Security Operations Center

Sopra Steria State of Security **2024**

sopra steria

CONTENTS

The Cyber Kill Chain

ABOUT
SOPRA STERIA

Sopra Steria in Norway is Scandinavia's leading digital transformation and managed services provider and delivers managed services to enterprise customers in the global market.

Sopra Steria deliver managed services for Private and Public Cloud, Security, End-user and Service Management, in multiple verticals including critical national infrastructure as well as public services. Sopra Steria Security Operations Center (SOC) in Norway supports customers to reduce risk of data exfiltration, service disruption or regulatory non-compliance through managed security services.

EXECUTIVE SUMMARY

Sopra Steria Scandinavia is consistently adapting to the evolving cybersecurity landscape, and this year`s report presents the dynamics and observations of cyber threats in 2023, observed in the different stages of the Cyber Kill Chain framework.

The evolving threat landscape presents increasing challenges for organizations, characterized by greater sophistication, professionalism, and effectiveness among malicious actors, along with lower barriers to entry. From Sopra Steria Scandinavia SOC observations, credential theft has become a favored approach among cybercriminals due to its potential profitability. Evolving trends reveal a shift toward the use of more advanced phishing techniques, expansion of attack surface, and complexities in attack patterns and strategies. The development of artificial intelligence (AI) has enabled advanced types of cyber-attacks including AI-powered phishing, deepfake attacks, and AI-driven malware.

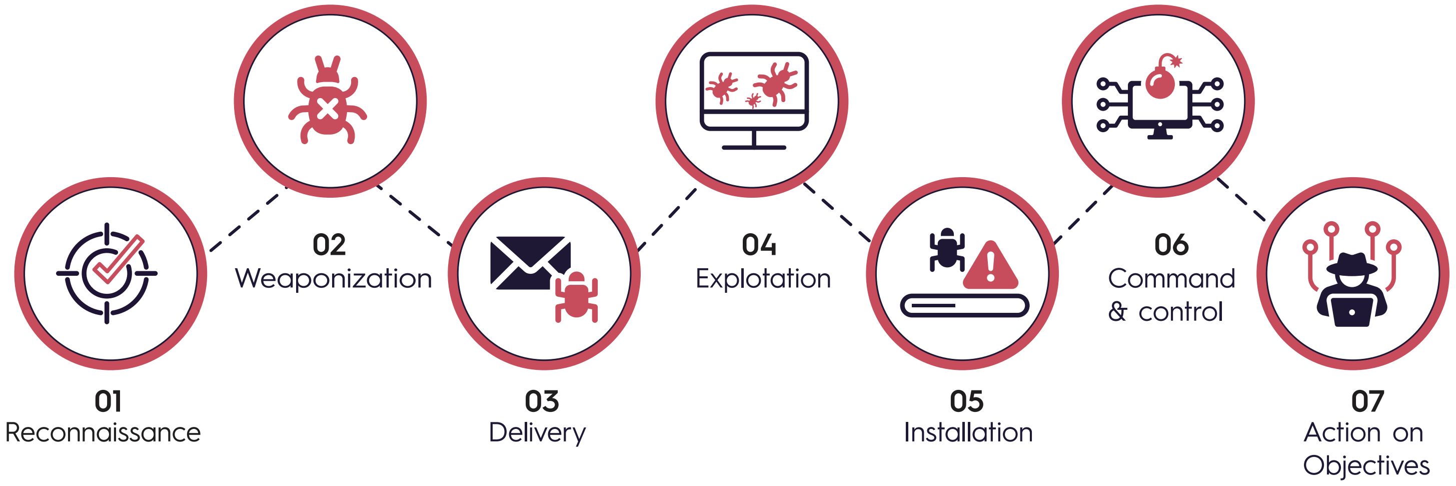
Supply chain attacks have become more sophisticated, emphasizing risks within open-source ecosystems. Stealer evolution has increased data leakage incidents, with stolen enterprise credentials fuelling unauthorized access. Cyber threats leverage platforms like Telegram and Discord for command and control, complicating detection efforts. Malicious infrastructures (including ransomware and loaders) frequently resurface shortly after takedowns. Moreover, the use of public clouds for hosting malware and data exfiltration has become increasingly prevalent in 2023.

In 2024, the cyber landscape is expected to face challenges through evolving geopolitical tensions, financial uncertainties, misinformation campaigns, and AI advancements. AI is anticipated to fuel the development of more advanced cyber-attacks, including advanced malware and zero-day exploits, leading to a surge in successful breaches. Additionally, amidst a hostile global geopolitical environment, state-sponsored cyberattacks and disinformation campaigns may escalate, adding further complexity to cybersecurity efforts for Sopra Steria Scandinavia as well as our customers.

THE CYBER **KILL CHAIN**

In this Year in Review report, we have chosen to utilize the Cyber Kill Chain framework to present the cybersecurity events and trends observed during 2023. The Cyber Kill Chain offers a structured and systematic approach to understanding the various stages of a cyber-attack, allowing us to break down incidents, identify patterns, and highlight key areas for improvement. By aligning our insights with the Cyber Kill Chain model, we aim to provide a detailed and strategic overview of the threat landscape, enabling a proactive and informed approach to cybersecurity defence.

The Cyber Kill Chain is a framework that describes the stages of a cyber-attack from initial reconnaissance to the final action on objectives. It was originally developed by Lockheed Martin and has since become a widely used model for understanding and analyzing the different phases of a cyber-attack.



1. RECONNAISSANCE

The first step of the Cyber Kill Chain is the reconnaissance and precursors phase. This phase includes the upfront work and preparation to execute an intrusion, and may include steps such as tasking, acquisition of tools and infrastructure, identification of targets, and organizational research.

A massive database built from previous breaches, leaks, and private databases across a wide range of business and consumer sites from Twitter and LinkedIn to Adobe and Dropbox has been released by an unknown source. This breach is composed of approximately 26 billion records and is being referred to as the "mother of all breaches".

Credential harvesting

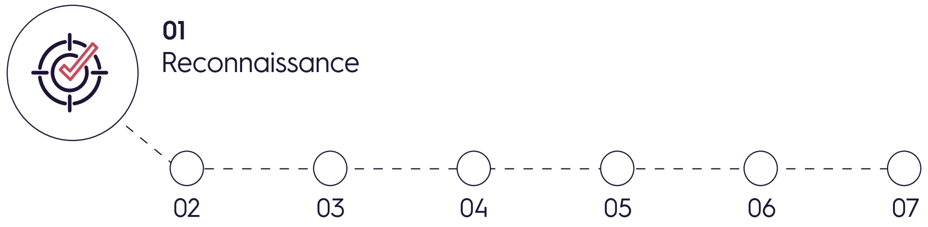
Criminal groups have emerged through 2023 with credential harvesting and distribution as their main business model. The frequency usage of stolen credentials is higher than previous years, and in addition to Sopra Steria Scandinavia SOC observations, this trend has been reported by other security vendors, such as Crowdstrike and Microsoft amongst others.

The increasing prevalence of data breaches over several years is a concerning trend that shows no signs of deceleration. Recent years have been marked by numerous thefts involving sensitive data. Large data collections which contain hundreds of thousands of stolen credentials are accessible for purchase, their cost being relatively low compared to the potential gains from a successful ransomware or Business Email Compromise (BEC) attack. These data lists are particularly beneficial to less advanced attackers who lack the skills to directly hack IT systems.

With new methods being implemented in phishing, information stealers, API exploitation and more, the value of valid credentials from malicious actors is increasing. This becomes evident when observing darknet marketplaces where credentials are sold in large quantities.

Scanning

The Reconnaissance phase is becoming increasingly efficient, speeding up the overall time for a successful cyber-attack. One trend is the prevalent use of zero-day vulnerabilities. These security flaws (often exploited before patches become available) significantly contribute to a decrease in the average time to exploit (TTE).
An observed trend in the cybersecurity landscape is a diversification of targeted technologies. While traditional technologies such as firewalls, operating systems, and access points remain prominent for exploits, a more diverse set of technologies are being scanned for malicious purposes. This indicates an expanding attack surface where threat actors demonstrate more complex attack patterns and strategies.



2. WEAPONIZATION

The attacker moves on to this phase once the reconnaissance is finished, and they will decide the best type of weapons they have at their disposal to carry out their attack on the target. One weapon could be to create a malicious payload designed to exploit the vulnerabilities identified in the reconnaissance stage. This can involve crafting phishing emails, creating malware, or building exploit tools. Another type of weaponization is to use methods such as DDoS- or botnet attacks.

Artificial intelligence

Throughout 2023, the cyber threat landscape witnessed significant adaptations of artificial intelligence (AI) by threat actors. New AI technologies have paved the way for a new era of cybersecurity threats characterized by ever more intricate and targeted cyberattacks. Notable AI-powered threats included advanced phishing, adversarial attacks, AI-generated malware, deepfake attacks, automated exploitation of vulnerabilities, credential stuffing, and automated botnets.

