CERT-EU

THREAT LANDSCAPE REPORT

2023
YEAR REVIEW

v1.1 - FEBRUARY 2024

TLP:CLEAR | NO LIMIT ON DISCLOSURE

This document can be disclosed to the world, there is no limit on disclosure of this information.
CERT-EU, the cybersecurity service for Union entities

Table of Contents

Introduction

We are monitoring the cyber threat landscape to help the European Union institutions, bodies, offices and agencies (Union entities), detect and protect against cyber attacks. Our monitoring focuses on attacks targeting Union entities or their vicinity.

We consider a malicious activity is in the *vicinity* of Union entities when some of the following factors are combined:

- The activity is targeting sectors of interest, entities located in the EU or in other European countries, software products or service providers known to be used by Union entities.
- The activity is a large-scale campaign possibly affecting any organisation worldwide.
- The activity is attributed to a well-resourced threat actor known to have targeted Union entities (we label it a Top Threat Actor).

We name *malicious activities of interest* (MAIs) the attacks targeting Union entities or their vicinity.

In 2023, we analysed 602 MAIs. For each MAI, we focus on the following key characteristics:

- victimology information (targeted sectors, countries, or software products)
- tactics, techniques and procedures (TTPs)
- malware strains or tools
- exploited vulnerabilities
- attribution
- indicators of compromise (IoCs) and detection rules.

While this analysis is essential to help Union entities detect threats and protect against them, it also provides us with a solid basis to identify patterns and trends in the threat landscape. This document presents a selection of notable characteristics of the 2023 threat landscape.

In the chapter "Threat actor activity", we provide an analysis of the active attackers looking at their likely motives, origins, and at the level of threat they posed to Union entities or their vicinity.

In the chapter "Software products", we report our observations related to the most targeted software products and we analyse how the exploitation of internet-facing products has been a predominant initial access method.

In the chapter "Spearphishing", we share our analysis of notable spearphishing techniques and how they were used against Union entities or their vicinity.

In the chapter "Sectors", we present the most targeted sectors and we analyse their attractiveness for attackers.

In the chapter "Ransomware", we focus on what has been the most significant cybercrime activity, in 2023, and how it has evolved recently.

Key Findings

- We noticed 80 threat actors active against Union entities or their vicinity, with critical exposure to 18, high exposure to 17, medium exposure to 21 and low exposure to 24. The motive of these threat actors was, in descending order of importance, cyberespionage, hacktivism, cybercrime or information operations.
- When it was possible to determine their origin, and based on information from reliable sources, we noticed that threat actors active against Union entities or their vicinity were linked mainly with two countries: People's Republic of China (hereafter China) and the Russian Federation (hereafter Russia). However, we also noticed a diversification in the origin of cyber attacks and the role played by private sector offensive actors (PSOAs).
- We noticed threat actors targeting 104 software products in 241 distinct malicious activities of interest. These targeting took different forms including exploitation of internet-facing vulnerable software products, supply-chain attacks leveraging trojanised software products, fake version of software products, abuse of public repositories used for programming languages, misuse by threat actors, or other forms of exploitation after initial access.
- There were significant attacks against products in various categories, including networking (Fortinet, Cisco or Citrix products for example), development tools and IDEs (for example JetBrains or Python libraries), security (such as 1Password or LastPass password managers), content management or collaboration tools (WordPress, Altassian Confluence for example), and cloud services (such as Azure or JumpCloud).
- Spearphishing remained the predominant initial access method for state-sponsored and cybercrime groups seeking to infiltrate target networks. We have analysed 177 such attacks, that we found notable. We observed that a number of adversaries used specific lures, related to EU affairs, in their attempts to deceive users in Union entities.
- We tracked cyber attacks that we think were targeting particular sectors. Given the high number of Union entities and the diversity of EU policies, the 25 sectors that we are monitoring are varied in nature. We noticed that, beside the public administration sector, 13 of these sectors were targeted by at least 10 attacks in 2023. The most targeted sectors of interest for us were, in descending order, diplomacy, defence, transport, finance, health, energy, technology, justice, telecommunications, research, education, fundamental rights, and space.
- In 2023, ransomware remained the predominant cybercrime activity, globally. However, we didn't detect any significant ransomware breach affecting Union entities. In Europe, according to information from open sources and data leak sites (DLS), we noticed activity by at least 55 ransomware operations and a total of 906 victims. One ransomware operation, Lockbit, accounted for 25% of the total cases.

