subsequent stages, such as "Command and Control" and "Actions on Objectives," enabling ongoing control and the achievement of threat actors' goals.

[7] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

Inside the systems

Sopra Steria detected and blocked several prominent malware threats targeting Sopra Steria clients in 2024.

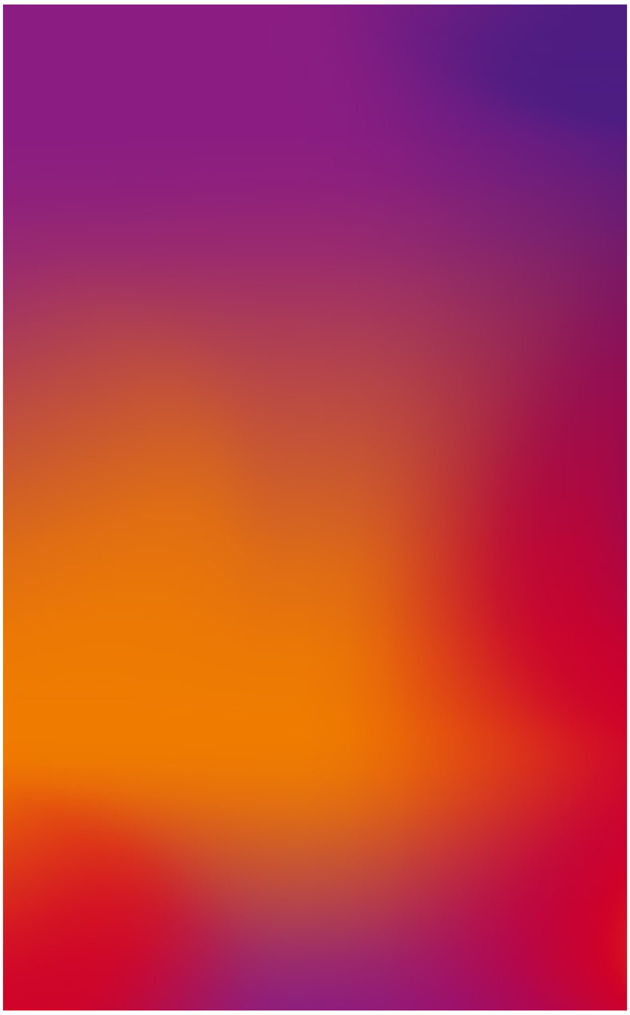
Malware are primarily associated with the Installation phase of the Cyber Kill Chain. Often engineered to secure an initial access point, facilitate the download of additional malicious tools, or grant threat actors' further access for subsequent breaches.

Malware cases occupied a relatively small amount of all true positive cases handled by our SOC. The highest amount was during the first half of 2024. On average, 10.1% of all TP cases handled by our SOC was malware related in 2024. This excludes malware instances that have been automatically blocked by antivirus.

Malware-as-a-Service (MaaS) is the business model where cybercriminals provide access to malicious software and related infrastructure for a fee, much like the legitimate service model Software-as-a-Service (SaaS). MaaS, such as the infostealers Vidar and Lumma Stealer, has been particularly exploited by financially motivated threat actor groups, who similarly deploy other variants of information stealers.

Info stealers pose a threat in the cybersecurity landscape, as threat actors commonly use them to harvest login credentials and sensitive information from compromised systems, which may lead to further breaches, financial fraud, or lateral movement within an organisation. Credentials are often sold on underground markets, and they play a crucial role in initial access operations often serving as the first step in multi-stage intrusions.

The rise in the use of stealers correlates with the increased activities of Initial Access Brokers (IABs), the expansion of distribution networks, and the growing sophistication of evasion techniques.