One of the most significant threats posed by AI in 2023 was advanced phishing attacks. Malicious actors can use AI to create highly personalized and convincing phishing emails or messages by analysing and emulating a target´s individual or organizational writing styles and behaviour patterns. Malicious emails might be challenging to differentiate from authentic communications, increasing the likelihood of success in tricking victims into disclosing sensitive information or downloading malware. AI can analyse vast amounts of data from various sources, including social media, to craft personalized and convincing phishing emails and social engineering attempts.

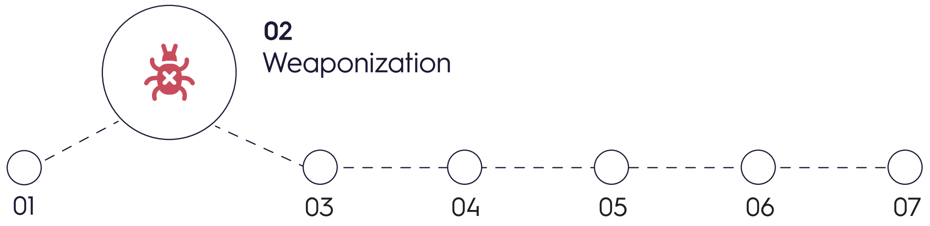
AI allows attackers to automate various stages of the attack process, such as reconnaissance, targeting, and exploitation. AI-powered attacks can potentially adapt in real-time to changes in the target environment, making them more difficult to detect and counter.

Another significant threat is the use of AI-driven deepfake technology, which can create highly realistic audio or video impersonations of individuals. This capability has already been exploited for various malicious purposes including spreading disinformation, conducting social engineering attacks, or with intent to cause reputational damage to an individual or organization.

DDoS

In 2023, there was a significant rise in Distributed Denial of Service (DDoS) attacks. The number and scale of DDoS attacks in Europe now rival those in North America. There is a marked shift, driven by pro-Russian hacktivist groups announcing massive and coordinated DDoS attacks on both European and U.S. organizations. These attacks have become more frequent, longer, and more sophisticated, with multiple vectors targeting multiple IP destinations in the same event.

Since the Russian invasion of Ukraine, pro-Russian hacktivist groups such as Killnet, NoName057(16), and Anonymous Sudan have been launching DDoS campaigns against countries supporting Ukraine's defence. Norway has been repeatedly targeted with attacks on organizations such as NSM, SSB, PST, Schibsted, Amedia, and various municipalities including Stortinget. Despite the persistent threat, impact on Norway has been relatively minimal, causing short downtimes or slow services for just a few hours.



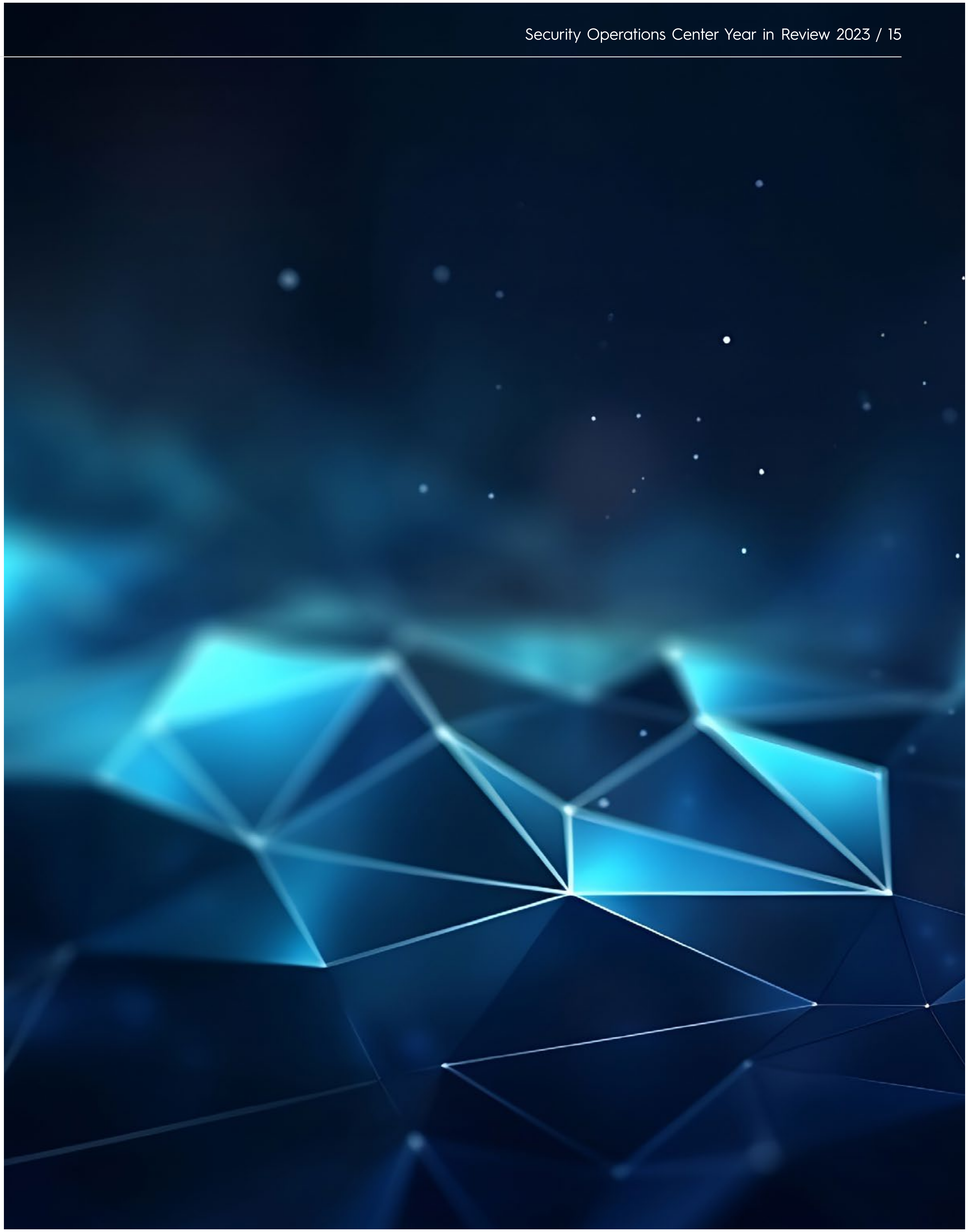
Software Supply chain

In general, the evolution of supply chain attacks in 2023 showed a trend towards more complex and highly targeted attacks, as well as increased sophistication in threat tactics and further targeting of specific organizations. Attackers used automation and obfuscation to stay ahead of defences and recognised the potential of the open-source ecosystem as an entry point to broader systems.

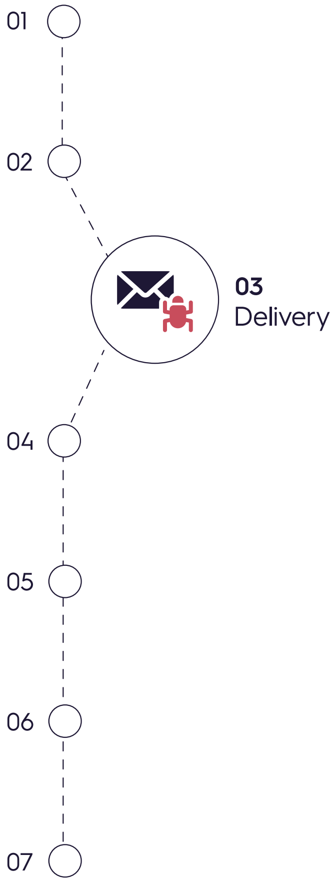
In the first half of 2023, the main threat observed was the proliferation of packages within various open-source ecosystems aiming to distribute malware. Some of these packages were essentially spam, but their sheer volume made it difficult for organizations to effectively identify and remove legitimate malware threats. The spam packages affected the ability of open-source ecosystems to triage and eradicate serious malware threats, thereby prolonging the time malicious packages are active and potentially infecting systems.

As the year progressed, we saw an escalation in the sophistication and specificity of attacks, with a surge in packages that targeted particular groups or organisations. Malware attacks were no longer just broad-brush efforts, but rather more tailored operations. Intruders became better at hiding their malicious activity through tactics such as code obfuscation, making their detection even more difficult.

The open-source ecosystem was also exposed to nation-state activity. Particularly notable was the rise of such activities linked to North Korea. These were usually sophisticated, multi-stage attacks, executed by scripts on the developer's workstations, often resulting in intellectual property theft.



3. DELIVERY



This stage involves delivering the harmful payload to the victim. Delivery methods could include email attachments, websites, USB drives, or physical access to the target's environment. At this point, the attacker tries to convince users to activate the payload, often through deceptive tactics.

