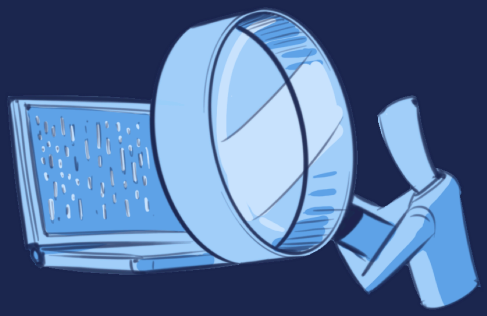
CERT-EU

THREAT LANDSCAPE REPORT

2024

A YEAR IN REVIEW

VERSION 1 – 25 FEBRUARY 2025



CERT-EU, the Cybersecurity Service for Union entities

This page is left intentionally blank.

Table of Contents

1 About CERT-EU

CERT-EU is the Cybersecurity Service for the European Union institutions, bodies, offices and agencies (Union entities). Our legal basis is Regulation (EU) No 2023/2841 laying down measures for a high common level of cybersecurity at the institutions, bodies, offices and agencies of the Union (OJ L, 2023/2842, 18.12.2023) (the 'Cybersecurity Regulation'). We were established in 2011.

2 Introduction & key findings

In 2024, we continued to scrutinise and dissect cyber threats to help the European Union institutions, bodies, offices and agencies (Union entities) detect and protect against cyberattacks.

With the ever-expanding array of cyberattacks, it is crucial to adopt proactive defence strategies, concentrating on the most pertinent and potentially harmful threats that could affect our stakeholders. As a result, **our cyber threat intelligence efforts are centred around what we call malicious activity of interest (MAI).**

To identify whether a cyberattack in the vicinity or in the digital ecosystem of Union entities warrants classification as MAI, we consider the following factors:

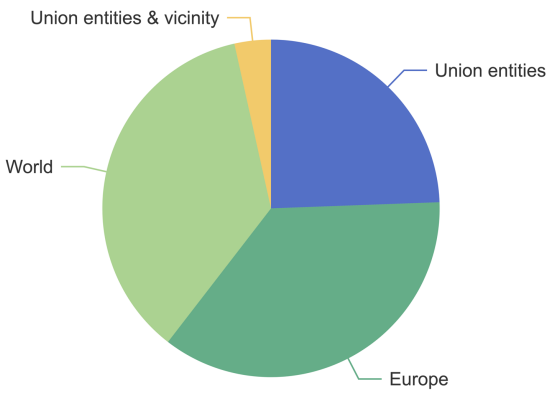
- The activity targets sectors of interest located in Europe.
- The activity involves software products or providers known to be used by Union entities.
- The activity targets partners of Union entities.
- The activity is related to geopolitical events (e.g. elections, conflicts, summits) involving Union entities.
- The activity is linked to a previously known advanced persistent threat actor that has targeted Union entities.
- The activity uses tactics, techniques, or procedures that are not automatically detected or blocked by cybersecurity tools because of their high level of sophistication.

For each MAI, we collect various elements such as:

- victimology: sectors, countries, software
- tactics, techniques and procedures (TTPs)
- malware strains and tools
- exploited vulnerabilities (CVEs)
- threat actor profile
- global events associated with the activity
- indicators of compromise (IoCs) and detection rules.

In 2024, we analysed 643 MAIs, compared to 602 the previous year. This allowed us to identify interesting patterns and trends in the threat landscape of Union entities.

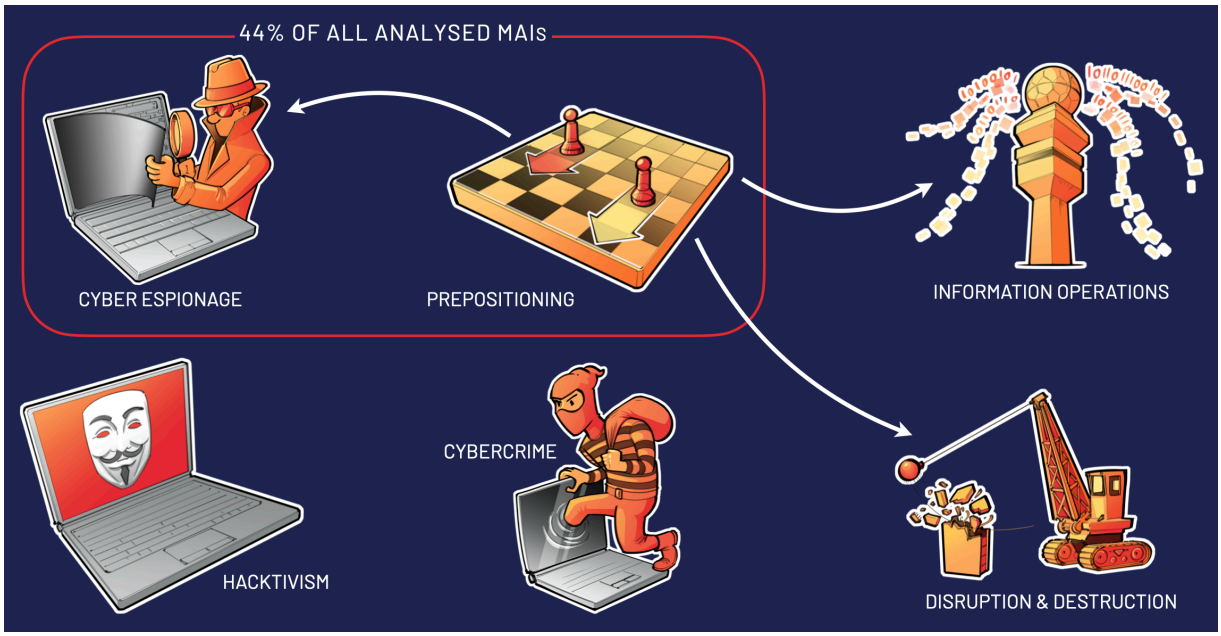
Domain targeting of analysed malicious activities of interest



The following report highlights some of the interesting patterns and trends that we have observed over the past year.