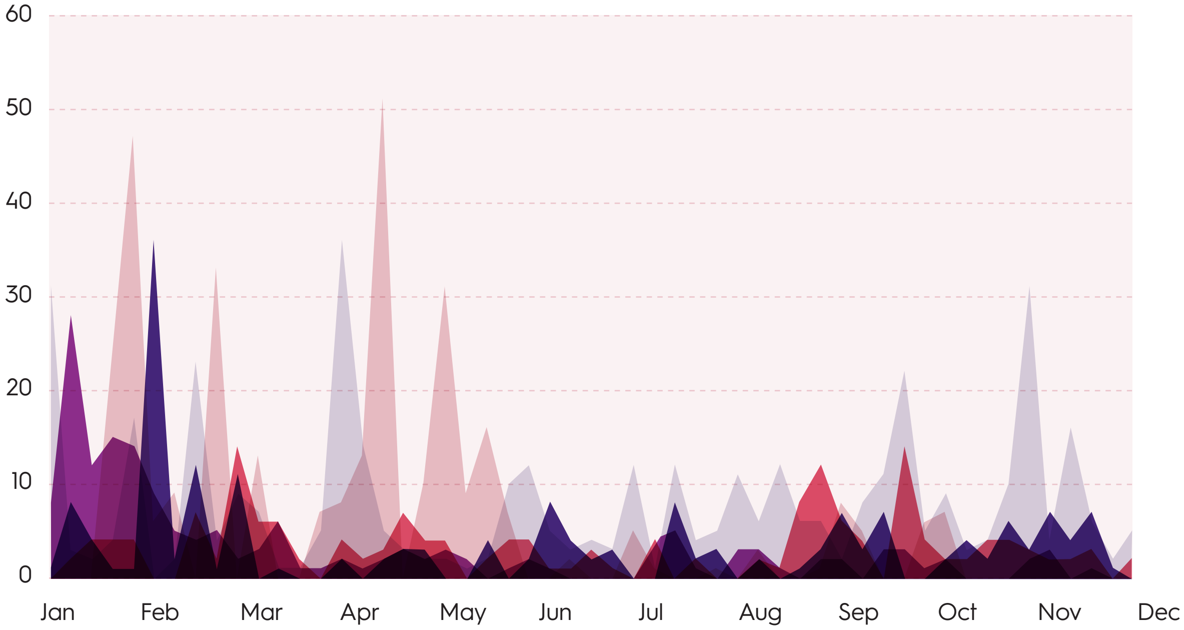
Observed and blocked

We have observed and blocked well-known commodity malware throughout 2024, with the malware types Bearfoos, MediaArena, Phonzy, Plasti and Wacatac (Microsoft naming) being the most prominent ones. These are the top five malware families observed last year :

Top 5 malware families

- Plasti
- Wacatac
- MediaArena
- Bearfoos
- Phonzy

Malware Families



Sopra Steria most observed malware throughout 2024 are all types of malware that pose significant threats to computer systems and share a lot of the same functionality. These malware families fall under the category of “commodity malware” and share very similar distribution methods.

Infection typically occurs through malicious email attachments, infected websites, downloading pirated software, or using infected USB drives.

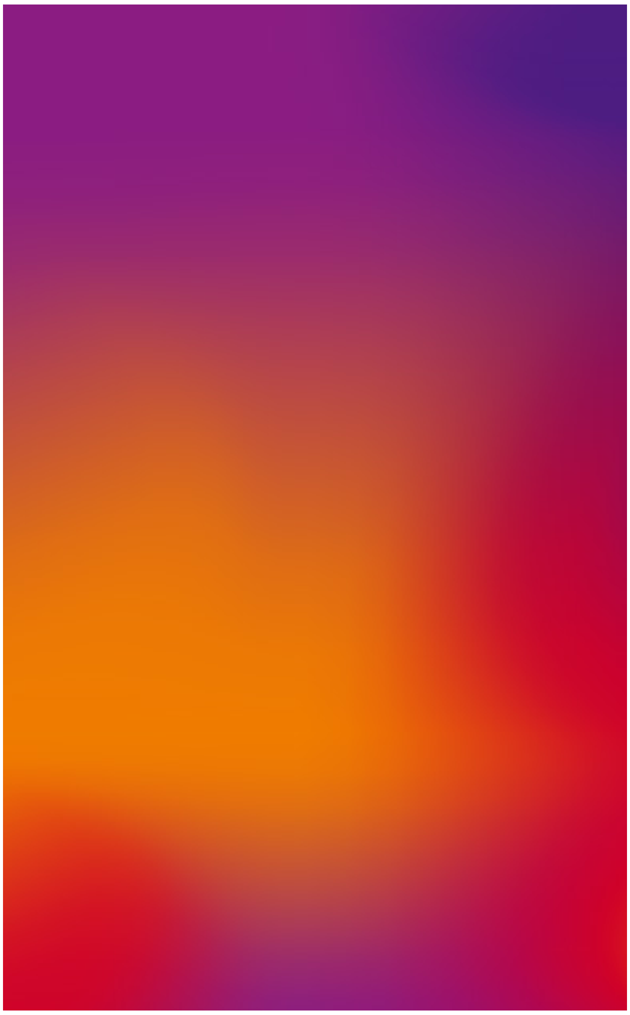
Commodity malware refers to malicious software that is readily available for purchase or download on the dark web or other illicit platforms. Unlike custom-built malware designed for specific targets, commodity malware is mass-produced and sold to a wide range of cybercriminals. This type of malware is often used in broad, opportunistic attacks rather than targeted campaigns.

Wacatac, also known as DeathRansom, began as a trojan and evolved into ransomware, encrypting files and demanding a ransom. It avoids infecting systems in Eastern European countries and is linked to Vidar malware. Similarly, Bearfoos is a trojan targeting Windows, executing commands to steal data, install malware, and provide remote access to attackers. This highlights the increasing sophistication of cyber threats.

In addition to trojans, MediaArena is a browser hijacker that changes your homepage and search engine, injects ads, and redirects searches. It can also open tabs with ads, push fake updates, and promote scams, complicating the digital threat landscape. Phonzy, known as Trojan :Script/Phonzy.A!ml, steals data, installs malware, and allows remote control by attackers. This underscores the need for robust cybersecurity measures. Similarly, Plasti, known as TROJ_PLASTI.A, performs harmful actions such as data theft, malware installation, and providing remote control to attackers.

Another type of malicious software Sopra Steria observe, and block, are hacktools, which is a program or utility designed to assist attackers with hacking. These tools come in a wide variety of applications and are commonly used to gain unauthorized access to a PC to insert worms, viruses and trojans.