1. Threat actors activity

In order to help Union entities detect targeted attacks and defend against them, it is crucial to have insights into the threat actors targeting Union entities or their vicinity. Actionable intelligence needs to combine details on TTPs, IoCs, and detection rules. Yet, gaining insight into the threat actor's profile, motivation, origin, and historical activities are equally important to pinpoint specific threats. In this chapter, we delve into these aspects to uncover trends, patterns, and to help stakeholders grasp the motives and identities of those targeting Union entities or their vicinity.

1.1 Exposure

Overall, for the year 2023, we know of at least 80 threat actors having been active against Union entities or in their vicinity. Union entities' exposure to these threat actors ranges from critical to low.

- Critical exposure: 18 threat actors successfully breached some of the Union entities. We could attribute some of the breaches to known threat actors, while others are unknown to us (we label them "Unidentified Threat Actors" UTA-xxx). It is possible that some of these unknown threat actors overlap.
- High exposure: 17 threat actors targeted Union entities but failed to breach any system. This consisted mainly of threat actors sending spearphishing e-mails that were detected and blocked by Union entities or adversaries attempting to exploit vulnerable, exposed software products, without success.
- Medium exposure: for 21 threat actors, we detected suspicious or opportunistic connections, or scanning from infrastructure they control towards the networks of Union entities. However, there was no sign of a breach or exploitation.
- Low exposure: for 24 threat actors, we noticed that they targeted the vicinity of Union entities (EU countries, sectors of interest, software products used by Union entities) but we did not detect any sighting in our constituency.

Note: Some threat actors performed activities resulting in different levels of exposure. For example, an unsuccessful spearphishing attack (high exposure) and, at a different period of time, active scanning (medium exposure). In such case, we have retained the maximum exposure level to that threat actor (high exposure).

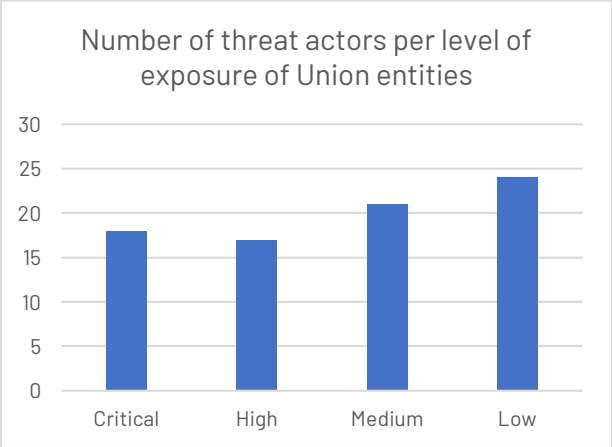


Figure 1 - Number of threat actors per level of exposure

1.2 Motive

The exact motive of threat actors is often difficult to determine, and therefore, in a number of cases, we categorised the motive as "unknown". We assess that these may be threat actors prepositioning themselves for a future exploitation (which may or may not arise), access brokers, or others.