Key findings

- In 2024, **cyberattacks frequently coincided with or were triggered by global events such as elections, conflicts, and major international conferences.** These events served as catalysts for a wide range of offensive cyber activities, including cyberespionage, information operations, hacktivism, and targeted attacks on critical infrastructure.
- **We identified 110 threat actors who were active against Union entities or their vicinity.** Union entities had critical exposure to 20 threat actors, high exposure to 20, medium exposure to 23, and low exposure to 47. The most frequent motive for these threat actors was cyberespionage, followed by cybercrime, hacktivism, and information operations.
- **44% of all analysed malicious activities of interest were classified as cyberespionage and/or prepositioning.**



- When we could determine their origins, based on information from reliable sources, we noticed that **threat actors active against Union entities or their vicinity were highly likely linked to the People's Republic of China (hereafter China) and the Russian Federation (hereafter Russia),** followed by the Islamic Republic of Iran (hereafter Iran) and the Democratic People's Republic of Korea (hereafter North Korea).
- **Union entities experienced 15 significant incidents**[1], five of which involved zero-day exploitation.
- We found that **several recurring techniques shaped the threat landscape in 2024. These include the use of Operational Relay Networks (ORBs) to obscure activities, exploitation of public-facing applications, and gaining access to edge devices.** Furthermore, the following techniques were used: Adversary-in-the-Middle (AitM), Living-off-the-Land (LoL) techniques, cloud-based persistence, API abuse, and supply-chain compromises. These methods were employed to infiltrate systems and maintain persistent access while evading detection.
- We noticed that the targeting of service providers – including those providing telecommunications, cybersecurity, remote access, and software solutions – **underscores the importance of supply-chain monitoring and prompt response.**
- **Threat actors targeted 110 distinct software products in the vicinity of Union entities.** The methods of targeting were varied and included exploiting vulnerable internet-facing software products, supply-chain attacks using trojanised software, fake software versions, and abuse of public code repositories.
- In addition to the public administration sector, **the most commonly targeted sectors in our constituency and its vicinity were defence, transportation, and technology.**

[1] For more information on reporting obligations concerning significant incidents, see Article 21 of Regulation (EU) No 2023/2841.

3 Global events shaping the cyber threat landscape

In 2024, cyberattacks were often related to or even driven by world events, highlighting the **increasingly close link between geopolitical developments and cyber threats**.

Elections, conflicts, and major international conferences acted as triggers for various cyber operations, including cyberespionage, information operations, hacktivism, and targeted attacks on critical infrastructure.

Instead of covering every type of global event, we have chosen a few that have significantly shaped the 2024 threat landscape from our perspective.

Elections

Nation-state actors and affiliated cyber operatives frequently engaged in cyber activities to influence the outcome of elections.

We tracked cyber activity related to nine elections in 2024, including eight national elections and one for the European Parliament.

We observed recurring strategies, including deliberately timed hack-and-leak operations designed to sway public opinion, and supposed hacktivist campaigns that exaggerated claims of hacking, with the intention of causing public concern.

In all elections we observed reports of information operations aimed at amplifying specific narratives. Moreover, we noted that increased reporting of cyberespionage activity towards entities within a certain country often coincided with its elections.

For example, during the European Parliament elections, held between June 6 and 9, 2024, supposed hacktivists claimed DDoS attacks against political parties and a Union entity. On June 7, supposed hacktivists targeted a voter registration website and a public transportation website with DDoS attacks. Although the disruptions had only a limited impact on the availability of a small number of websites, the intent was likely to create a sense of chaos and undermine public trust in the electoral process.

Conferences

International private conferences, high-profile political meetings, and major cultural events often become prime targets for cyberattacks.

Cyberespionage actors take advantage of such occasions by creating fake invitations as lures in social engineering campaigns. **They also capitalise on the fact that interesting targets from a specific sector are gathering physically.** This facilitates the simultaneous targeting of specific groups of individuals.

For example, in October, a Russia-linked advanced persistent threat actor (APT) targeted individuals and entities active in the European energy sector with spearphishing. The lure was an upcoming conference in the European gas sector.[2]

Hacktivists often carry out DDoS attacks on such events to boast about their attacks on social media while the events are trending topics. This allows them to surf the wave of media coverage, amplifying their own visibility and messages.

Conflicts

Conflicts such as Russia's war on Ukraine and the Israel-Hamas war continued to drive intense levels of cyber activity across the threat spectrum. This included everything from destructive and disruptive attacks, cyberespionage, hacktivism, and coordinated information operations. Each was used by various threat actors to further their strategic and political objectives. Especially destructive activities, such as wiper attacks and targeted attacks on industrial control systems (ICS), are generally rare outside the context of armed conflict.

Such conflicts also drive a surge in hacktivist activity against the perceived allies of the warring parties. These hacktivist campaigns typically seek to exert political pressure or amplify narratives that align with one side of the conflict.

[2] https://strikeready.com/blog/ru-apt-targeting-energy-infrastructure-unknown-unknowns-part-3/

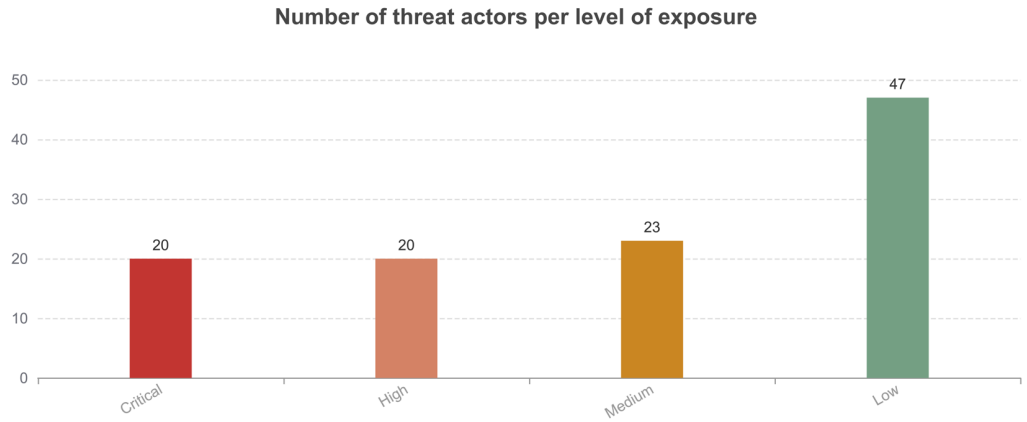
For example, in October, pro-Russia supposed hacktivists claimed DDoS attacks against Belgian government websites amid ongoing conversations relating to Belgium's intention to purchase and donate weapons to Ukraine.[3]

4 Threat actors

In 2024, **we identified at least 110 malicious actors who engaged in MAIs against Union entities or those in their vicinity.** The level of exposure of Union entities to these actors ranged from critical to low.

- **Critical: 20 threat actors conducted cyberattacks that impacted or successfully breached some Union entities.** We were able to link some of these breaches to known threat actors, while others remained unidentified[4]. Some of these unidentified threat groups may have partial overlap.
- High: 20 threat actors targeted Union entities or their vicinity, but failed to intrude any Union entity system. For example, often these threat actors sent spearphishing e-mails that were detected and blocked by Union entities, or the adversaries attempted but failed to exploit exposed software products.
- Medium: We detected 23 threat actors attempting to scan the networks of Union entities. However, we saw no signs of a breach or exploitation.
- Low: We observed 47 threat actors targeting the vicinity of Union entities, such as European countries, sectors of interest, or the supply chain, such as software products or providers used by Union entities. We did not detect any sightings in our constituency.