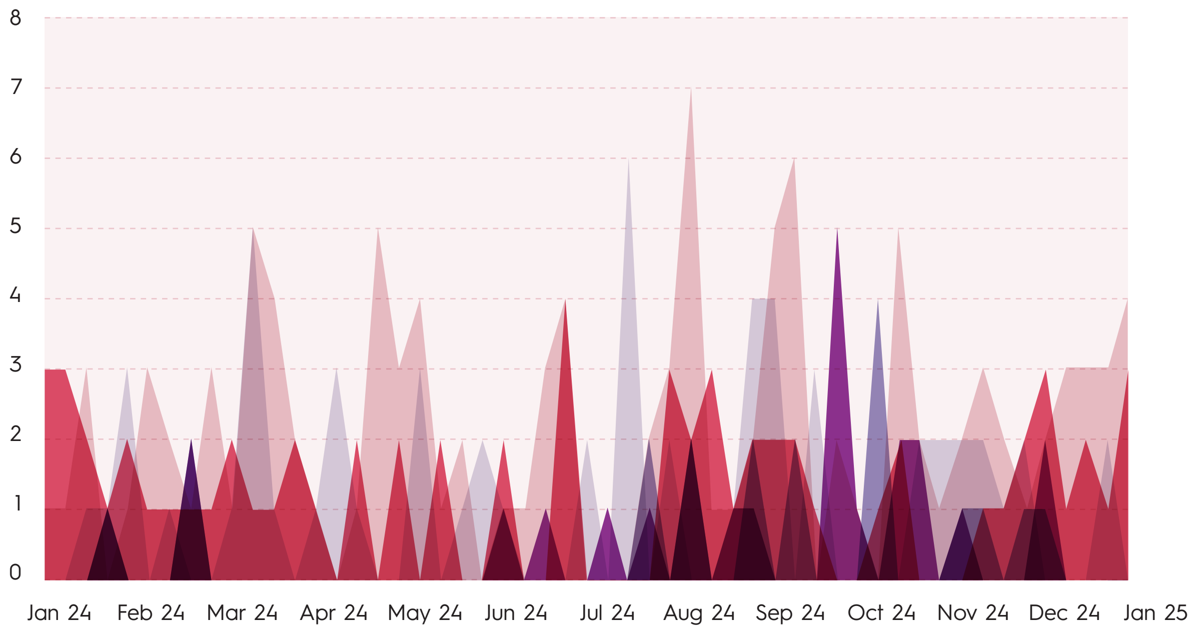
This section is based on Microsoft's definition of hacktools. Microsoft categorizes many cracking and license bypass software as hacktools, which are more prevalent than traditional hacking tools like Metasploit, Cobalt Strike, Brute Ratel, and Bloodhound. While we do encounter instances of these tools within Sopra Steria's customer base, they are not as common as the various types of cracking and license bypass software.



Top 5 Hacktool families

- AutoKMS
- Crack
- Keygen
- Patcher
- RemoteAdmin

Hacktool Families

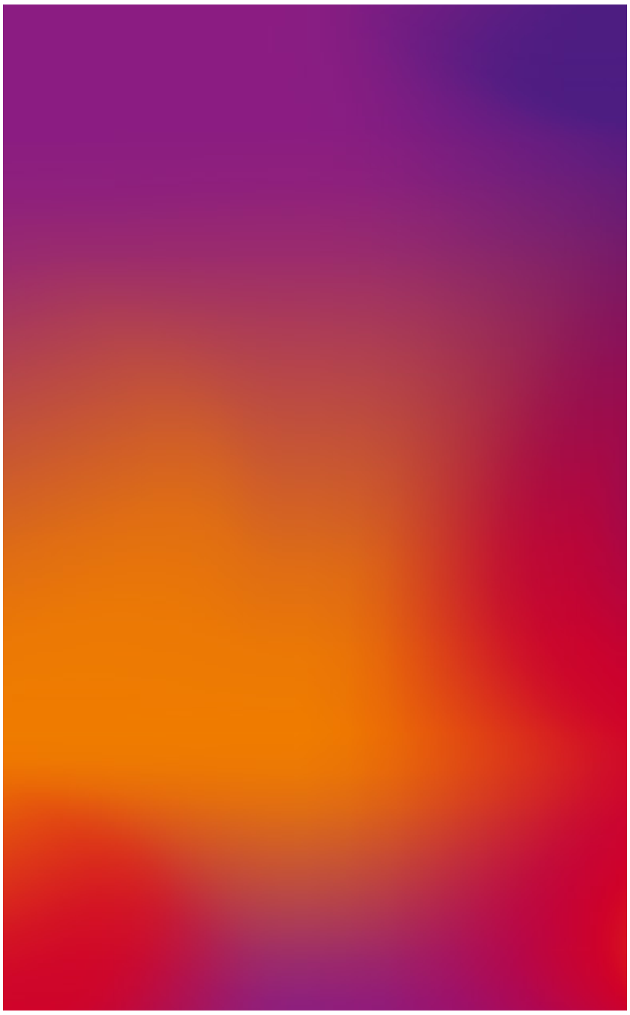


The most prominent ones observed by Sopra Steria are the hackTools AutoKMS, Crack, Keygen, Patcher, and RemoteAdmin. Most of these are tools designed to bypass software licensing mechanisms, posing risks to both system security and legality.

AutoKMS, Crack, and Keygen are hacktools used to illegally activate unregistered or pirated software by bypassing licensing mechanisms. Though not inherently malicious, they often come bundled with malware, creating security vulnerabilities. Patcher similarly modifies software to bypass licensing restrictions, posing risks such as malware association and security vulnerabilities. Using these tools violates software licensing agreements and copyright laws.