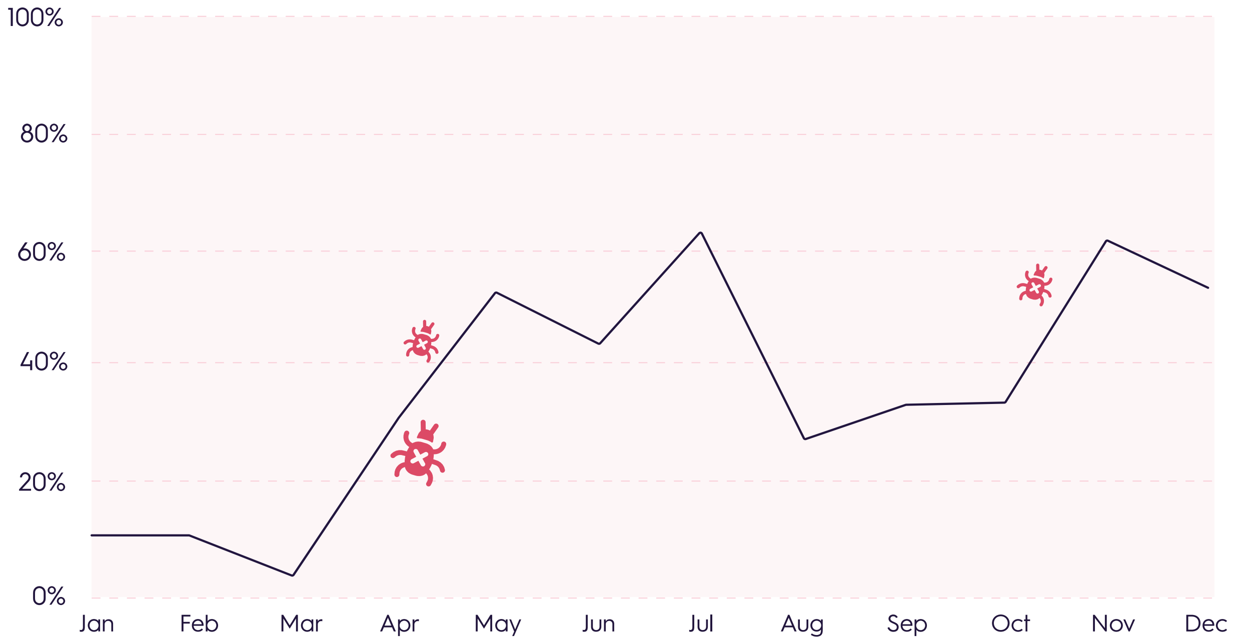


Figure 1: Percentage of phishing amongst all true positive incidents

Phishing-as-a-Service

Phishing attacks are on the rise, with a notable shift in techniques observed in 2023. Threat actors are gravitating towards user-friendly, automated platforms with low entry costs while advancing their methods. Some are abandoning traditional email services for other communication tools used by target organizations. The surge in Phishing-as-a-Service (PhaaS) on the dark web poses new cybersecurity threats, employing tactics such as Adversary-in-the-Middle (AiTM) attacks and Teams-phishing, impacting all sectors. Users can purchase phishing kits for as low as $40, enabling easy deployment of attacks. PhaaS services are often advertised on Telegram channels and on darknet forums and attract notable levels of interest.

Adversary-in-the-middle

Adversary-in-the-Middle (AiTM) attacks, evolving from phishing emails, intercept and manipulate network communications. These attacks have become complex, using proxy servers to steal session cookies and control user sessions. Sopra Steria Scandinavia SOC phishing statistics show increased AiTM attacks, mainly cloud-based platforms like EvilProxy.

The data show that a proportion of phishing attacks are utilizing AiTM, and that organizations hit with more phishing will consequently experience more AiTM attacks. This aligns with general global security trends.

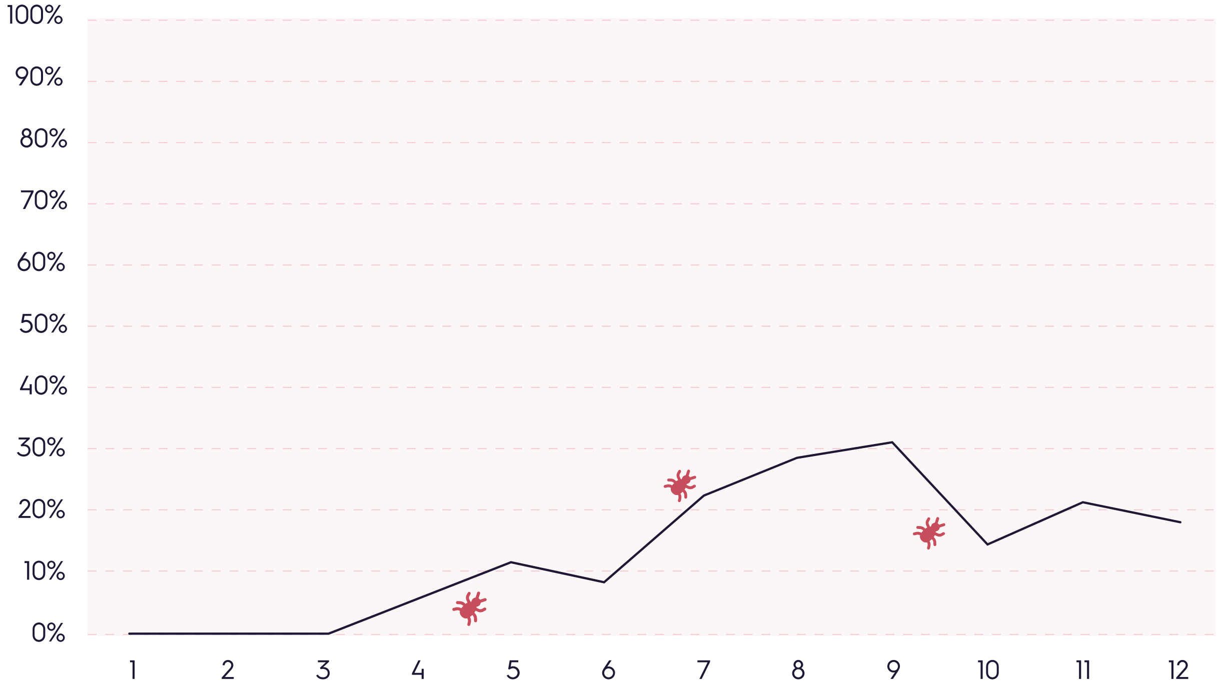


Figure 2: Percentage of phishing incidents with AiTM

An external Teams user tried to masquerade as a Sopra Steria employee and sent a phishing message through Microsoft Teams to several employees in Sopra Steria. The attachment was a .rar file, which led to a landing page mimicking the Brazilian agency for education. Seemingly, this was an attempt to phish for credentials.

Teams-Phishing

Microsoft Teams has over 280 million active users and is used as a communication and collaboration platform for many organizations. Unfortunately, Teams are now increasingly being abused in phishing campaigns. The objective for the threat actor is to send lures that attempt to steal credentials from a targeted organization by engaging a user and eliciting approval of MFA prompts.

Teams-phishing was first detected in Sopra Steria Scandinavia SOC customer base in June of 2023. At the time this method was closely associated with actors tied to Foreign Intelligence Services of the Russian Federation (SVR) but was quickly adopted by threat actors on the broader cybercrime scene. Microsoft since then has reported on this method being used by initial access brokers and other cyber criminals.

Another form of Teams-phishing, is to trick users to download malicious files to enable the threat actor to remotely access the target`s computer in order to carry out cryptocurrency mining, reverse shell, keylogging, clipboard stealing, and information stealing (files, browser, data). One of the preferred techniques is to use compromised Office 365 tenants (often owned by small organizations) to create new domains that appear as technical support entities.

Quishing

Fraudulent QR code campaigns are targeting European organizations, including Sopra Steria Scandinavia and its customers. Deceptive websites mimic legitimate services to steal login credentials or personal information and may also be used to distribute malware. This method exploits vulnerabilities in Bring Your Own Device (BYOD) policies, as users often open malicious URLs on less secure personal devices.

Sopra Steria Scandinavia SOC saw its first incident of this method being used in July 2023. Over the following months there was a large uptick in the use of QR codes to conduct phishing attacks in all sectors across Sopra Steria Scandinavia customer base.

Exact numbers are difficult to track due to the challenges faced by email security vendors to implement technology to be able to detect QR codes in emails. Numbers from open sources suggest there was a substantial growth in 2023, starting in August. It was not until transition from November to December that Microsoft was able to decode QR codes and run the URLs in their detection and response systems.

Removable media

Removable media-based attacks, mainly USB fall under this phase when malicious software or payloads are delivered through infected devices. For example, an attacker might use a USB device loaded with malware and strategically place it where it can be connected to a target system. When the unsuspecting user connects the USB device to their computer, the malware is delivered, initiating the attack. This delivery method is a tangible way for attackers to gain access to a system, and it aligns with the broader concept of the delivery phase in the Cyber Kill Chain.