> Note
> Certain threat actors have engaged in several activities that have led to different levels of exposure. For example, an unsuccessful spearphishing attack (high exposure) and, at a different time, active scanning (medium exposure). In such a case, we have assigned the highest threat level to that actor (high exposure).



Critical exposure

Out of the 20 threat actors to which Union entities had critical exposure in 2024, we highlight two hereunder.

UTA-62. An unknown threat actor, which we track as UTA-62, successfully exploited a zero-day vulnerability in a Union entity's FortiGate Manager, a network management and security operation solution.

UTA-63. Another unknown threat actor, UTA-63, conducted a search engine optimisation (SEO) poisoning attack on a Union entity's web application. Containment measures were swiftly taken, resulting in a temporary service disruption.

[3] https://www.vrt.be/vrtnws/en/2024/10/07/pro-russian-group-launches-cyber-attack-on-belgian-cities-and-pr/
[4] In this case, we refer to them as as Unidentified Threat Actors (UTAs) and we give them a number such as UTA-62.

High exposure

Out of the 20 threat actors to which Union entities had high exposure in 2024, we highlight four below.

APT29. APT29 sent spearphishing e-mails to individuals in government, academia, defence, and non-governmental organisations.[5] The e-mails were highly targeted, using social engineering lures relating to Microsoft, Amazon Web Services (AWS), and the Zero Trust concept.

UAC-0050. UAC-0050 is an APT group primarily focused on targeting Ukrainian entities, as well as organisations throughout Europe involved in issues related to Russia's war in Ukraine.[6]

Kimsuky. Kimsuky[7] is a North Korea-linked cyberespionage group that targets government, military and diplomatic entities, particularly those working on matters involving the Korean peninsula. In 2024, the actor targeted an entity that works closely with Union entities, specifically attempting to compromise an e-mail account. The threat actor also sent social engineering phishing e-mails to at least three Union entities, but none of them led to any compromise or impact on the target side.

Sandworm. In the first half of October, Sandworm sent spearphishing e-mails to entities in the European energy sector.[8] An organisation working closely with Union entities was used as a lure. However, no breaches were detected in our constituency. This threat actor is known for its sophisticated destructive attacks. This recent targeting is notable because there had been very few previous attacks by this threat actor in our vicinity.

Medium exposure

Out of the 23 threat actors to which Union entities had medium exposure in 2024, we highlight two hereunder.

Callisto. In 2024, Callisto continued its cyber activities, targeting civil society, journalists, think tanks, defence, and non-governmental organisations across the US[9] and Europe[10]. Specifically, Callisto conducted credential-phishing operations in Europe for information-gathering activity in the vicinity of Union entities.

Mustang Panda. Mustang Panda continued to conduct spearphishing campaigns in Europe in the vicinity of Union entities, but was less prevalent in targeting them than in previous years. Notably, Mustang Panda zeroed in on the European cargo shipping industry, allegedly gaining initial access through removable media.[11]

Low exposure

We detected 47 threat actors targeting the vicinity of Union entities. This included entities located in European countries, and operating in sectors of interest. We will not name them, but we note that this is almost double the number from last year.

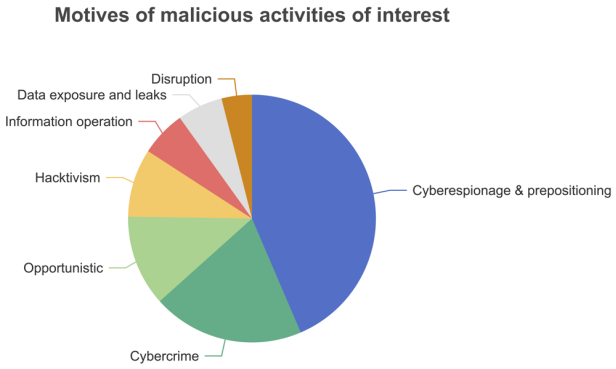
Motives

When examining malicious activities of interest, we categorise each attack based on the inferred motives of the threat actor. While this classification is not an exact science, it takes into account several factors, including the apparent objective of the attack, the identity of the attacker, the profile of the targeted victims, and the sophistication and persistence of the observed behaviour.

In 2024, a staggering 44% of the recorded activity was classified as cyberespionage and/or prepositioning. We categorise attacks in this way because they are typically carried out by state-backed threat actors. **When these actors infiltrate a target, they often initially exfiltrate data, and try to maintain long-term covert access without drawing much attention to themselves.**

Interestingly, we discovered that 20% of MAI activity was classified as cybercrime, while 12% was deemed opportunistic.

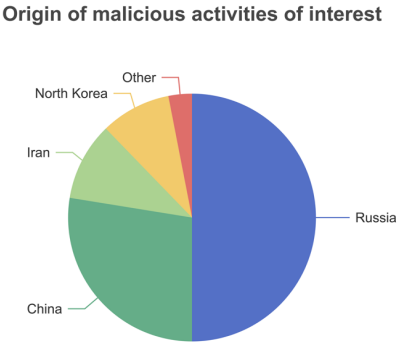
[5] https://www.microsoft.com/en-us/security/blog/2024/10/29/midnight-blizzard-conducts-large-scale-spear-phishing-campaign-using-rdp-files/
[6] https://socprime.com/blog/uac-0050-financially-motivated-attack-detection/
[7] https://www.cisa.gov/news-events/cybersecurity-advisories/aa20-301a
[8] https://strikeready.com/blog/ru-apt-targeting-energy-infrastructure-unknown-unknowns-part-3/
[9] https://blogs.microsoft.com/on-the-issues/2024/10/03/protecting-democratic-institutions-from-cyber-threats/
[10] https://www.consilium.europa.eu/en/press/press-releases/2024/06/24/cyber-attacks-six-persons-added-to-eu-sanctions-list-for-malicious-cyber-activitiescyberattacks-against-eu-member-states-and-ukraine/
[11] https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q2-2024-q3-2024.pdf



Origin

Identifying an adversary's geographic origins can be quite challenging. We rely on attribution by reliable sources in order to link a particular MAI to its country of origin, whenever possible.

In this document, we will only consider cases where we could determine the origin of a threat actor and where the information was available to us. **Among the cases where we could determine the origin, we discovered that attacks could be linked to at least six different countries. We found that 50% likely originated from Russia, and 28% from China**, followed by Iran and North Korea respectively.