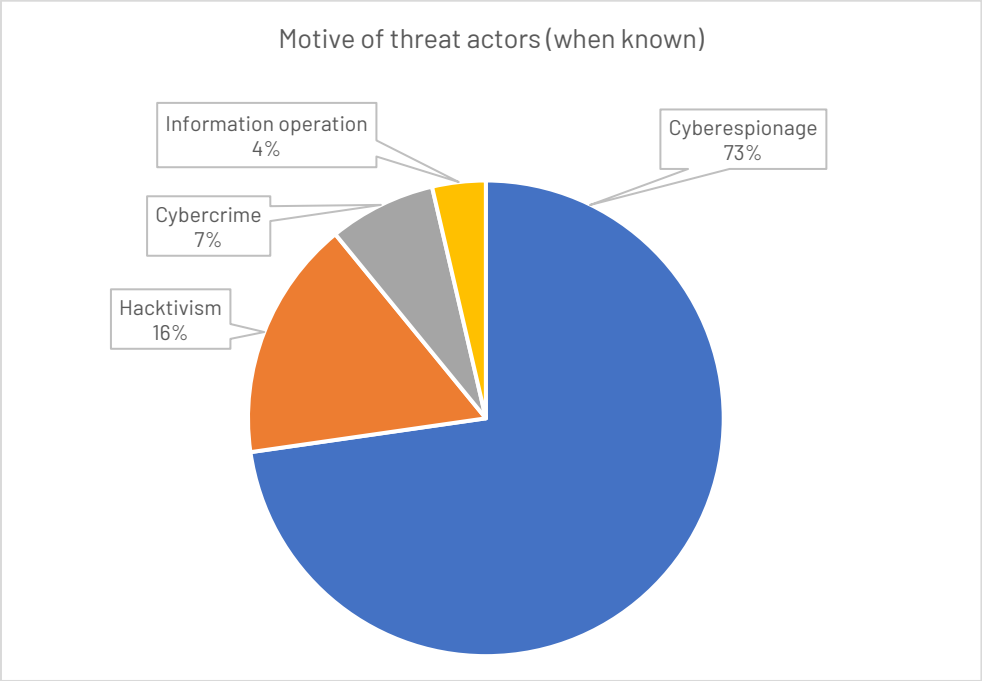


Figure 2 - Motive of threat actors

For the cases that it was possible to determine the motive with a sufficient degree of confidence, 73% of threat actors operating in our constituency's vicinity had cyberespionage objectives. Threat actors behind such attacks are usually state-sponsored groups (including a number of well-known ones) interested in sensitive information owned by Union entities or their partners (see also the chapter "Sectoral targeting" for analysis of sectors of interest for threat actors). They typically aim to gain unauthorised access to either user accounts/e-mails or to servers which store sensitive information. Some cyberespionage actors conduct targeted intrusions which may require weeks or months of preparation; such actors also typically attempt to plant false flags to disguise their activity. Other cyberespionage actors in our vicinity prefer to cast a wide net: they engage in high volume spearphishing attacks, or they conduct mass scanning of our public-facing IT assets automatically, in attempts to find unpatched zero-day or n-day vulnerabilities. Still, such scanning makes them highly visible, which suggests that maintaining stealth is less of a priority for them compared to the benefits of achieving an opportunistic breach.

About 16% of the threat actors were supposed hacktivists. Their attacks resemble genuine hacktivism but are sometimes a front for nation-state activity. Hacktivist attacks are often boasting, they aim for the highest degree of publicity and to be picked up by media, to weaponise their attack as part of an information operation. A classic example is the endless DDoS attacks by pro-Russia supposed hacktivists which have almost no business impact, but which sometimes succeed in drawing the attention of the media.

Only a very limited group of cybercrime actors executed notable attacks against our constituents or their vicinity, perhaps because their activity is more opportunistic than targeted; hence they look for low-hanging fruits. When we do see financially motivated attacks, they are in most cases attempts to deliver commodity malware and start an infection chain that would typically lead to ransomware. There have also been cases of cryptomining, which are very quickly detected, as well as ones where access brokers attempt to sell their unauthorised access to a network on underground forums.

We identified a few known threat actors conducting information operations with a cyber component in our vicinity. These generally only gained limited visibility.

1.3 Origin

Determining the origin of a threat actor is often complex. We do not link threat actors to particular countries ourselves, but we rather rely on attribution made by reliable sources. In this document, the analysis of the origin of threat actors is limited to cases where this attribution was possible and was available to us.