RemoteAdmin, on the other hand, is designed to provide remote access to a computer, allowing a user to control the system from a different location. While remote administration tools can be used for legitimate purposes, such as IT support and management, they can also be exploited by malicious actors to gain unauthorized access to systems. RemoteAdmin allows attackers to control a computer as if they were physically present, including accessing files, running programs, and managing system settings.

> — In the cyber kill chain, malware typically plays a crucial role in the “Delivery”, ”Exploitation” and “Installation” stages.



Repository poisoning

In 2024, the landscape of open-source malware expanded at an alarming rate, presenting challenges to the integrity of software supply chains. The year witnessed an increase in the identification of malicious packages according to OSINT reporting. Unlike accidental coding errors that lead to vulnerabilities, open-source malware is purposefully designed to infiltrate and exploit supply chains by masquerading as legitimate components.

During 2024 Shadow downloads have become a major concern as well. Shadow downloads occur when malicious packages bypass repository managers, directly entering a developer's machine or shared build infrastructure.

This process introduces unchecked dependencies into projects, undermining established security checks and increasing the risk of malware introduction.

This has inflated the risk significantly as security checks are frequently bypassed, leaving systems vulnerable to unvetted software. The sheer volume of these shadow downloads has skyrocketed, with numbers reaching billions monthly, thus highlighting a profound governance gap within software supply chains.

Open-source malware's stealthy nature and its ability to infiltrate through seemingly benign repositories make it particularly difficult to detect. The eco-systems that support these repositories, like npm, GitHub, and PyPI, have become hotspots due to their low entry barriers and lack of stringent author identity verifications.

This has allowed attackers to introduce various malicious components easily, exploiting dependency management gaps and build pipelines to spread their malicious code.

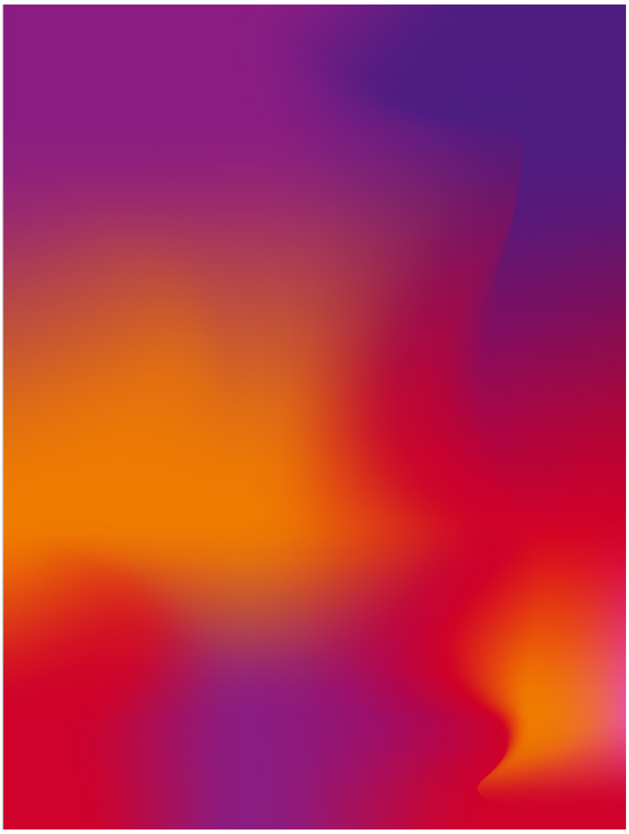
Organisations must implement stringent security measures to protect their software supply chains. This includes conducting thorough security reviews of open-source components, using automated tools to detect malicious packages, and maintaining a robust incident response plan to address potential threats.

Example

State actors have been observed using code repositories to target mainly developers to gain access, like the North Korean actor Moonstone Sleet distributing malware through npm repositories to exfiltrate sensitive data from cryptocurrency wallets.

Example

In March 2024, a backdoor was discovered in xz-utils, a suite of software that gives developers lossless compression. Malicious code added to xz Utils versions 5.6.0 and 5.6.1 modified the way the software functions. The backdoor manipulated sshd, the executable file used to make remote SSH connections. Anyone in possession of a predetermined encryption key could stash any code of their choice in an SSH login certificate, upload it, and execute it on the backdoored device. The XZ Utils backdoor incident sparked extensive discussions within the security community. One major concern was how the developer of the backdoor went undetected for so long, highlighting potential weaknesses in current security processes.



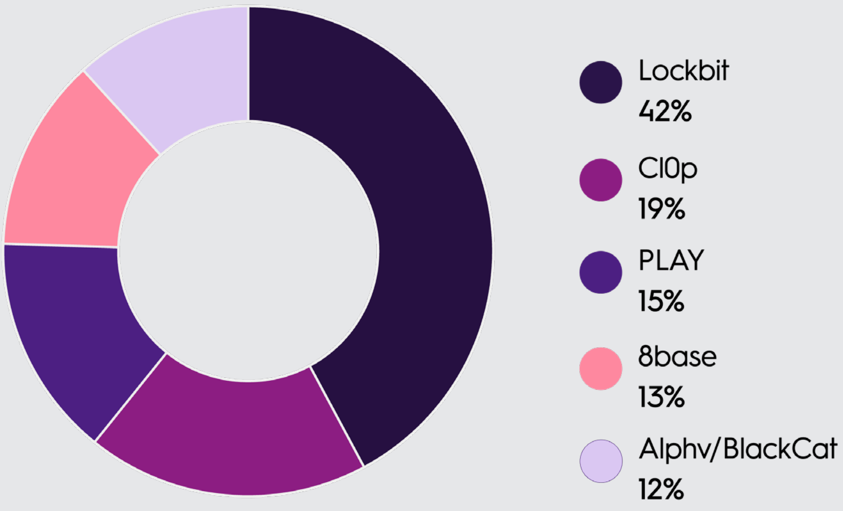
Ransomware ecosystem

The RaaS model continued to develop during 2024, allowing cybercriminals to delegate extortion operations to ransomware operators in exchange for a share of the profits or a payment. This approach has democratized ransomware attacks by providing ready-to-use tools to inexperienced affiliates.