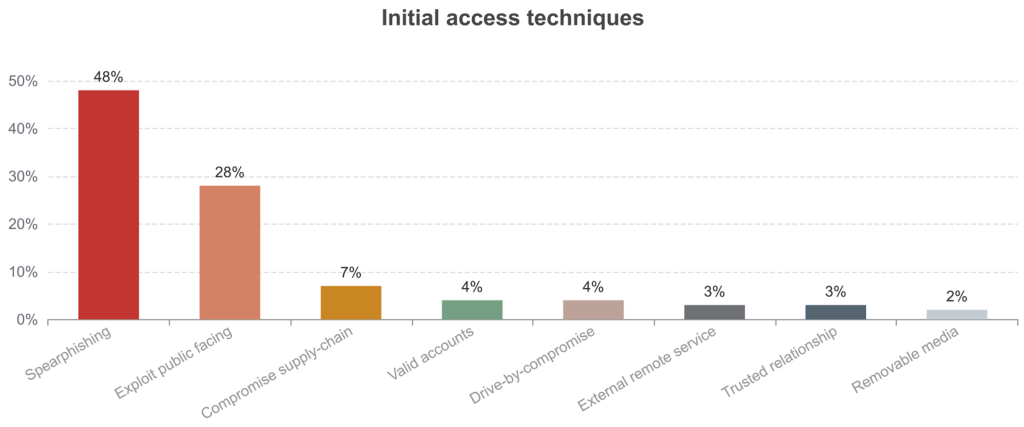


5 Techniques

During our analysis of malicious activities of interest, we identified several recurring techniques that played a significant role in shaping the 2024 threat landscape from our standpoint. Rather than providing an exhaustive list of all observed techniques, we highlight below a select few that we assess as particularly impactful.

Initial access techniques

Within our MAI dataset, we noticed that **threat actors most often resorted to spearphishing, to the exploitation of public-facing software, and to supply-chain compromises as initial access techniques.** However, they do not necessarily correlate with high success rates. Interestingly, spearphishing, the most prevalent method, does not seem to result in substantial success compared to the number of attempted attacks.



In 2024, Union entities experienced at least 15 significant incidents. **In five of these cases, initial access was achieved through the exploitation of a zero-day vulnerability.** The remaining 10 incidents involved various initial access vectors, including: n-day vulnerability exploitation in seven cases, misconfiguration abuse in one case, and a spearphishing e-mail in another. In one significant incident, the initial access technique could not be determined.

Use of Operational Relay Box networks

Operational Relay Box (ORBs) networks are collections of compromised devices. They are mainly made up of a combination of vulnerable and often end-of-life SOHO routers, IP cameras, and VPS nodes.

An example is consumer routers, which are particularly valuable to attackers because their IP addresses often belong to trusted ranges, complicating the identification of malicious intentions.

Threat actors use ORBs to browse, conduct reconnaissance, scan for or exploit vulnerabilities. ORBs are often used in parallel with commercial VPN services offering anonymisation. Some well-known ORB networks are being leveraged by Chinese threat actors such as GhostVPN and ZRNet. For example, in 2024, China-linked[12] Volt Typhoon exploited legacy vulnerabilities in Cisco and Netgear ProSafe routers to establish ORB networks such as the KV-Botnet[13].

Several cyberespionage actors use ORBs to obscure the true origin of their activities, which further complicates detection and attribution.

Exploiting public-facing applications and edge devices

APT groups frequently target internet-facing systems and edge devices such as VPN appliances, firewalls, load balancers, and network management solutions to gain initial access.

In 2024, sophisticated adversaries leveraged, among others, vulnerabilities in Fortinet FortiGate, Cisco ASA, Ivanti Connect Secure, Palo Alto GlobalProtect, and Citrix ADC to infiltrate corporate networks.

These edge devices are particularly attractive targets because they often lack endpoint detection and response (EDR) capabilities and serve as entry points to critical infrastructure within networks.

For example, in January 2024, a widespread campaign targeted the Ivanti Connect Secure VPN, exploiting a vulnerability that allowed an unauthenticated threat actor to execute arbitrary commands on the appliance with elevated privileges.[14]

Adversary-in-the-Middle attacks

Adversary-in-the-Middle (AitM) attacks are a highly effective technique used by APTs to intercept, manipulate, and hijack communication sessions between a victim and a legitimate service.

[12] https://www.justice.gov/archives/opa/pr/us-government-disrupts-botnet-peoples-republic-china-used-conceal-hacking-critical
[13] https://www.bleepingcomputer.com/news/security/volt-typhoon-rebuilds-malware-botnet-following-fbi-disruption/
[14] https://cloud.google.com/blog/topics/threat-intelligence/investigating-ivanti-zero-day-exploitation/?hl=en

Unlike traditional Man-in-the-Middle (MitM) attacks, which primarily rely on network-layer interception, AitM techniques have evolved to target web-based authentication flows, session tokens, and encrypted communications, allowing attackers to bypass Multi-Factor Authentication (MFA) and other security controls.

AitM attacks enable session hijacking, real-time credential interception, and browser-in-the-browser (BitB) techniques to steal authentication tokens, providing persistent access to cloud environments.

By intercepting traffic in real-time, APTs can manipulate authentication processes, harvest session cookies, and execute advanced account takeovers, effectively enabling them to infiltrate even highly secure enterprise networks.

In June 2024, cybersecurity researchers identified a novel AiTM phishing kit named Mamba 2FA, designed to intercept and relay multi-factor authentication processes.[15]

Living-off-the-Land techniques

APTs regularly minimise their footprint using legitimate systems and tools available on the victim machine, such as PowerShell, WMI, CertUtil, and Rundll32 instead of deploying custom malware.

This Living-off-the-Land (LoL) approach allows adversaries to blend in with normal system activity, evade signature-based detection, and maintain persistent access while minimising forensic artefacts.

By abusing trusted system utilities, APTs can execute commands, move laterally, exfiltrate data, and establish persistence, all while bypassing traditional security defences and endpoint detection mechanisms.

For example, Volt Typhoon uses LoL techniques when they exploit legitimate system tools and processes to carry out malicious activities, thereby minimising their footprint and evading detection. By leveraging standard administrative utilities and avoiding custom malware, Volt Typhoon effectively blends into normal network operations.[16]

Cloud-based persistence & API abuse

With the rapid adoption of cloud technologies, APTs have shifted their focus to exploiting weak API security, misconfigured Identity and Access Management (IAM) policies, and exposed cloud secrets.

Threat actors could abuse overly permissive IAM roles, leverage stolen API keys, and exploit misconfigured storage buckets to move laterally within cloud environments, escalate privileges, and exfiltrate sensitive data.