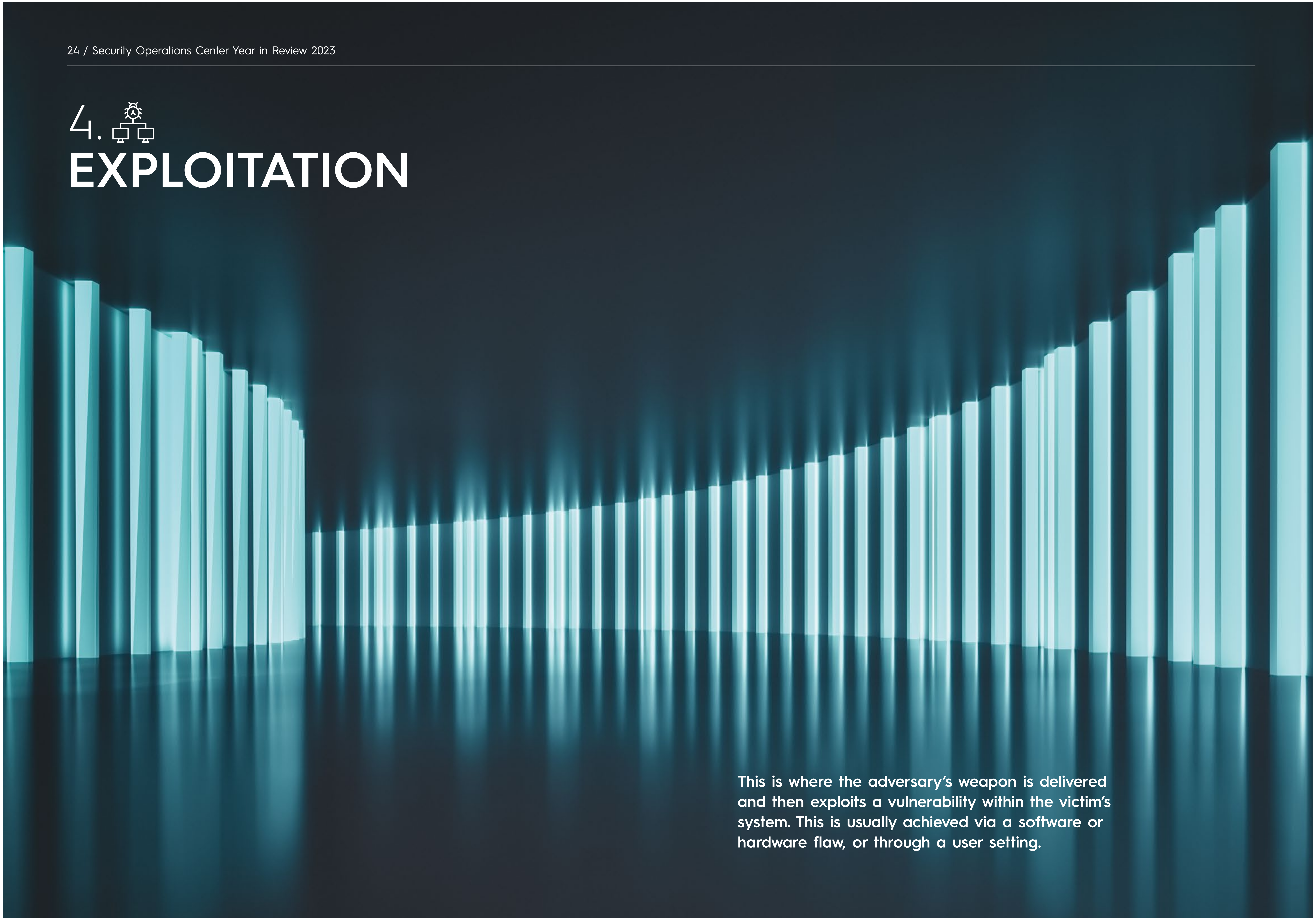
This method is by far most observed in the Shipping sector among Sopra Steria Scandinavia' customers. Due to limited internet access on ships, extended periods at sea, and an international workforce, those employed on ships use removable media devices far more than in other industries. In addition, many of these crew workers dock at various harbours worldwide and often find themselves in regions where it is more common to buy pre-loaded media devices that are potentially loaded with malware.

Web-Based Exploitation

Malvertising and Search Engine Optimization (SEO) poisoning are two prevalent techniques used by cybercriminals to deliver malware to exploit vulnerabilities in the delivery phase of the Cyber Kill Chain. In Sopra Steria Scandinavia SOC observations, the delivery of malicious codes using these tactics is quite prevalent. When integrated with freeware versions of applications such as Photoshop, Adobe, MS Visio and more, these methods constitute a particularly effective strategy for actors aiming to target a wide victim base.

Throughout 2023, the global employment of malvertising and SEO poisoning by malicious actors increased, emerging as a commonly used delivery approach. Even though such methods have long existed, the latter part of 2022 witnessed a surge in this trend. This pattern of growth persisted well into 2023, and numerous campaigns have been observed utilizing both commodity and specialized malware. These techniques are compelling to hackers in the delivery phase of the Cyber Kill Chain as they provide wide-reaching and covert avenues for deploying malware.

4. EXPLOITATION



This is where the adversary's weapon is delivered and then exploits a vulnerability within the victim's system. This is usually achieved via a software or hardware flaw, or through a user setting.

Vulnerabilities

In 2023, the cyber security world saw an acceleration in the speed and efficiency of attackers exploiting vulnerabilities. The most significant risks were associated with a small fraction of the total vulnerabilities (less than one percent) which were exploited frequently in the wild. The top three modes of attack were identified as the exploitation of remote services, public-facing applications, and privilege escalation.

The trend towards remote exploitation is particularly noteworthy with over a third of high-risk vulnerabilities being remotely exploitable. Network devices and web applications were found to be a hotbed for these vulnerabilities, clearly indicating areas that require increased vigilance. The potential impact of these vulnerabilities is amplified where there is opportunity for attackers to bypass authentication systems or escalate their privileges - effectively opening all doors to threat actors and simplifying system compromise and data exfiltration. Surprisingly, the ability to exploit these vulnerabilities is not limited to highly skilled hackers. With the proliferation of hacking tools and knowledge, even less experienced cyber actors can deal significant damage, marking a significant shift in the cyber threat environment.

- **Microsoft patched a total of 909 CVEs (Common Vulnerabilities and Exposures) as part of their regular Patch Tuesday releases, marking a slight dip of 0.87% compared to the previous year.**

- **From the vulnerabilities released by Microsoft nearly 90% of them were tagged as 'important', where a lower 9.6% fell into the 'critical' category.**

- **Remote Code Execution (RCE) topped the list by constituting 36% of the vulnerabilities. Elevation of Privileges (EoP) was the second most common, at 26%, followed by Information Disclosure, which made up 12.5%. Despite having a dedicated category, no vulnerabilities were labelled as Tampering in 2023.**

- **In terms of zero-day vulnerabilities, which refer to software vulnerabilities exploited in the wild or publicly disclosed prior to patches being available, Microsoft patched a total of 23 in 2023. More than half of these were EoP flaws, often exploited by advanced persistent threat (APT) actors as part of hpost-compromise activities.**

Noteworthy Vulnerabilities 2023

Cisco

Threat actors started exploiting CVE-2023-20198 when it was a zero-day before Cisco disclosed it on October 16. Ten days after that, the Censys platform for threat hunting found on October 25 around 28,000 Cisco IOS XE hosts showing signs of compromise spread all over the world. According to Censys' findings, many of the hacked devices are at major telecommunications and internet providers offering their services country-wide. Initial estimates after the disclosure from Cisco counted around 10,000 instances running a malicious implant. Norwegian National Security Authority (NSM) publicly stated in October that several Cisco IOS XE units in Norway had been compromised.

Citrix Bleed

This flaw, impacting Citrix NetScaler ADC and Gateway, has become a focal point of global concern, as evidenced by targeted attacks on government networks and financial institutions. The vulnerability, dubbed Citrix Bleed, allows threat actors to exploit session tokens, potentially leading to unauthorized access and data compromise. When the first observed attack took place there were over 60,000 Internet-visible NetScaler instances, of which over 10,000 had not yet been patched against CVE-2023-3519.

Microsoft Outlook zero-touch

CVE-2023-23397 is a critical Elevation of Privilege vulnerability in Microsoft Outlook that is triggered when an attacker sends a specially crafted Outlook attachment designed to steal NTLM hashes. In March 2023, APT28 started to launch high volume campaigns exploiting CVE-2023-23397 targeting higher education, government, manufacturing, and aerospace technology entities in Europe and North America. APT28 is attributed by the United States Intelligence Community to the Russian General Staff Main Intelligence Directorate (GRU).

MOVEit

Roughly 600 organizations worldwide have fallen prey to a ransomware organization known as CL0P, whose latest extortion scheme involves exploitation of a zero-day SQL injection vulnerability within MOVEit Transfer, a Managed File Transfer (MFT) application. The latest data suggests that this MOVEit Transfer vulnerability has served as a catalyst for one of history's most severe supply chain cyber-attacks. The magnitude of this cyber-attack is akin to the notorious SolarWinds exploit of 2020 and the Log4J vulnerability discovered in 2021.