RaaS operators develop and maintain the infrastructure while affiliates carry out the attacks. This model complicates the attribution of attacks and allows for increased resilience : the arrest of affiliates does not affect the operators, and affiliates can switch kits if necessary.

Threat actor groups exploiting this model include Lockbit, DarkSide, REvil, Dharma, and Akira. Attackers use a combination of native and downloaded tools to reach their end-goals, and they have a focus on data theft and exfiltration. Affiliate of one ransomware-group, Cactus, has been seen using a tool that automatically exfiltrates files to the cloud during a compromise, which later was displayed on their leak site. They then threatened to disclose more to exert pressure on their victim.

The five most active ransomware groups in 2024



Source : ENISA

04 Threat landscape

In 2024, the objectives of cyber threat actors, including both cybercriminals and state-sponsored groups, are rapidly evolving with notable changes in their tactics, techniques, and procedures (TTPs) as discussed earlier in this report.

The shifting threat landscape poses considerable challenges as cyber-criminals become more sophisticated and effective, largely due to reduced barriers to entry. Their primary aim is unauthorized access to sensitive information and systems, often for financial gain, and they utilize various advanced attack techniques to achieve this.

With the ongoing digital transformation, cybercriminals have adapted by increasingly targeting network infrastructures, cloud storage services, and Software as a Service (SaaS) platforms. They exploit a variety of vulnerabilities, including inadequate patch management, misconfigurations, unsecured APIs, and outdated software. There's a rising trend of malicious software packages designed to infiltrate and exploit supply chains by posing as legitimate components.

Additionally, the hacktivism scene is heavily influenced by geopolitical conflicts, particularly those related to Gaza, Israel-Iran, and Ukraine. State-sponsored actors are key contributors to the threat landscape, utilizing substantial resources for espionage and intellectual property theft.

They engage in comprehensive reconnaissance to prepare for, and sometimes disrupt, critical infrastructure, underscoring the complexity and severity of these threats. Notable actors like the Chinese state-sponsored group Volt Typhoon have infiltrated IT networks in the U.S., with potential intentions to disrupt critical infrastructure. Similarly, Salt Typhoon has breached telecommunication companies in several countries. This was likely done to gain large-scale access to telephone traffic data in the form of Call Detail Records and possibly also traffic content from a larger set of telephone calls. Both types of information can for the attacker, carry high value for further exploitation.

Their unconventional methods underscore a heightened threat environment, exhibiting compromised environments across key sectors such as telecom and energy.

Volatility of ransomware groups

In 2024, several ransomware groups have been both created and dissolved. This may not be specific to 2024, but we saw significant changes caused by judicial actions involving multiple countries, such as the operation in February against the LockBit group, thanks to an unpatched PHP vulnerability on their site. Although it did not eliminate LockBit, it significantly reduced their threat level. As a result of the operation, encryption keys were dissolved and provided to its victims, showing how international efforts and coordination makes a difference.

However, the disappearance of a ransomware group does not necessarily imply a decrease in overall ransomware activity. Indeed, groups may change names over time, but many of the actors involved often remain the same. For example, the RansomHub operation, active since early 2024, has attracted an influx of affiliates who abandoned LockBit (and BlackCat) operations.

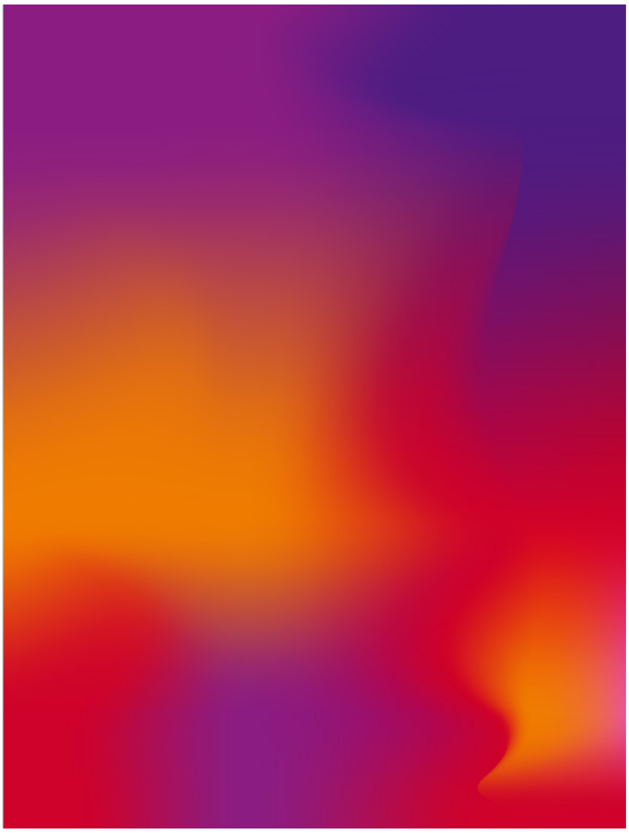
Key observations

> *"The proliferation of data stealers has led to an increase in data leakage incidents, often facilitated by the use of stolen credentials."*