Additionally, APTs could take advantage of cloud-based identity federation weaknesses, OAuth token theft, and serverless function vulnerabilities, allowing them to persist within compromised cloud infrastructures while evading traditional security controls.

For example, in December 2024, the US government experienced a significant security breach whereby attackers exploited vulnerabilities in BeyondTrust's remote technical support software, obtaining an API key that gave them access to government workstations.[17]

This incident underscores the risks associated with cloud-based persistence and API abuse, as threat actors leveraged legitimate software tools to maintain unauthorised access and exfiltrate sensitive information.

Supply-chain compromise

APT groups infiltrate third-party vendors, software providers, and managed service providers (MSPs) as strategic entry points to reach their ultimate targets.

By compromising trusted supply-chain partners, software update mechanisms, and widely used enterprise applications, adversaries can distribute malware at scale, inject backdoors into legitimate software, and bypass traditional security defences.

This technique enables them to gain privileged access to multiple downstream victims, often remaining undetected for extended periods of time.

[15] https://blog.sekoia.io/mamba-2fa-a-new-contender-in-the-aitm-phishing-ecosystem/
[16] https://www.picussecurity.com/resource/blog/volt-typhoon-living-off-the-land-cyber-espionage
[17] https://legacy.www.documentcloud.org/documents/25472740-letter-to-chairman-brown-and-ranking-member-scott/

In May 2024, a significant supply-chain attack was uncovered involving the exploitation of a backdoor in the Justice AV Solutions Viewer software, identified as CVE-2024-4978.[18] The vulnerability allowed attackers to compromise the software, which is widely used in the justice sector, and inject malicious code into the affected systems.

This attack, which affected several organisations, highlights the risks posed by compromised software updates and underscores the importance of securing supply chains, particularly for sensitive government and legal sectors.

6 Service providers: prime targets for threat actors

In 2024, we observed that **malicious activities of interest recurrently involved abuse of prominent service providers in the vicinity of Union entities.**

By targeting service providers, threat actors can exploit trusted connections to reach downstream clients.

Rather than providing an exhaustive list of all observed types of provider abuse, we highlight below a select few types of abuse of providers that we assess as particularly impactful.

Remote access & security software providers

Vendors offering remote access tools, endpoint security, or VPN services are vital for many organisations. Threat actors often target these platforms, aiming to exploit their privileged positioning within corporate networks. A few examples from 2024 below.

- TeamViewer suffered unauthorised access to employee credentials, though no suspicious activity was reportedly found in production systems. The incident, attributed to APT29 (Midnight Blizzard), highlighted credential theft risks for providers with large user bases.[19]
- Following a CrowdStrike software update glitch, malicious actors sent fraudulent e-mails offering bogus fixes which installed remote-access malware and data wipers. The incident underscored broader supply-chain risks of security software updates.[20]

Software & cloud providers

Software vendors and cloud service operators were frequently targeted in 2024. This is significant as a successful compromise of popular platforms can generate wide-reaching impact. A few examples include:

- A DDoS attack on July 30 caused ten hours of downtime for Microsoft Azure, with Microsoft's own defences amplifying disruptions.[21]
- An attack on the language course company Altissia exposed e-mails, raising concerns over potential further data leaks and the security of language-learning platforms.[22]

Telecommunications & Internet Service Providers

Telecommunication and Internet Service Providers (ISPs) control vast networks and often store personal data for millions of users, factors that sustained their appeal to threat actors in 2024. A few examples below.

- China-linked threat actor Salt Typhoon conducted a widespread cyberespionage campaign targeting at least nine US telecommunications companies, including major providers like AT&T and Verizon.[23]
- Orange Spain reportedly experienced a service disruption following unauthorised access to a key online account interface.[24]
- Free, a major ISP in France, disclosed a breach exposing personal data belonging to around 19.2 million clients.[25] The data set for sale, estimated at 43.6 GB, allegedly included more than 5.11 million IBANs.

[18] https://www.rapid7.com/blog/post/2024/05/23/cve-2024-4978-backdoored-justice-av-solutions-viewer-software-used-in-apparent-supply-chain-attack/
[19] https://www.teamviewer.com/en/resources/trust-center/security-bulletins/tv-2024-1005/
[20] https://www.csa.gov.sg/alerts-and-advisories/alerts/al-2024-091
[21] https://azure.status.microsoft/en-us/status/history/#incident-history-collapse-KTY1-HW8
[22] https://www.luxtimes.lu/luxembourg/luxembourg-learning-app-hit-by-data-breach/18676097.html
[23] https://www.politico.com/news/2024/12/27/chinese-hackers-telco-access-00196082
[24] https://www.reuters.com/business/media-telecom/orange-suffers-cyber-attack-affecting-clients-internet-access-spain-2024-01-03/
[25] https://www.lemonde.fr/pixels/article/2024/10/26/free-porte-plainte-apres-une-cyberattaque-sur-les-donnees-personnelles-de-ses-abonnes-dont-l-ampleur-reste-inconnue_6360440_4408996.html

7 Software

In 2024, **exploitation of vulnerable internet-facing software products remained among the primary initial access vectors used in the vicinity of Union entities.**

We observed 110 software products being targeted in our vicinity. Below we highlight a non-exhaustive list of abused software types which we consider reflective of the 2024 threat landscape from our viewpoint.

- Exploitation of vulnerable internet-facing software products
- Supply-chain attacks leveraging trojanised software products
- Fake versions of software products
- Abuse of public repositories used for programming languages
- Abuse of misconfigurations by threat actors.

Notable software exploitations

While all of the above types of attack patterns against software products were observed in 2024, **our monitoring efforts focused on exploitation of internet-facing applications as we deem it the most relevant software threat for Union entities**.

Below is a non-exhaustive list of software exploitations. Notably, these are widely adopted products, making the exploitation of their vulnerabilities a risk for Union entities.

Adversaries actively exploited multiple high-impact vulnerabilities across Microsoft products and protocols. These included Windows, NTLMv2, Microsoft 365, Office, and SmartScreen. The exploited vulnerabilities enabled attackers to execute remote code, bypass authentication mechanisms, and steal credentials, often as part of cyberespionage or cybercrime campaigns. Notable examples include the following.

- Remote code execution and privilege escalation vulnerabilities[26, 27, 28] in Windows were widely reported of having been exploited to compromise systems across different environments.
- Authentication bypass flaws[29, 30] in NTLMv2 allowed threat actors to evade authentication checks, particularly in legacy deployments.
- Credential harvesting vulnerabilities[31, 32] in Microsoft 365 and Office were leveraged in targeted cyber operations to extract sensitive user data.
- SmartScreen bypass methods were facilitated by multiple vulnerabilities[33, 34], often exploited through malicious e-mail attachments in spearphishing attacks.