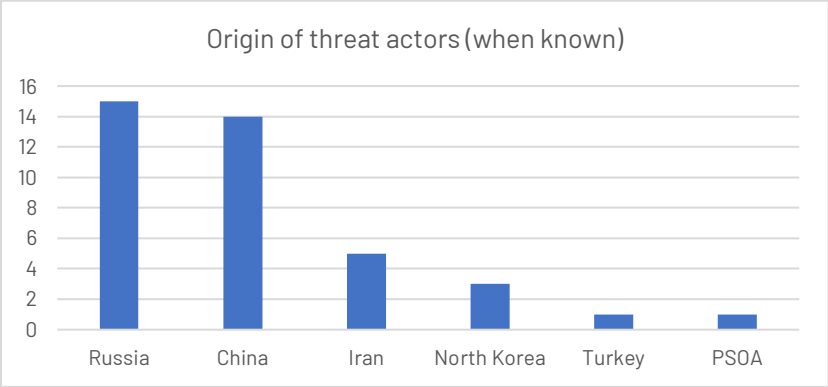
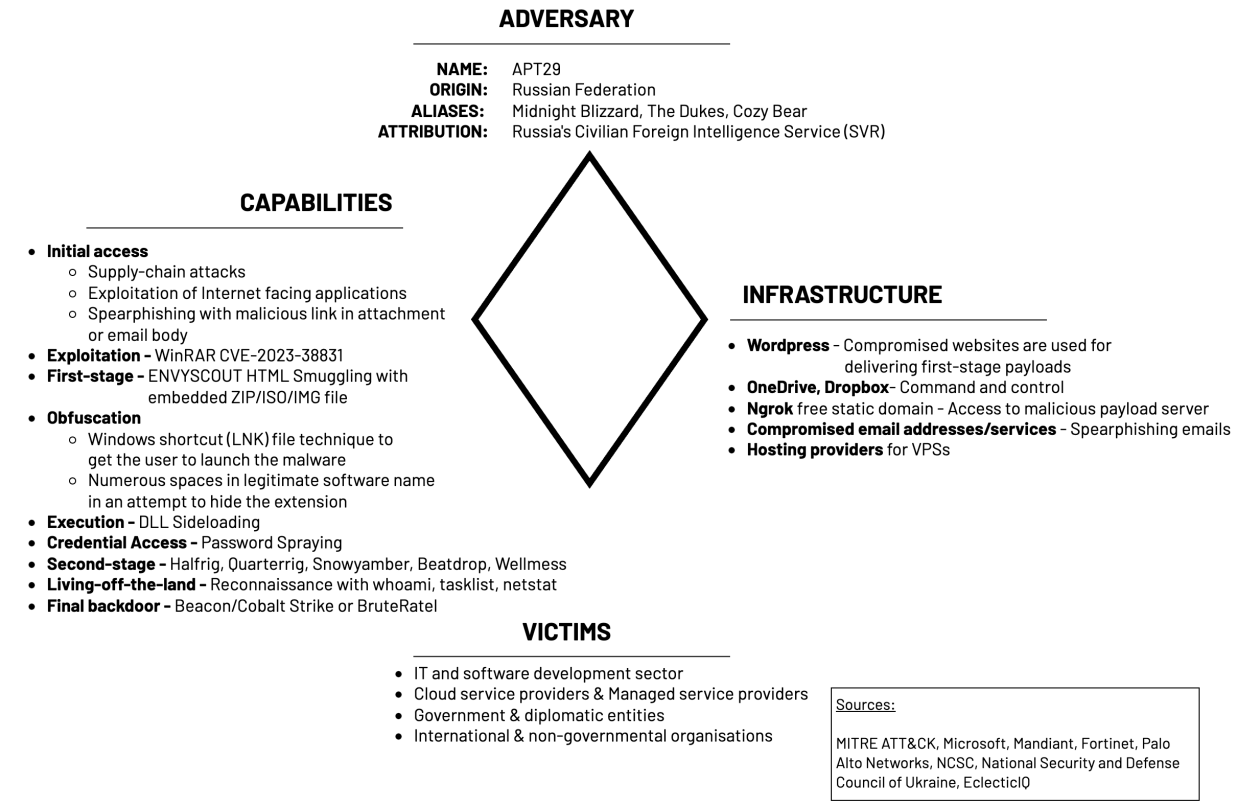


Figure 3 - Origin of threat actors

We consider it likely that 15 of the known actors active against Union entities or their vicinity have a Russia-nexus. In 2023, Ukrainian organisations and organisations in other countries associated with Russia's war on Ukraine remained the centre of gravity of Russia-linked cyber activity. We assess that Russia-related activity in our vicinity often had the motive of cyberespionage, with a focus on organisations in the defence and diplomatic sectors. For example, in 2023 alone, APT29, a Russia-linked cyberespionage actor, sent several waves of spearphishing e-mails towards European entities in the government or diplomatic sector (see also chapter "Spearphishing"). Another prominent motive of Russia-linked activity was hacktivism. A number of pro-Russia groups claimed DDoS attacks in the EU almost on a daily basis. They were attempting to sow discord in the context of European support for Ukraine or in the context of the Israel-Hamas conflict.