The proliferation of data stealers has led to an increase in data leakage incidents, often facilitated by the use of stolen credentials. Cybercriminals frequently use malicious infrastructures and public cloud services to host malware and exfiltrate data. Meanwhile, ransomware and destructive campaigns remain dominant, with operators utilizing Ransomware-as-a-Service (RaaS) models to expand their attack capabilities and target a broader array of victims. These actors not only encrypt and steal data but also use the threat of public exposure to extort payments, often leveraging cloud storage for data transfers. Moreover, sophisticated ransomware groups are increasingly used by state actors to obtain insights into other nations' data, critical infrastructure, or other valuable information.

Observations indicate a higher level of sophistication in exfiltration methods to bypass security measures. In response to the cybersecurity industry developing detection methods specifically to defend against the latent threat posed by infostealers, cybercriminals are attempting to evade detection by innovating with archiving tools or alternative exfiltration protocols. There has also been an increase in the use of exfiltration techniques, such as exfiltration to cloud storage and the use of encrypted channels. This reflects attackers' adaptation to the growing use of cloud solutions for data exfiltration, while securing their communications.

Furthermore, this cloud-based exfiltration method aims to "blend into the noise" of data traffic, considering that many companies store their data in third-party clouds. Tools such as Cobalt Strike, Mimikatz, PsExec, RClone and PowerShell remain heavily used by attackers, highlighting both their effectiveness and versatility in attacks, whether for lateral movement, exfiltration, or the collection of sensitive data. This underscores the critical need for dedicated detection rules to identify both widely spread hack tools and the malicious use of legitimate tools.



Artificial intelligence

In 2024, we saw remarkable progress within AI, particularly in the field of Generative AI, with new and more powerful models made available almost on a weekly basis, showing significant improvements in quality, accuracy and how much information they could process. Many models also introduced full multimodality where input and output were no longer limited to just text but also images/audio/video giving the models the ability to see and listen. While the market is still largely dominated by OpenAI, Microsoft, Google, Meta, and Amazon, there is also a rise of open-source and 3. party models from smaller companies that also rival the bigger models. New capabilities have also been made available that allow us to run the models on our own local hardware as well, which gives us the ability to run image/video/audio/text processing within our own infrastructure or at the edge.

This year, many organisations started to use Generative AI for application development (GitHub Copilot) and collaboration (Microsoft 365 Copilot), and more are in the early phases of evaluating the use of GenAI for business automation. A risk many companies have faced this year is Shadow GenAI, where employees started to use one of many thousand GenAI tools and services in the market with corporate data, and not knowing how the different services process the data. This lack of visibility and control creates potential security vulnerabilities, compliance issues, and the possibility of sensitive data leaks.

There has also been an increase of cybercriminals and even state threat actors using Generative AI for

• Generating deepfake content with the intent to conduct social engineering attacks or to manipulate public opinion through false information, particularly in relation to political matters or ongoing international conflicts.

• New methods of social engineering using Generative AI to replicate a person's voice or face. Improvements made to the models and hardware have now also made it possible to generate real-time deepfake video even over Microsoft Teams calls.

• Generating new malicious code such as new malware, viruses or trojans. While the quality of GenAI generated malware is currently quite low, we expect with all the improvements in the models this will become a bigger risk in the upcoming years.

Fortunately, many of the AI vendors have added more safeguards in their models to prohibit this type of abuse, and we are now seeing is that cybercriminals are now finding new methods to bypass these safeguards using a technique called prompt injection.

"A risk many companies have faced this year is Shadow GenAI, where employees started to use one of many thousand GenAI tools and services in the market with corporate data, and not knowing how the different services process the data."

Another trend that emerged is the use of virtual agents, where one can combine generative AI with a virtual agent that has a set of predefined integrations and a set of instructions. These agents can take on a variety of tasks, like gathering information or doing reconnaissance with tools like AutoGPT, Autogen, or MetaGPT.

They can also handle automated security testing using frameworks like PentestGPT. These agent frameworks are now becoming so powerful that they can be used to do automated attacks and can even interact locally with computers using features such as Anthropic Compute Use APIs or run in a virtualized environment.

While we do not see any AI Cyber-attacks becoming the norm anytime soon, we notice that cybercriminals are using GenAI to aid them. AI is likely to assist with malware and exploit development, vulnerability research and lateral movement by making existing techniques more efficient. However, in the short term, these areas will continue to rely on human expertise.

AI will also lower the barrier for novice cyber criminals, and hacktivists to carry out access and information gathering operations.

Generative AI will become an even more important topic in the upcoming years with more and more businesses looking to take advantage of the technology in multiple areas within the business.

05 Recommendations for defenders

Organisations should take a comprehensive approach to security, integrating resilience into their core operations to better manage the rapidly changing digital landscape. It is important to adopt threat-based testing and improve incident response. Security efforts should be dynamic, adapting to the evolving threat landscape.