Ivanti's Connect Secure and Policy Secure solutions were targeted by adversaries, with several high-impact vulnerabilities exploited in the wild. These flaws enabled attackers to achieve remote code execution, bypass authentication, and escalate privileges, often as part of cyberespionage and cybercrime campaigns against public-facing Ivanti appliances.

- Remote code execution vulnerabilities[35] in unpatched Ivanti devices allowed adversaries to gain unauthorised access and execute arbitrary code.
- Authentication bypass and privilege escalation vulnerabilities[36, 37, 38] were leveraged in targeted attacks, compromising Ivanti appliances in specific configurations.

[26] https://nvd.nist.gov/vuln/detail/CVE-2024-49039
[27] https://nvd.nist.gov/vuln/detail/CVE-2024-43451
[28] https://www.cert.europa.eu/publications/security-advisories/2024-067
[29] https://nvd.nist.gov/vuln/detail/CVE-2024-30040
[30] https://nvd.nist.gov/vuln/detail/CVE-2024-30051
[31] https://nvd.nist.gov/vuln/detail/CVE-2024-26234
[32] https://nvd.nist.gov/vuln/detail/CVE-2024-29988
[33] https://nvd.nist.gov/vuln/detail/CVE-2024-21412
[34] https://nvd.nist.gov/vuln/detail/CVE-2024-21351
[35] https://nvd.nist.gov/vuln/detail/CVE-2023-46805
[36] https://nvd.nist.gov/vuln/detail/CVE-2024-21887
[37] https://nvd.nist.gov/vuln/detail/CVE-2024-21888
[38] https://nvd.nist.gov/vuln/detail/CVE-2024-21893

Apple disclosed multiple vulnerabilities affecting iOS, iPadOS, macOS, and tvOS, some of which were actively exploited by adversaries. These vulnerabilities enabled remote code execution, privilege escalation, and data exfiltration through malicious applications or links.

- Remote code execution and privilege escalation vulnerabilities[39, 40, 41] were exploited in Apple operating systems, compromising device security and user data.
- Some threat campaigns leveraged these flaws to deploy spyware or extract personal information from targeted devices.

Google identified multiple Chrome vulnerabilities that were actively exploited by attackers. These flaws, affecting rendering and sandbox mechanisms, enabled remote code execution and privilege escalation.

- Remote code execution vulnerabilities[42, 43, 44] in Chrome allowed adversaries to compromise users through maliciously crafted web pages. Threat actors leveraged these exploits to steal personal data or escalate privileges by bypassing Chrome's security mechanisms.

Palo Alto Networks identified multiple vulnerabilities in PAN-OS that were actively exploited by adversaries. These flaws allowed attackers to execute remote code, escalate privileges, and compromise unpatched firewalls.

- Remote code execution and privilege escalation vulnerabilities[45, 46, 47] in PAN-OS were exploited to deploy malicious code or exfiltrate sensitive data.

Finally, several other vendors suffered serious vulnerabilities that were actively exploited in the wild. They affected Citrix Netscaler, Cisco security appliances, MOVEit by Progress Software, and PHP. These flaws allowed unauthorised access, remote code execution, privilege escalation, and data exfiltration.

- Citrix Netscaler products (ADC, Gateway) contained vulnerabilities[48, 49] that allowed unauthorised access and remote code execution in specific deployments.
- Cisco Adaptive Security Appliance and Firepower Threat Defense solutions were affected by privilege escalation vulnerabilities[50] which adversaries leveraged for further access.
- Progress Software's MOVEit contained a flaw[51] which attackers exploited to exfiltrate personal data in targeted campaigns.
- PHP was impacted by a vulnerability[52] which permitted attackers to execute arbitrary commands on compromised systems.

The non-exhaustive table below is a list of notable exploited vulnerabilities per vendor. The list includes CVEs that were widely exploited in our vicinity and that reflect the 2024 threat landscape as we see it.

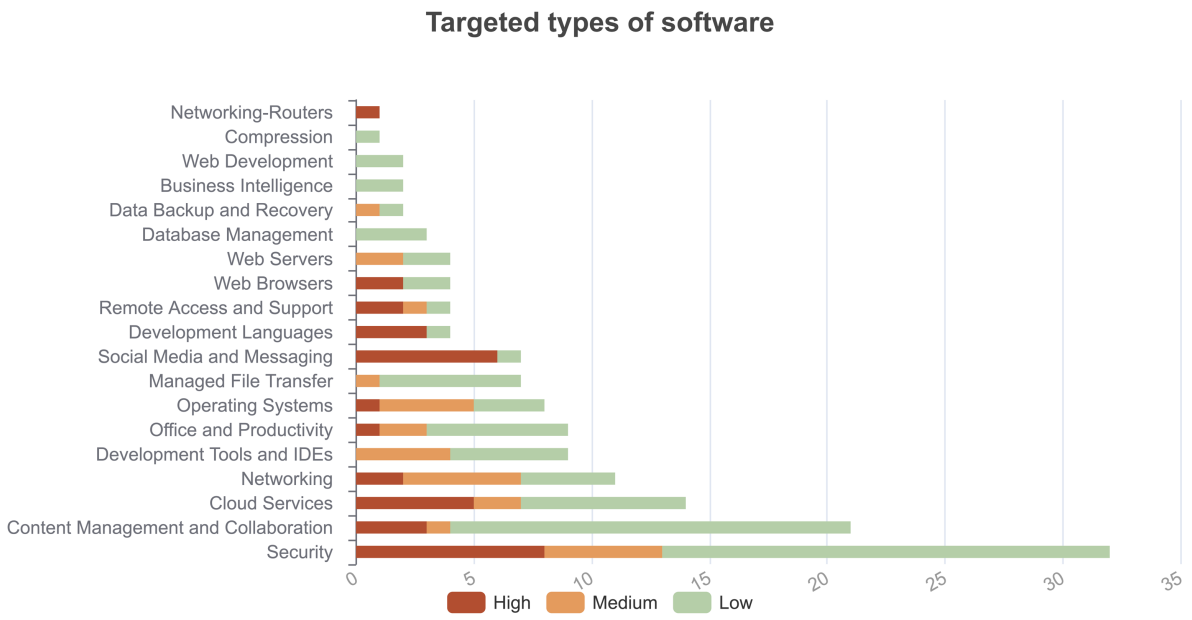
[39] https://nvd.nist.gov/vuln/detail/CVE-2024-23225
[40] https://nvd.nist.gov/vuln/detail/CVE-2024-23296
[41] https://nvd.nist.gov/vuln/detail/CVE-2024-23222
[42] https://nvd.nist.gov/vuln/detail/CVE-2024-7971
[43] https://nvd.nist.gov/vuln/detail/CVE-2024-7965
[44] https://nvd.nist.gov/vuln/detail/CVE-2024-4947
[45] https://nvd.nist.gov/vuln/detail/CVE-2024-0012
[46] https://nvd.nist.gov/vuln/detail/CVE-2024-9474
[47] https://nvd.nist.gov/vuln/detail/CVE-2024-3400
[48] https://nvd.nist.gov/vuln/detail/CVE-2023-6548
[49] https://nvd.nist.gov/vuln/detail/CVE-2023-6549
[50] https://nvd.nist.gov/vuln/detail/CVE-2024-20353
[51] https://nvd.nist.gov/vuln/detail/CVE-2024-5806
[52] https://nvd.nist.gov/vuln/detail/CVE-2024-4577