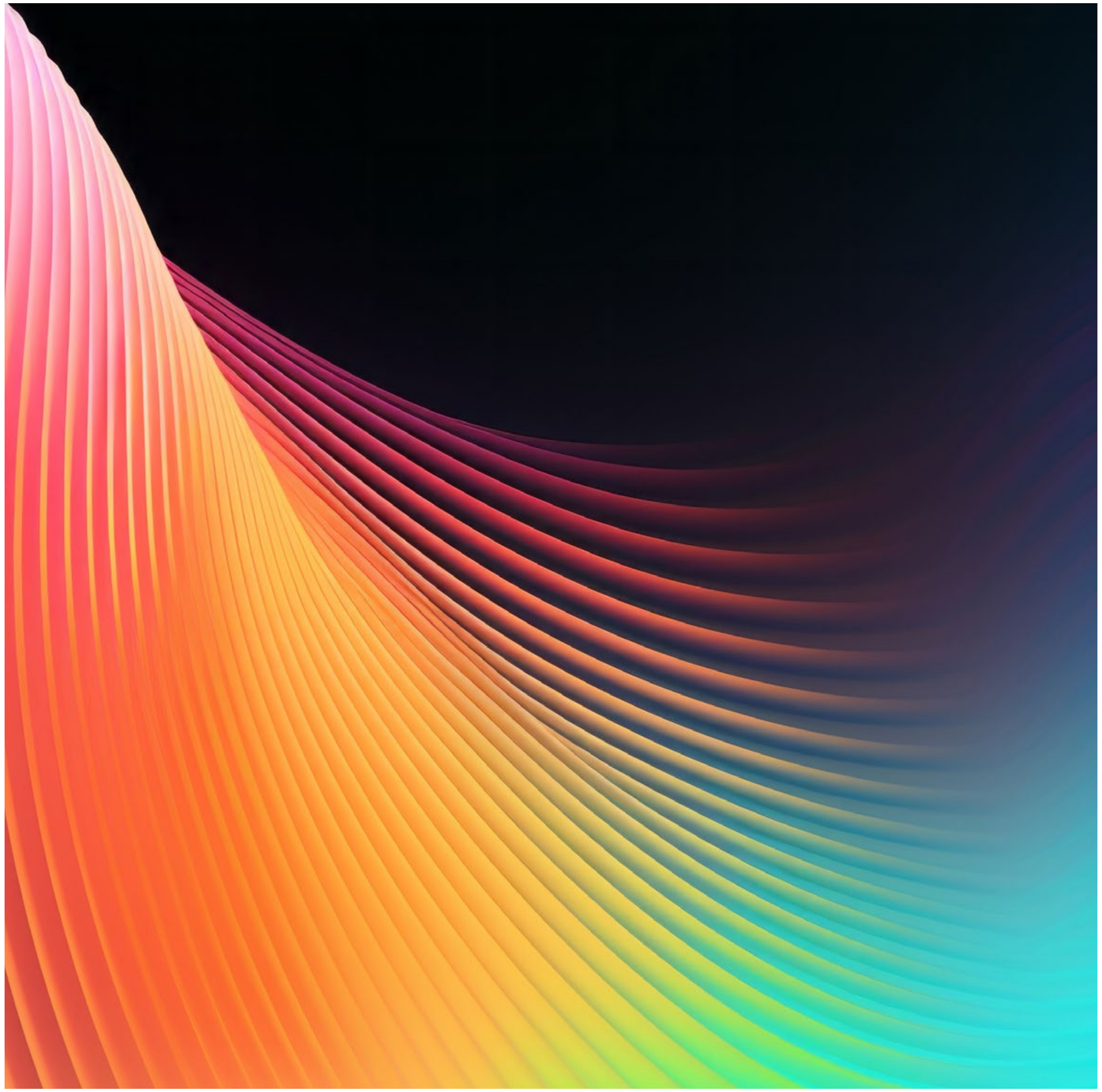
Ivanti

In July the software company Ivanti patched a critically rated zero-day vulnerability in its EPMM platform, formerly known as MobileIron Core, after an unidentified threat actor used it to attack a dozen government ministries. The company later found the zero-day can be chained with another zero-day flaw and released a second emergency patch.

Misconfiguration

In the context of the cyberthreat landscape, misconfiguration of infrastructure systems poses several dangers. One key risk arises from the misconfiguration of hybrid identity setups such as on-premises Active Directory and Microsoft Entra ID. Due to their complex architecture, these systems can be challenging to configure correctly. When they are compromised due to misconfigurations, it might provide a gateway for threat actors to gain significant access, allowing them to persist undetected within the infrastructure and potentially seize control of all identities.

Equally concerning is the threat of token theft from highly privileged accounts, granting of excessive privileges to users and workload identities, device and access control, misconfigured permissions, and misconfiguration of conditional access policies. Each of these misconfigurations presents potential pathways for threat actors to gain unauthorized access, escalate their privileges, compromise sensitive data, introduce malware and persistent threats, and cause significant operational disruption. A keen focus on mitigating these misconfigurations is crucial in today's cyber threat landscape.



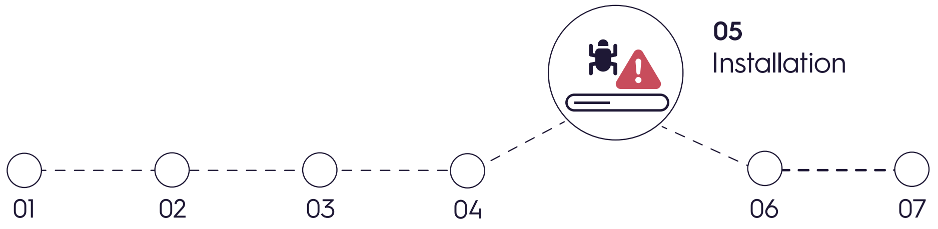
API

API Cyber Attacks are sensitive to the rising rates of cyber-crimes. The shift towards an API-first design signifies their central role in web development in the current landscape. This approach highlights the importance of strong, robust APIs capable of serving as the backbone of both the front-end and backend systems. However, the rising importance also indicates their vulnerability for cyber-attacks.

Increased API usage has attracted cyber criminals, leading to a surge in API attacks ranging from simple to sophisticated methods exploiting insecure coding practices like input validation failures, weak authentication, and security misconfigurations. One prevalent strategy involves automated bot attacks systematically exploiting vulnerabilities. In 2023, Shadow APIs emerged as a major threat, operating without organizational knowledge, and exposing APIs to significant risks including data breaches. Cloudflare's machine learning-based discovery revealed an additional 30.7% of API endpoints, highlighting the substantial risk posed by Shadow APIs. Despite their importance in the digital landscape, APIs represent a growing vulnerability to be exploited by cyber criminals.

5. INSTALLATION

Once access is gained, the attacker installs malicious software on the targeted system. The software will establish a persistent presence, allowing the attacker to maintain control over the compromised system even if the initial exploit is detected and closed off.



Commodity Malware

Well-known malware types have been observed and blocked across Sopra Steria Scandinavia SOC customers during 2023. These kinds of malware are often designed to gain initial foothold and download additional malicious tools or give access to threat actors for further compromise. Wacatac, Detlock, Presenoker, Bearfoos, Plasti, and MediaArena were the most detected malware families. There has also been an increase in keygen malware, and numerous instances of Rasberry Robin delivered through USB-devices to endpoints. The latter is often used by initial access brokers associated with ransomware operators. Furthermore, malware such as Andromeda and Mistcloak have been observed in incidents linked to infected USB-devices.

In 2023, commodity malware, primarily represented by loaders such as Qakbot, Ursnif, Emotet, Trickbot, and IcedID, continued to pose significant cyber threats. Having initially functioned as banking trojans, they have diversified their capabilities to support advanced operations. These well-known loaders have become popular tools in cyber operations, especially for enabling ransomware attacks.

Significant changes to these loaders in 2023 included the release of new versions tailored for ransomware actors. They featured enhanced reconnaissance features and had certain functions removed to avoid triggering antivirus detections, making them particularly attractive to ransomware groups and initial access brokers.

In response to Microsoft's default disabling of macros in 2022, commodity loader operators either innovated new techniques to use undetected macros or else refrained from using them altogether. This led to the use of a variety of file types, scripting languages, packers, and exploits to deploy the loaders.

Also noteworthy is the fact that these commodity loaders have been deployed against organizations all over the world, with particular focus on North America and Europe, which marks a shift away from individuals' financial data. This change correlates with the loaders' evolution away from their original role as banking trojans.