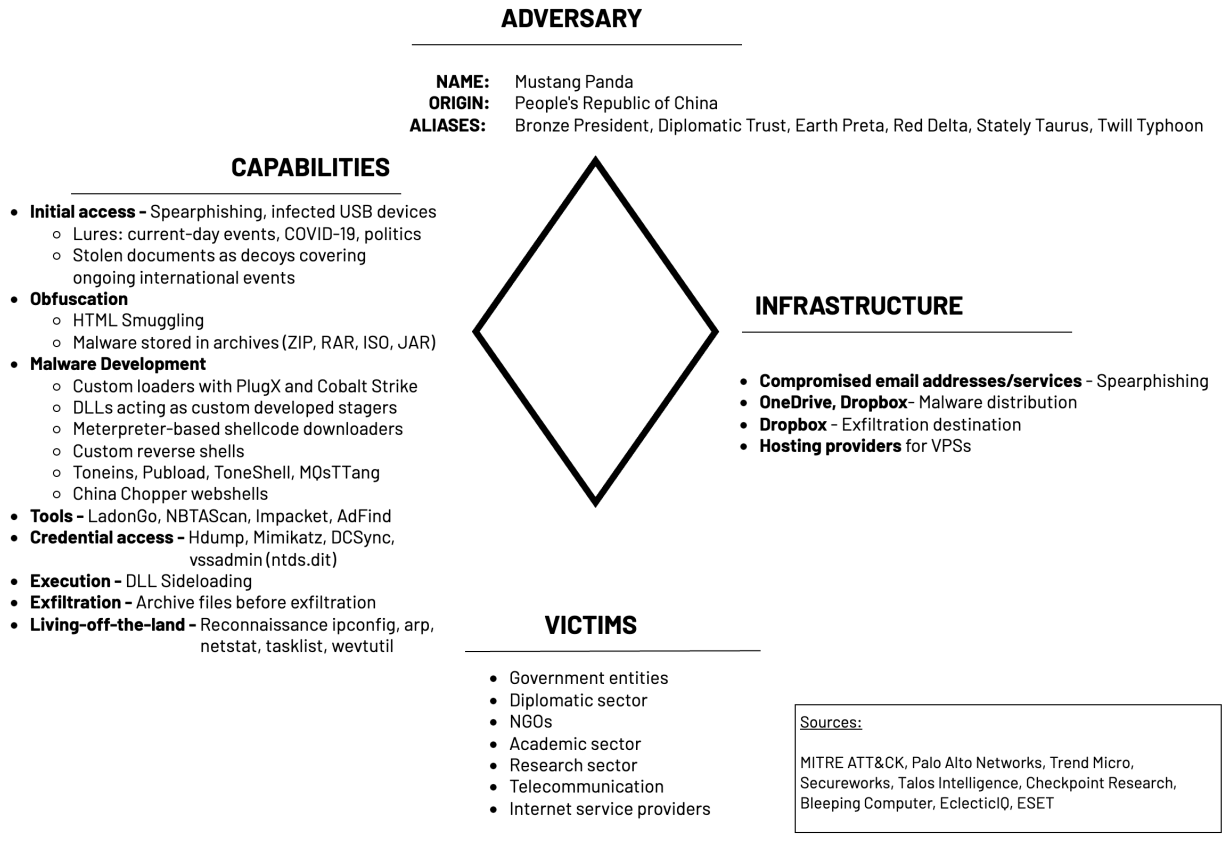
***APT29 in the spotlight**: APT29 is a Russian state-sponsored threat actor, which US CISA has attributed to the Russian Foreign Intelligence Service (SVR)[i]. First observed in 2008, they are known for targeting governmental organisations in Europe and NATO countries as well as research institutes and think tanks. On one hand, APT29 is running spearphishing campaigns while, on the other hand, the threat actor engages, in an expert manner, at supply-chain attacks. Following their 2020 Solarwinds supply-chain attack, they continued to target strategic technology companies such as cloud service providers and managed service providers. In 2023, they reportedly exploited vulnerable JetBrains TeamCity instances on a global scale and conducted a slow password spraying campaign[ii] which allowed it to remain hidden.*