Vendor	Product	Notable CVE
Microsoft	Windows, NTLMv2, 365, Office, SmartScreen	CVE-2024-49039, CVE-2024-43451, CVE-2024-38080, CVE-2024-38112, CVE-2024-30040, CVE-2024-30051, CVE-2024-26234, CVE-2024-29988, CVE-2024-21412, CVE-2024-21351
Palo Alto Networks	PAN-OS	CVE-2024-0012, CVE-2024-9474, CVE-2024-3400
Apple	iOS, iPadOS, macOS, tvOS	CVE-2024-23225, CVE-2024-23296, CVE-2024-23222
Google	Chrome	CVE-2024-7971, CVE-2024-7965, CVE-2024-4947
Citrix Netscaler	ADC, Gateway	CVE-2023-6548, CVE-2023-6549
Ivanti	Connect Secure, Policy Secure	CVE-2023-46805, CVE-2024-21887, CVE-2024-21888, CVE-2024-21893
Cisco	Adaptive Security Appliance (ASA), Firepower Threat Defence (FTD)	CVE-2024-20353
Progress Software Corporation	MOVEit	CVE-2024-5806
PHP Group	PHP	CVE-2024-4577

Types of abused software

Throughout 2024, we observed a wide range of software being subjected to attacks, with different attackers targeting various products. This section categorises these affected products, analysing which ones are particularly attractive for threat actors.

The diagram below shows the number of products in each category, as well as the exploitation level, based on our MAI dataset. When a software product was targeted in significant attacks, we considered the exploitation level as high. When a software product was targeted in at least two attacks in our vicinity, we considered the exploitation level as medium. When a software product was targeted in one attack in our vicinity, we considered the exploitation level as low.



Security software

Throughout 2024, many vulnerabilities emerged in firewalls and virtual private networks, giving threat actors opportunities to gain unauthorised access, install malware, and move laterally within target networks.

- In January, Ivanti disclosed two zero-days affecting Ivanti Pulse Connect Secure VPN.[53]
- At the end of the year, a campaign targeted exposed Fortinet FortiGate management interfaces, allowing unauthorised administrative logins, new account creation, and SSL VPN access, followed by credential theft for lateral movement.[54]

Content management and collaboration

Threat actors persistently exploited collaboration platforms and e-mail systems. These attacks often leveraged cross-site scripting or spearphishing to infiltrate enterprises handling extensive data flows.

- Since at least May, an APT exploited Roundcube vulnerabilities[55] in Ukrainian government environments and European defence entities, switching to Horde for exploitation of a cross-site scripting vulnerability in at least one instance.[56]
- In January, Atlassian Confluence instances were compromised using a template injection[57] by multiple threat actors in opportunistic and targeted attacks.[58] Additionally, the same vulnerability was exploited using the Godzilla fileless backdoor in August.[59]

Cloud services

Threat actors increasingly focused on misconfigured or unpatched cloud platforms, using credential phishing and malicious packages to bypass security. Several zero-day exploits also appeared in appliances managing enterprise cloud operations.

- In February, a cloud account takeover campaign targeting Microsoft Azure compromised hundreds of user accounts including those of senior executives. Threat actors used credential phishing with personalised lures in shared documents.[60]
- In November, a malicious Python package, named Fabrice, stole Amazon Web Services credentials across Windows and Linux, using a platform-agnostic trigger.[61]
- Ivanti identified three zero-days[62,63,64] in its Cloud Service Appliance, confirming active exploitation since at least September.[65]

Networking

Switches, routers, and configuration tools remained prime targets for intrusions. Threat actors seeking persistent access or lateral movement often exploited core network devices to harvest credentials or implant custom malware.

- In April, Velvet Ant exploited a zero-day vulnerability[66] in Cisco NX-OS, acquiring administrative credentials and installing a custom, previously unseen root-level malware on Nexus switches.[67]
- In October, unknown threat actors abused Palo Alto Networks Expedition vulnerabilities, delivering unauthenticated HTTP requests to steal usernames, passwords, and API keys for PAN-OS firewalls, occasionally installing crypto mining malware.[68]

[53] https://www.volexity.com/blog/2024/01/10/active-exploitation-of-two-zero-day-vulnerabilities-in-ivanti-connect-secure-vpn/
[54] https://thehackernews.com/2025/01/zero-day-vulnerability-suspected-in.html
[55] https://nvd.nist.gov/vuln/detail/CVE-2023-43770
[56] https://fieldeffect.com/blog/roundcube-webmail-flaw-actively-exploited
[57] https://nvd.nist.gov/vuln/detail/CVE-2023-22527
[58] https://www.trendmicro.com/en_us/research/24/b/unveiling-atlassian-confluence-vulnerability-cve-2023-22527--und.html
[59] https://www.trendmicro.com/en_be/research/24/h/godzilla-fileless-backdoors.html
[60] https://www.proofpoint.com/us/blog/cloud-security/community-alert-ongoing-malicious-campaign-impacting-azure-cloud-environments
[61] https://socket.dev/blog/malicious-python-package-typosquats-fabric-ssh-library
[62] https://nvd.nist.gov/vuln/detail/CVE-2024-9379
[63] https://nvd.nist.gov/vuln/detail/CVE-2024-9380
[64] https://nvd.nist.gov/vuln/detail/CVE-2024-9381
[65] https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-CSA-Cloud-Services-Appliance-CVE-2024-9379-CVE-2024-9380-CVE-2024-9381?language=en_US
[66] https://nvd.nist.gov/vuln/detail/CVE-2024-20399
[67] https://eclypsium.com/blog/squashing-the-velvet-ant-how-eclypsium-protects-cisco-nx-os-and-f5-load-balancers/

Development tools

Malicious actors frequently compromised development environments and code repositories, inserting malware into legitimate extensions or repository projects.