Many of the cybercrime trends reported on globally in 2024 reflects Sopra Steria observations and incidents. Phishing, with its new methods, constitutes the largest category of security incidents handled by our Security Operation Center in 2024. EDR tools coverage is crucial for detecting and responding to malicious activity. We recommend all organisations to adhere to the NSM core principles for ICT-Security. Organisations that have developed a higher level of security maturity, which include good patch policy, asset inventory and control over exposed access points have an easier time protecting their infrastructure and fewer security incidents.

Phishing

Defending against phishing requires a multi-layered approach to effectively protect against these deceptive attacks.

Multi-factor authentication (MFA) for all user accounts is a necessity, with the increase of AiTM phishing, phishing resistant MFA should be chosen.

Regularly educate employees on how to recognize and report phishing attempts, as human vigilance is a crucial line of defence. Utilize advanced anti-phishing tools and services that can monitor, block, and filter phishing attempts in real-time, reducing the chances of malicious emails reaching your inbox.

- Enable Strong Multi-Factor Authentication (MFA) : Implement MFA for all user accounts to protect against advanced phishing techniques. Ideally, phishing-resistant MFA should be used.
- User Awareness Training : Regularly educate employees on identifying and reporting phishing attempts.
- Anti-Phishing Tools and Services : Utilize tools that monitor, block, and filter phishing attempts in real-time.

Authentication methods

Method	AiTM Protection
Passwordless phone sign-in	X
Phone number + SMS	X
Username and password	X
Microsoft Authentication App + Number matching	X
FiDO 2	V
Certificate-Based Authentication	V
Conditional Access (Compliant Device)	V
Conditional Access Trusted Locations	V
Require device to be marked as Hybrid Azure AD joined device	V

Vulnerabilities

Organisations should prioritize securing their APIs by implementing strong authentication and authorization mechanisms, regular security testing, and continuous monitoring, while ensuring proper configuration and validation to mitigate associated risks.

Additionally, upgrading VPN solutions to more secure alternatives and enforcing multi-factor authentication is crucial to control and secure all exposed access points, ensuring only authorized access. Regularly updating and patching VPN software, combined with strong authentication mechanisms, can significantly reduce risks. Furthermore, organisations must prioritize regular patching and updates across all aspects of their infrastructure, including network devices, virtualization systems, and standalone applications. Given the decreasing time-to-exploit trends[8], with adversaries now able to exploit vulnerabilities within an average of just five days, timely patching is more critical than ever.

- Regular Patching and Updates : Prioritize regular patching and updates to mitigate risks associated with vulnerabilities.

- Secure APIs and Streaming Technologies : Implement strong authentication and authorization mechanisms, regular security testing, and continuous monitoring.

Malware

Defending against malware requires a combination of preventive measures and monitoring. Ensure that antivirus software is installed on all devices and kept up to date to detect and remove malicious software. Implement network monitoring tools to detect unusual activity that may indicate the presence of malware.

Educate employees about the risks of downloading and opening suspicious files or clicking on unknown links, as these are common methods for malware distribution. Additionally, employ endpoint detection and response (EDR) solutions to monitor endpoint activities and quickly respond to potential threats.

- Device Insight and Real-Time Threat Intelligence : Monitor network traffic with advanced analytics and stay informed about emerging threats.

- Install and Update Antivirus Software : Ensure antivirus software is installed and regularly updated.

- Strengthen Data Exfiltration Detection : Implement dedicated detection rules for widely spread hack tools and the malicious use of legitimate tools.

[8] https://socradar.io/top-10-exploited-vulnerabilities-of-2024/

Pen-tester perspective

Over the past year, the penetration testing team has identified several recurring vulnerabilities and weaknesses among clients. Many of these reflect fundamental issues that have persisted over the years and remain as relevant today as ever.

These vulnerabilities continue to provide attackers with opportunities to escalate privileges and achieve significant impact, highlighting the importance of addressing them effectively.

Key Findings from Penetration Testing

Poor Password Hygiene : Poor password hygiene remains something we frequently exploit to gain domain access. Through password spraying attacks using simple and predictable passwords, we often achieve unauthorized access to user, service, and administrative accounts.

Sensitive Files in File Shares : We often discover configuration files containing plaintext connection strings and tokens, as well as passwords and other sensitive data in file shares. This provides attackers with straightforward opportunities for horizontal escalation and exposure of critical information. The lack of proper access controls and logging further exacerbates this issue.

Vulnerable Certificate Templates : Misconfigured certificate templates are a recurring issue, enabling privilege escalation. This includes instances where regular domain users have been able to gain domain administrator rights due to improper settings in the certificate templates.

Misconfigurations : Misconfigurations remain a common problem, with examples including :

- Weak configurations in cloud platforms, leading to unintended access to sensitive data or resources.

- Poorly implemented network segmentation, making it easy for attackers to move laterally within an environment.

Authorization Issues and Cross-Site Scripting in Web Applications : We frequently encounter missing or weak authorization implementations in APIs and web applications. These vulnerabilities have resulted in unauthorized access to sensitive data and systems, as well as the ability to perform unauthorized actions. In some cases, this has allowed us to escalate privileges vertically (gaining higher-level permissions) or horizontally (accessing other users' data).

Additionally, we often identify cross-site scripting (XSS) vulnerabilities in web applications. These flaws allow us to inject malicious scripts, potentially compromising user sessions, defacing websites, or stealing sensitive data.