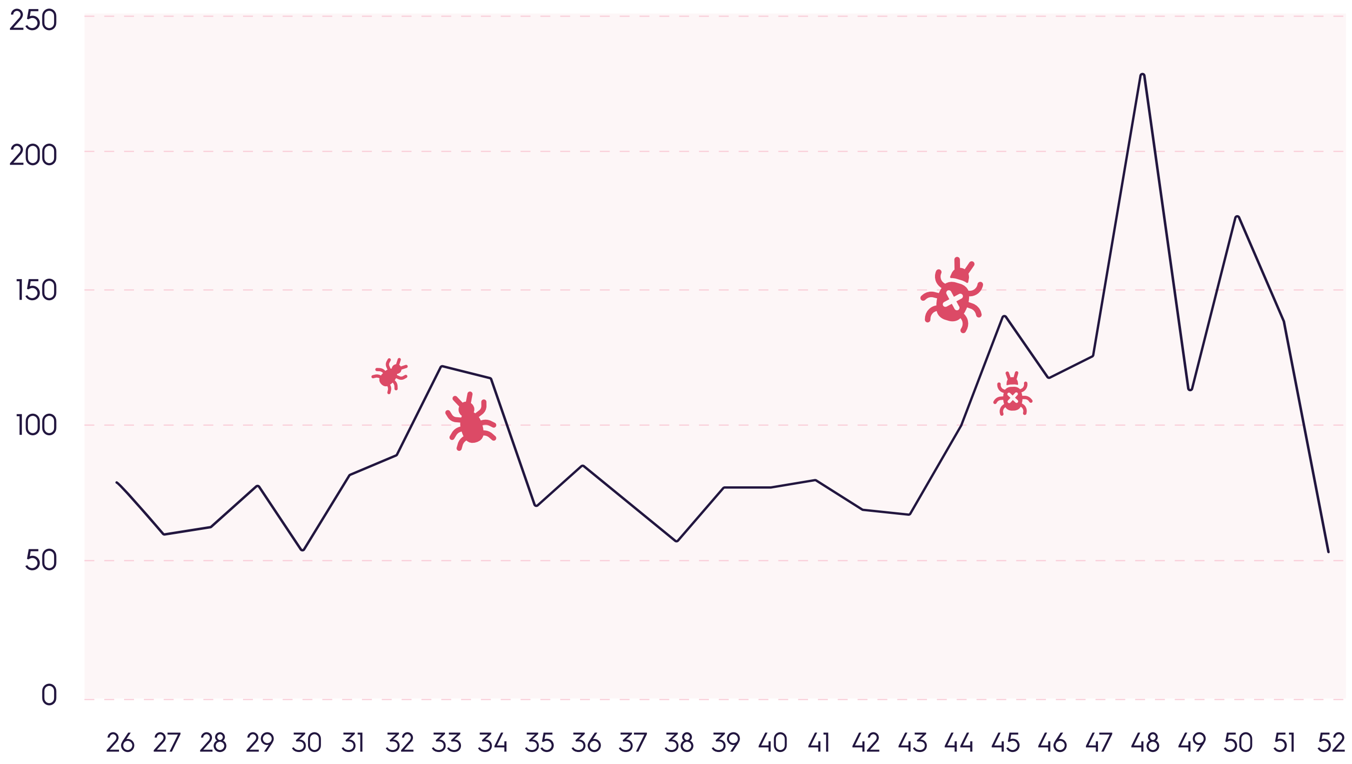


Figure 3: Malware trend Q3-Q4

In 2023, two cases involved compromised USB devices with Mistcloak malware, linked to actor UNC4191 by Mandiant. This actor focused on targets in the Philippines, employing Mistcloak to spread through infected USB devices. Their strategy involved the deployment of trojans DarkDew and BlueHaze to establish backdoors and propagate through connected removable USB devices within the compromised network.

A Sopra Steria Scandinavia customer was affected by the malware SocGholish. This malware leverages drive-by-downloads masquerading as software updates to gain initial access, and has been linked to the Russian cybercrime group Evil Corp since April 2018. When SocGholish is executed a JavaScript payload connects back to SocGholish infrastructure, where it shares details about the infected host and can retrieve additional malware. Secondary payloads are NetSupport, and Blister with an embedded Cobalt Strike payload. Some known SocGholish intrusions have led to various ransomware families such as Lockbit.

Several notable observations from Sopra Steria Scandinavia SOC include the Gootloader malware, often distributed through SEO-poisoning. This initial access tool serves to open the door for more damaging malware and hacking tools, such as Cobal Strike or other penetration testing tools. Gootloader is regularly observed as the start point for Ransomware attacks and has been in consistent use throughout 2023. Another malware variant that gained attention in 2023 is the Vigorf malware. This is part of a larger cybersecurity threat identified by Microsoft as Storm-0300, an anonymous activity connected to ransomware attacks. It includes both preliminary ransomware activities as well as full-on ransomware distribution. Observed usage of Vigorf malware notably increased after the summer of 2023.

Stealers

Throughout 2023, the cybersecurity landscape saw a significant rise in the prevalence and sophistication of information-stealing malware, often referred to as "stealers". This upsurge reflects a wider trend within cybercriminal operations aimed at exploiting the increasingly digital nature of personal and professional life. There are several notable aspects of this evolution.

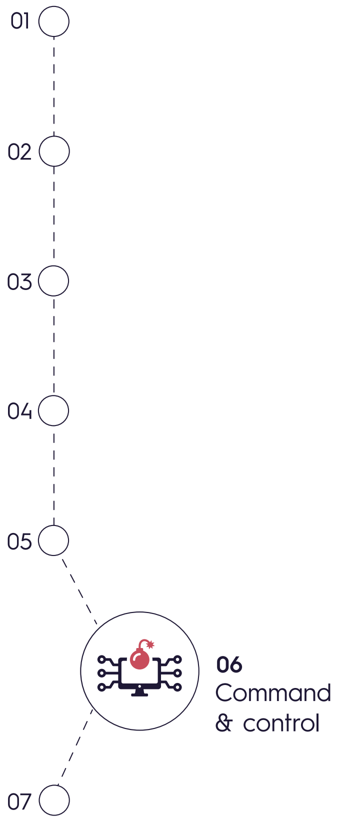
The use of stealers has skyrocketed compared to 2022. The reason behind this rapid growth likely relates to the increase in the amount of valuable and sensitive data stored online. Stealers provide cybercriminals with easy access to users' private data, such as banking information, social media credentials, and crypto wallets. The easy and quick profitability offered by these stealers makes them highly attractive to cybercriminals.

Stealers have evolved to operate more stealthily, going undetected for longer periods by antivirus products. Malware developers have employed various techniques and tactics to avoid detection, including the use of polymorphic code, encryption, and zero-day exploits. Stealers have also seen increased reliance on 'living off the land' (LoTL) techniques, using already installed legitimate software for their malicious activities.

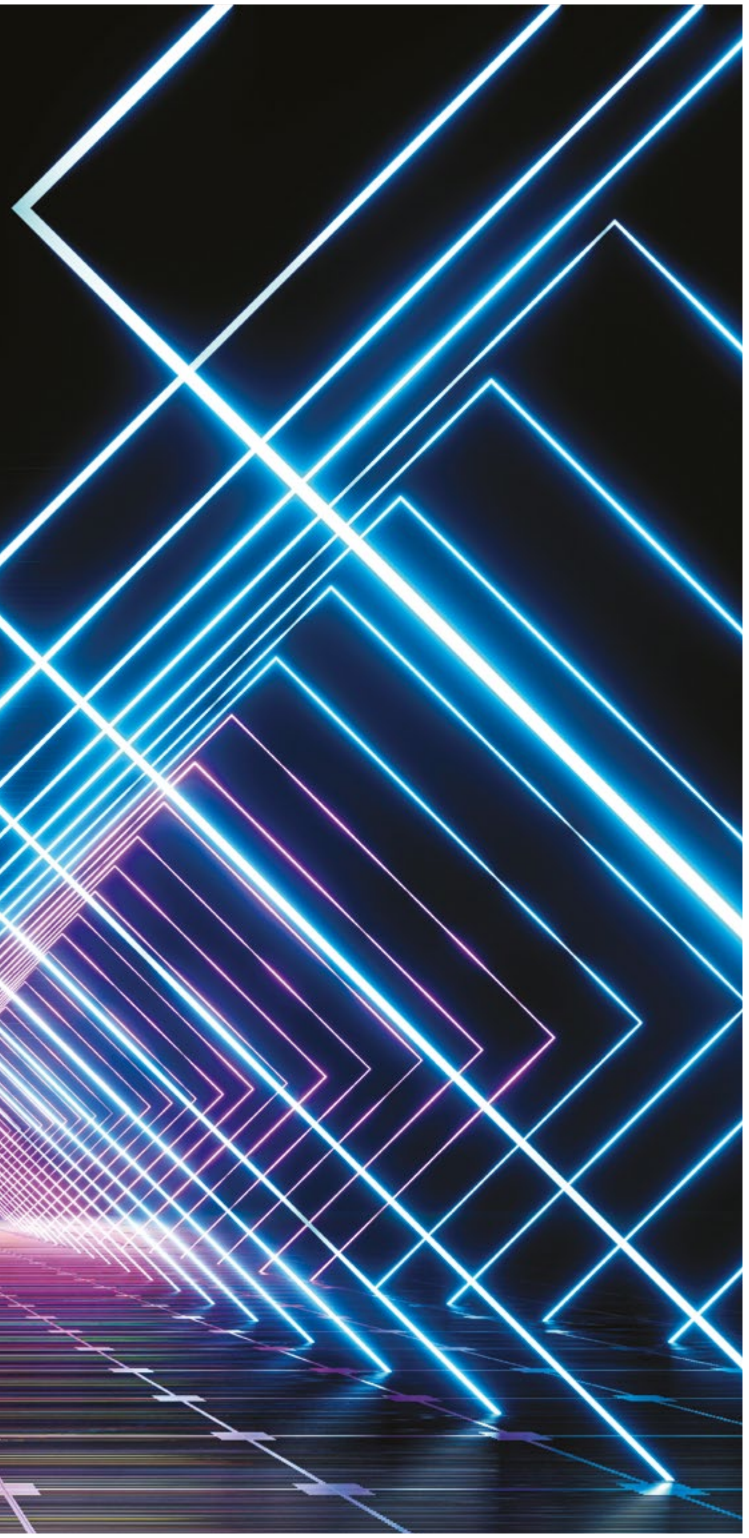
Stealers have expanded their scope, targeting a wider range of data. Besides regular personal identification information (PII), they now go after corporate files, intellectual property, trade secrets, legal documents, and medical records. The dark web has served as a thriving marketplace for the sale of info stealers. Malware as a Service offerings, which lower the technical bar for aspiring cybercriminals, have accelerated the dissemination and use of stealers. Additionally, threat actors are sharing stolen data via platforms like Telegram or Discord, complicating the task of tracking and preventing further distribution of stolen data.