- In June, security researchers discovered harmful Visual Studio Code extensions, including a trojanised Dracula Official theme used to infiltrate over 100 organisations.[69]
- The Stargazers Ghost network on GitHub lured victims on Discord to download scripts hosting stealer malware, as reported by security firm Checkpoint in July 2024.[70]

Operating systems

Zero-day exploits in mobile and desktop platforms repeatedly surfaced throughout 2024, targeting memory handling, pointer authentication, and browser components. These flaws often allowed data theft.

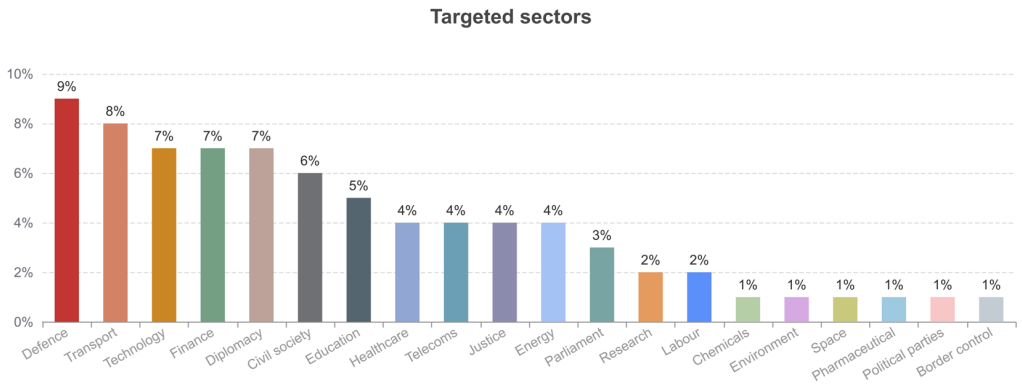
- An authentication bypass vulnerability [71] in iOS, iPadOS, macOS, tvOS, and watchOS permitted arbitrary read and write operations, prompting official advisories and widespread patching.
- A threat actor introduced WolfsBane, a Linux backdoor linked to the Gelsemium group, featuring stealth techniques and rootkit components.[72]

8 Sectors

In our analysis of malicious activities of interest, we categorised targeted entities into distinct sectors, excluding public administration. We did this because most targets in our area are from the public sector, in addition to being classified in other sectors.

It is important to note that the targeting of a particular entity within a sector does not necessarily indicate a deliberate focus on that sector by the threat actor.

Such incidents may be opportunistic or coincidental. However, when assessing sectoral targeting from a statistical perspective, particularly in relation to the sophistication of the threat actor, valuable insights can emerge.



The defence sector was the most targeted sector within our dataset of malicious activities of interest. The ongoing conflicts, such as Russia's invasion of Ukraine and the Israel-Hamas conflict, have increased the attractiveness of this sector for threat actors. The defence sector includes both public and private entities, including defence ministries and private companies engaged in weapons manufacturing.

Cyberespionage threat actors likely aimed to steal sensitive information related to weapon development, monitor military communications, and track arms shipments. For example, in September, APT group Kimsuky reportedly targeted a German defence company specialised in the production of advanced military systems.[73]

[69] https://www.bleepingcomputer.com/news/security/malicious-vscode-extensions-with-millions-of-installs-discovered/
[70] https://research.checkpoint.com/2024/stargazers-ghost-network/
[71] https://nvd.nist.gov/vuln/detail/CVE-2022-48618
[72] https://www.welivesecurity.com/en/eset-research/unveiling-wolfsbane-gelsemiums-linux-counterpart-to-gelsevirine/
[73] https://www.spiegel.de/netzwelt/web/diehl-defence-hacker-aus-nordkorea-zielen-auf-mitarbeiter-des-ruestungskonzerns-a-8735f440-670c-40df-9e46-06c620fe9be6

We note that entities in the transportation sector were the second most frequently targeted in incidents categorised as malicious activities of interest. This broad sector includes organisations involved in maritime, air, and rail transportation, as well as courier and postal services.[74]

These entities were frequently the target of cyberespionage groups, cybercrime groups and supposed hacktivist groups, particularly during election periods and high-profile events. It is likely that this was done to amplify the perception of disorder in the public eye.

For example, the APT group Mustang Panda conducted a cyberespionage campaign targeting the European cargo shipping industry throughout the first half of 2024, deploying its Korplug loader.[75]

The technology sector ranked third among those most targeted. It is likely that malicious actors are drawn to this industry due to its role in the supply chain, seeking to infiltrate downstream clients through targeted attacks or by stealing their login credentials.

For instance, in April, it was revealed that Sisense, a data analytics company, suffered a data breach that may have exposed user credentials.[76]

The finance sector was frequently targeted with malicious activities of interest, often by supposed hacktivist groups reacting to perceived support for Ukraine. This highlights the sector's prominence as a high-profile target in the ongoing information warfare landscape.

For example, in July, the Czech Republic signed a security agreement with Ukraine[77], which prompted DDoS attacks by pro-Russian supposed hacktivists such as NoName057(16) against entities in the Czech finance sector.[78]

Finally, entities in the diplomatic sphere, such as Ministries of Foreign Affairs and embassies, remained a focal point of cyberespionage campaigns in 2024.

For example, GoldenJackal[79] reportedly exploited bespoke malware to infiltrate air-gapped systems, targeting embassies and other governmental entities with sophisticated techniques tailored to bypass security defences.

Another example is MirrorFace[80], who allegedly carried out a cyberespionage operation against a European diplomatic organisation.

[74] https://www.ft.com/content/c05c9b21-77bd-4ddf-82e1-02356acf0899
[75] https://www.eset.com/fileadmin/ESET/US/B2B_Resource_centre/reports/APT_Activity_Report_Q2_2024-Q3_2024.pdf
[76] https://www.cisa.gov/news-events/alerts/2024/04/11/compromise-sisense-customer-data
[77] https://vlada.gov.cz/scripts/detail.php?id=214687&tmplid=766
[78] https://nukib.gov.cz/download/publications_en/Cyber-Security-Incidents-from-the-NUKIB-s-Perspective-August-2024.pdf
[79] https://www.welivesecurity.com/en/eset-research/mind-air-gap-goldenjackal-gooses-government-guardrails/
[80] https://therecord.media/russia-aligned-hackers-target-european-and-iranian-embassies-cyber-espionage

This page is left intentionally blank.

10 years

CERT-EU

THINK CONSTITUENT
CREATE VALUE

https://cert.europa.eu

services@cert.europa.eu

infosec.exchange/@cert_eu