> — Poor password hygiene remains something we frequently exploit to gain domain access.

Recommendations for Improved Security

Strengthen Password Practices :

nforce robust password policies and mandatory MFA for all critical systems. Block the use of simple, commonly used passwords.

Review Access Permissions :

Regularly audit shared file areas and ensure sensitive information is not stored without adequate protections.

Harden Configurations :

Review and update configurations, including certificate templates, to align with best practices.

Test Authorization Mechanisms :

Conduct regular testing of web applications to ensure authorization is correctly implemented and no sensitive data can be accessed without valid permissions.

Outlook 2025

In 2025, the use of AI in cyber-attacks is highly likely to become even more sophisticated and widespread.

Cybercriminals will increasingly leverage AI to create highly convincing phishing emails and social engineering attacks, mimicking human behaviour and language patterns with greater accuracy, making them harder to detect. Deepfake technology will also be utilized by many threat actors to create realistic videos and audio recordings for identity theft, fraud, and bypassing security measures, enabling attackers to impersonate individuals and gain unauthorized access to sensitive information.

Moreover, information operations will see AI being leveraged to scale content creation, producing more persuasive and fake personas. This will enhance the ability of threat actors to influence public opinion and conduct disinformation campaigns. Overall, the integration of AI in cyber-attacks will make them more scalable, sophisticated, and difficult to defend against. Organizations will need to invest in advanced security measures and continuous monitoring to stay ahead of these evolving threats.

In parallel, the value placed on stolen credentials by threat actors will remain high, driven by several key trends observed in 2024. Throughout 2024, there was a significant increase in the use of legitimate credentials for initial access in cyber-attacks. The market for compromised credentials, often acquired through information-stealing malware, continued to thrive. Attackers recognized that even a single employee credential, which could be obtained for as little as $10, could lead to high-profile compromises. This trend is highly likely to persist into 2025, as the demand for such credentials remains strong due to their effectiveness in gaining unauthorized access to systems. Organizations will need to prioritize credential security, including robust authentication methods and continuous monitoring, to mitigate the risks associated with credential theft.

As cybercriminal groups continue to specialize, this trend is likely to persist or even intensify in 2025 to meet the evolving demands of the cybercrime market. We will likely see groups solely dedicated to one narrowly specified area like exfiltration or cloud infrastructure exploitation. Additionally, collaborations between these groups could become more frequent, with temporary alliances formed for specific campaigns or resource sharing, such as vulnerabilities and infrastructures.

State-aligned Advanced Persistent Threat (APT) groups are increasingly collaborating with cybercriminals, particularly in the use of ransomware, initial access brokers, and destructive attacks. This collaboration blurs the line between cybercrime and state-sponsored attacks, significantly impacting attribution of attacks and security management overall.

Furthermore, the EU's recently approved NIS 2 directive aims to significantly enhance collaboration between EU member states in combating cybercrime. Besides contributing to enhanced protection of systems, this will likely impact the preventative and operational efforts of law enforcement, intelligence agencies, and various Computer Security Incident Response Teams (CSIRTs) across different countries. The directive promotes increased and standardized reporting, improved information sharing, enhanced cooperation mechanisms, and a more harmonized legal framework.

Probability matrix

Highly Unlikely	<10 %
Unlikely	10–40 %
Even chance	40–60 %
Likely	60–90 %
Highly Likely	>90 %

> — State-aligned Advanced Persistent Threat (APT) groups are increasingly collaborating with cyber-criminals, particularly in the use of ransomware, initial access brokers, and destructive attacks.

How can Sopra Steria help you

Given our observations throughout 2024, there is much to address to gain acceptable security. The threat in the cyber domain is growing, and the pace is increasing. At Sopra Steria, we have over 300 experts who can help your business reduce the likelihood of a successful cyberattack by systematically reducing risk and measurably increasing security maturity.

If you "only address three things" in 2025 for maximum security impact, you should focus on these three areas :

Better Handling of Phishing

- Train and raise awareness among employees on phishing through email, chat and phone.
- Implement anti-phishing tools that instantly help employees assess the risk of emails.
- Establish reporting and alerting routines so employees can alert about potential security risks or behavior.

Understand the Threat Landscape

- Ensure that the business has an updated understanding of the threat landscape for your business.
- Know which of your business-critical assets and information that is valuable to an attacker.
- Understand how artificial intelligence and new regulations affects the landscape.

Reduction of Attack Surface

- Fix vulnerabilities, focusing on known exploited or those exposed to the Internet.
- Measure the quality of IT systems against known frameworks and set clear compliance requirements.
- Use phishing-resistant multi-factor authentication (MFA).

In security work, there will always be a battle where threat actors quickly and opportunistically exploit an ever-increasing digital space of opportunities. It can be difficult to navigate and know where to focus security efforts.

- How do you set up a project that will better protect us against phishing?
- How do you systematically reduce the attack surface?

Such questions often arise when we are flooded daily with cyber threats and new technologies. At Sopra Steria, we can help your business with maturity assessments, security tests, security enhancements, security monitoring, response capacity, strategy work, target image work, compliance, and most things in between. Our customers deliver critical services to the society, and we work 24/7 to assist in securing them and their critical societal functions. We want to help, and we can help.

Jorgen Rorvik

Director of Cybersecurity
Sopra Steria Nordics

jorgen.rorvik@soprasteria.com