The amount of credentials being sold on dark net forums and marketplaces is indicative of the high volume of stealer malware activity. Information from darknet forums obtained by Sopra Steria Scandinavia SOC, includes posts that advertise leaks, showing an updated version of chrome and a long list of credentials from what appears to be private websites, such as gaming, auctions, news and entertainment. Sopra Steria Scandinavia SOC have seen instances where the data leakage of corporate access details is due to the synchronization of browsers between corporate laptops and personal computers, where the presence of stealer on private computers is the credential theft method and subsequent listing on darknet forums.

6. COMMAND & CONTROL



Post-installation, the malware establishes communication with the attacker's command and control (C2) servers, granting remote control over the target's systems and enabling data exfiltration or the delivery of additional payloads. The command & control stage involves various details including backdoor type, communication protocol, embedded protocol nuances, external infrastructure, and operating mode characteristics.



New ways to communicate

Both state-actors and cybercriminals are increasingly using established, commodity, and open-source tools, including command-and-control frameworks and anonymization networks. The earlier adoptions of offensive security tools like Cobalt Strike, and remote access tools (RATs) such as AsyncRAT, QuasarRAT, PlugX, and ShadowPad, are still broadly used in 2023 by threat actors.

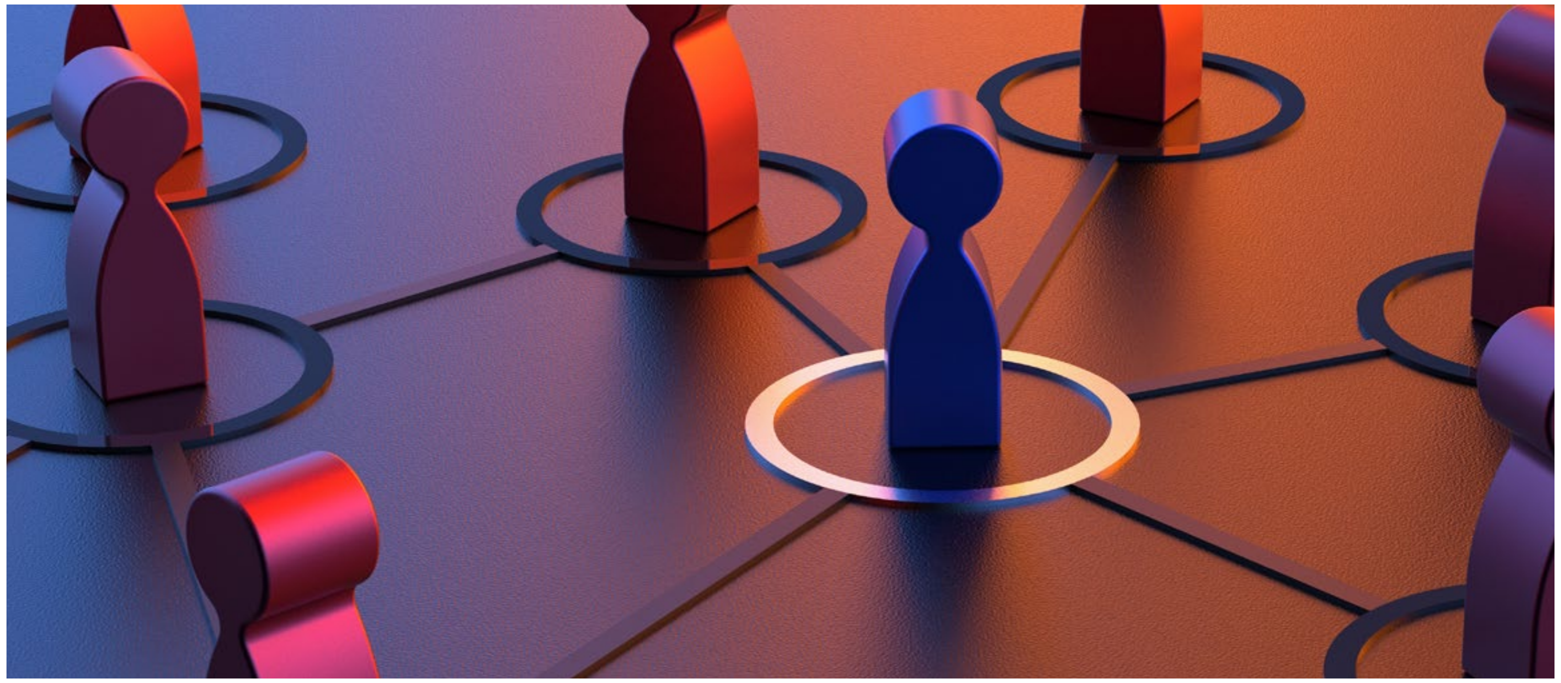
The evolving threat landscape introduces new tactics such as messaging and collaboration tools like Telegram and Discord to obscure C2 traffic. Adversaries leverage these platforms for secure, reliable, and long-term communication channels that blend with normal network traffic, making detection increasingly challenging. In 2023, these methods were observed more frequently.

During May, a compromised host was discovered for one of Sopra Steria Scandinavia customers. The infection was first detected during a firewall log audit, showing strange connections made in specific time intervals to foreign IP addresses. Further investigation showed that the threat actor had dropped the RDP-program Aeroadmin as a backdoor after the initial breach, and that the host was infected by the XMRig cryptominer. XMRig is an infamous cryptominer that was being regularly observed during the first half of 2022.

Efforts from law enforcement

There were some major takedowns of malicious infrastructure in 2023 by law enforcement, such as the QakBot takedown and the attempt to take down unlicensed versions of the commercial red-teaming product Cobalt Strike. Also, worth mentioning here is the disappearance of Emotet in July 2023, possibly an effect of the takedown of this botnet in 2021.

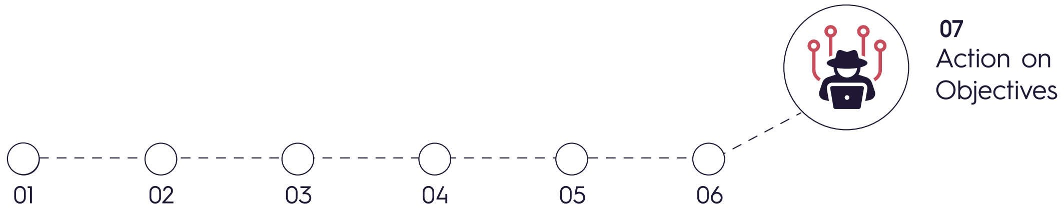
All these infrastructure takedowns exhibit varying efficacy, influenced by factors such as physical custody of perpetrators, infrastructure redundancies, and operators' contingency plans. Recorded Future has examined three cases from 2023 (Emotet, QakBot, and Cobalt Strike), where the results indicate mixed outcomes. While Emotet demonstrated post-takedown resilience, QakBot experienced a temporary halt with subsequent resurgence, and Cobalt Strike's impact was limited due to a narrow focus on specific instances. Cobalt Strike servers were back in their original range within a few weeks. Despite the infrastructure-takedowns, their related malwares are still being observed among Sopra Steria Scandinavia customers. Takedowns disrupt criminal operations reactively, but are only part of a wider solution which requires regular effort to protect our continuously evolving systems.



7. ACTION ON OBJECTIVES

Sopra Steria Scandinavia has encountered only a small number of instances where the adversary has reached the action on objective phase with severe consequences. To analyse trends and to assess the effects of various adversaries on their targets, we need to look beyond Sopra Steria Scandinavia customer base for a broader understanding of this phase.

> The 2024 annual threat and risk assessments from the Norwegian Intelligence Service, Norwegian Police Security Service and the Norwegian National Security Service provide valuable insights into the capabilities and expected intent of threat actors relevant to Sopra Steria Scandinavia and our customers.



Action on objective means everything that happens after the adversary has operational control of a system. This may include data theft, system damage, disruption to organizational operations, or preparing for additional attacks. This is often considered the end goal of the cyber kill chain, but in actuality it feeds back into the start of the cycle, offering further opportunities for reconnaissance and escalation. As the last stage, one can say that all actions that the adversary takes over the established C2 channel are considered actions on objectives.

Generally, ransomware remains the primary threat to organizations and this is something that seems unlikely to change during 2024. The accelerating development of Ransomeware-as-a-service (RaaS) gives power to a broader range of malicious actors at affordable rates. Just as many industries have shifted towards short-term contracts for efficiency, criminals rent or sell their ransomware tools for a portion of the profits, rather than carrying out the attacks themselves.

While state-sponsored actors, typically tasked with government objectives, conduct their cyber activities for political, economic, defence, or strategic reasons. They may be involved in a variety of activities, such as cyber espionage, sabotage, destructive malware deployment against high-value targets and critical infrastructures and coordinating propaganda or disinformation campaigns.

As state threat actors advance in sophistication, governments are increasingly leveraging them to gain insights into the plans of other nations, transnational bodies, and non-governmental organizations. Critical infrastructure continues to be a favoured target, with threat actors employing more discreet techniques to establish persistence and to avoid detection. Concurrently, certain governments have employed cyber-enabled influence campaigns to manipulate public opinion both domestically and internationally.

Ransomware

In the first half of 2023, ransomware breach events increased by over 75% compared to the same period in 2022, totalling nearly 2,000 incidents, according to Intel471. The ransomware-as-a-service (RaaS) affiliate model, particularly utilized by LockBit, 3.0, ALPHV, Cl0P, Royal, and Play remained popular, lowering entry barriers for attackers. The United States experienced the highest impact, with almost 46% of reported incidents, followed by the United Kingdom and Canada. Professional services, consumer products, and manufacturing sectors were the most affected.

While established ransomware players continued to dominate, new variants emerged, notably Akira. This ransomware, which surfaced in March but became fully active in April. Akira follows the double-extortion tactic of encrypting data and threatening its release on a victim shaming site if the ransom isn't paid. Interestingly, Akira's resemblance to parts of the Conti strain suggests potential use of leaked Conti ransomware files from 2022 by its developers, although its RaaS affiliate program wasn't openly advertised on cybercrime forums.

Data Theft

Data theft has become common among actors in the evolving ransomware landscape. Where actors gain unauthorized access to an organization's sensitive data and then proceed to exfiltrate, or remove this data from the system. Once the data has been exfiltrated, the criminals threaten to publicly release this information unless a ransom is paid. Cloud Storage and file sharing services, such as Dropbox, Google Drive, or OneDrive, are becoming a commonly used by actors to transfer data. Other methods can include remote desktop protocols, instant messaging or chat services and web-based data exfiltration.

These data exfiltration techniques can lead to significant monetary and reputational damage for the targeted organizations. Organizations can incur additional costs from incident response processes, legal issues from violation of data protection laws, and reputational damage leading to loss of clients.

State actors are often more focused on trying to remain unseen and undetected to keep their access within an infrastructure. This causes them to opt for more stealthy techniques when exfiltrating data. Popular methods include encoding data into web traffic parameters, such as URL parameters, cookies, or HTTP headers, DNS tunnelling to transmit it to remote servers. This type of method can evade traditional network monitoring tools by blending in with normal traffic flows.

Some state operations observed focus on long-term network infiltrations designed to stealthily extract data. This type of activity often targets defence networks and broader critical infrastructure sectors worldwide. In our observed cases, the perpetrators not only aimed to steal technology secrets but also engaged in continuous surveillance efforts against individuals beyond their territorial borders who they considered enemies of the state.

Sabotage

Cyber sabotage operators in 2023 evolved from a diverse portfolio of actors, with many campaigns stemming from sophisticated state-aligned as well as non-state actors. Since the invasion of Ukraine in 2022, Russian cyber sabotage operations have been the prime source of learning in relation to cyber sabotage and hybrid warfare.

Various methods were employed to achieve operational objectives, causing significant disruptions, and revealing the complex and evolving nature of cyber warfare. Among the primary tactics used was the integration of cyber operations into wider military campaigns. These operations capitalized on a range of offensive capabilities including the utilization of malware attacks, wiper activity, and sophisticated system intrusions. A notable shift was observed in the spring of 2023, when these actors shifted their focus away from high-volume destructive attacks, back to more frequent cyber espionage operations, targeting information to support troop movements on the ground.

Another aspect is the prepositioning in infrastructure as a future capability. Threat actors have been observed gaining access to predominately critical infrastructure and in some cases OT environments with a view to remaining dormant for long periods of time. Thus, malicious actors hope to retain the ability to shut down or to destroy critical systems at some time in the future

OUTLOOK 2024

The overall geopolitical landscape is tense with war raging in Europe and escalating uncertainties in the middle east impacting global trade and economy. Increasing uncertainties and tensions in South-East Asia in combination with an upcoming presidential election in the US is sparking discussions on the future of US-NATO relations. The list is long when discussing factors impacting cybersecurity for Sopra Steria Scandinavia and our customers in 2024 and none of these elements is necessarily isolated from the other. Understanding and adapting to these external factors is crucial for us as a managed service provider to maintain resilience, competitiveness, and the ability to meet our clients' evolving needs.

In a scenario where Donald Trump again steps into the Oval Office an even bolder Russia might rise within multiple domains to challenge NATO, particularly on where the «Article 5» line is drawn. Russia will in such a scenario likely escalate its destructive cyberoperations where it can invoke plausible deniability through threat actors loosely linked to the Russian Government or Private Military Companies.

China`s focus on strategic positioning within multiple domains to eventually challenge US superiority is highlighted through the annual threat assessment by the Norwegian Intelligence Service. Increased trust and cooperation with Russia to achieve this strategy has been evident since the invasion of Ukraine. Growing relations and military cooperation, although limited in 2023, could potentially lay grounds for the same within cyberspace in 2024. A cooperation that would fuel the tactic of plausible deniability.

2024 will highly likely see significant surge in cyber threats driven by AI. AI will undoubtedly enhance cyber-attack capabilities, a trend we have already observed targeting our customers. However, its impact is highly dependent on the threat actor utilizing it, their access to specialized competence and the data-quality at their hands. AI has proven to be extremely effective through reconnaissance for both skilled and un-skilled threat actors enabling more effective target development. In 2024 we will highly likely see examples of AI-developed zero-day exploits and advanced malware creation. AI will for Cyber criminals, hackers-for-hire and hacktivists therefore likely contribute to a surge in successful breaches in the year to come.

Probability Matrix

Highly Unlikely	Unlikely	Even Chance	Likely	Highly Likely
<10%	**10-40%**	**40-60%**	**60-90%**	**>90%**

CONCLUSION & RECOMMENDATIONS

The general trends show a threat landscape becoming more advanced, more professionalized, more effective, and with a lower barrier-to-entry. Organizations need to be aware of the specific threats that saturate their respective industries. Industries such as manufacturing and healthcare often find themselves embroiled in ransomware attacks due to their critical nature and the high value of the data they hold. Meanwhile, sectors like research and defence often find themselves in the crosshairs of state-sponsored actors for strategic reasons.

When identifying which malicious actors are relevant, it needs to start with an understanding of the organization. The type of data it handles, the assets they possess as well as their respective value, will offer insights into what might attract threat actors. Understanding the valuable assets of an organization is the first part of creating a good security posture.

Most of the cybercrime trends reported on globally in 2023 reflects Sopra Steria Scandinavia observations and incidents. Phishing, with its new methods, constitutes the largest category of security incidents handled by our Security Operation Center in 2023. Other featured categories include stealer malware, commodity malware and suspicious user behaviour. EDR-tools on servers and client are an absolute must for detecting and responding to malicious activity.
We recommend all organizations to adhere to the NSM core principles for ICT-Security. We observe that any of our customers who have developed a higher level of security maturity have fewer security incidents.

There are a couple of areas from the core principles that we would like to highlight:

Attack Surface Reduction

Several of our customers have worked diligently with attack surface reduction by implementing controls, such as preferred CIS benchmarks, best practice controls for malware/ransomware prevention and setting ambitious targets for vulnerability management.

Once controls are in place, a successful attack surface reduction program should include capabilities and processes such as:

- Asset-based attack surface monitoring.
- External attack surface monitoring.
- Monitoring of the external vulnerability landscape, supplemented with threat intelligence and situational awareness from a Security Operations Center.
- Automated regular scanning of clients, servers, and network components.
- Vulnerability telemetry categorized and followed up upon based on information from Configuration management database (CMDB) and prioritized based on exposure and criticality.

A strict policy for handling removable media

- Throughout 2023, Sopra Steria Scandinavia SOC continued to observe malware incidents caused by infected USB-devices. Customers with stricter execution policy (such as properly configured ASR-rules in Defender) and mature processes for handling USB devices had fewer security incidents overall.

Automated detection and response of known threats

- Implementing a centralized XDR-solution such as Microsoft Defender for Endpoint or SentinelOne ensures processes, files, and network connections on endpoints (clients and servers) are monitored for malware and suspicious activity.
- A detection program should include support for both signature and heuristics-based detection.
- Phishing awareness and reporting
- Customers that have worked actively with security awareness and have implemented solutions for user-friendly reporting of malicious email have significant higher submission and detection rate on phishing campaigns.
- Responding to alerts on potentially malicious activity based on deployed tooling or based upon custom threat detection
- Ensure a user-friendly method for users to report suspicious e-mails that includes both verdict and feedback.

Contact

For feedback, comments or enquiries about our services, don't hesitate to contact us. If you would like to subscribe to our weekly security newsletter, please click here.

Jørgen Rørvik
Director of Cybersecurity
& Connectivity - Scandinavia

Email: jorgen.rorvik@soprasteria.com
Mobile: +47 97 05 77 30
Norway

The world is how we shape it.

www.soprasteria.no