We found that at least 14 of the known threat actors active against Union entities or their vicinity last year have a China-nexus. Chinese threat actors in our vicinity aim to gain a persistent foothold in the networks of

organisations they target. Often they attempt to use such access to install malware which exfiltrates data, thus achieve cyberespionage objectives. In a limited number of cases, the motive was less clear, the China-linked actor appeared to be prepositioning for an unknown future activity, without noticeably exfiltrating data. China-linked groups consistently target entities in specific sectors, for example, the European diplomatic sector, but they are also driven by current events. A number of China-linked actors have become difficult to distinguish from each other due to their shared use of tools and infrastructure. Their complex obfuscation networks conduct automated mass scanning and have been seen attempting to exploit vulnerabilities the day they were announced. The automation of this activity likely explains the high volume of activity and global impact when these networks attempt to compromise targets.

***Mustang Panda in the spotlight**: Mustang Panda was first observed in 2017, but has possibly been conducting operations since at least 2014[iii]. Mustang Panda has targeted government entities, non-profit, religious, and other non-governmental organisations in the EU, the USA, Germany, Mongolia, Myanmar, Pakistan, and Vietnam, among others. Since the end of 2021, early 2022, we observed an uptick in campaigns targeting entities in the EU. Mustang Panda uses both proprietary and publicly available hacking tools. In 2023, Mustang Panda continued to send a significant number of waves of spearphishing e-mails to the European governmental sector. Apart from spearphishing with malicious attachments or malicious links, Mustang Panda attempted to conduct watering hole attacks and spread infections through USB drives.*



In 2023 we observed an increase in Islamic Republic of Iran (hereafter Iran) nexus scanning and attempted exploitation activity in our vicinity compared to previous years. Activity linked to Iran is often driven by current events, for example, in the cases of pro-Iran supposed hacktivists targeting individuals and organisations deemed to support Israel in the context of the current Israel-Hamas conflict.

Finally, we observed a small number of actors associated to other countries targeting organisations in our vicinity. For example, in 2023 we learned of malicious activity in our vicinity ranging from cyberespionage to hacktivism from actors linked to the Democratic People's Republic of Korea (hereafter North Korea), and the Republic of Türkiye (hereafter Turkey). We also noticed activity by at least one private sector offensive actor (PSOA).

2. Software products

In 2023, we stepped up our capacity to detect threats targeting software products used or likely to be used by Union entities. This allowed us to tackle the different forms of attacks abusing software products (such as exploitation of flaws in the code, trojanised versions used in supply-chain attacks, fake versions). We noticed software products being targeted in different stages of the intrusion chain. Our major observation was that the exploitation of vulnerable, internet-facing products has become a predominant initial access method used by diverse threat actors.

We observed 104 software products being targeted in 241 distinct MAIs. We analysed different types of software products targeting, including

- exploitation of internet-facing vulnerable software products
- supply-chain attacks leveraging trojanised software products
- fake version of software products
- abuse of public repositories used for programming languages
- misuse by threat actors
- other forms of exploitation after initial access.

However, our monitoring focussed in particular on the first type of attacks, because we consider it to be the most impactful.

2.1 Product categories

In 2023, we noticed a large variety of products being targeted in cyber attacks. In this section, we group products into categories and we provide an assessment of the reasons why some categories are particularly attractive for threat actors. In an annexe, we are sharing a "Software Products Heatmap." In this heatmap, we highlight three possible levels of targeting:

- Low: we recorded one attack in our vicinity.
- Medium: we recorded at least two attacks in our vicinity.
- High: we recorded significant attacks or it was targeted by APT groups in our vicinity.

The diagram below provides the number of products targeted, per category and per levels of targeting.

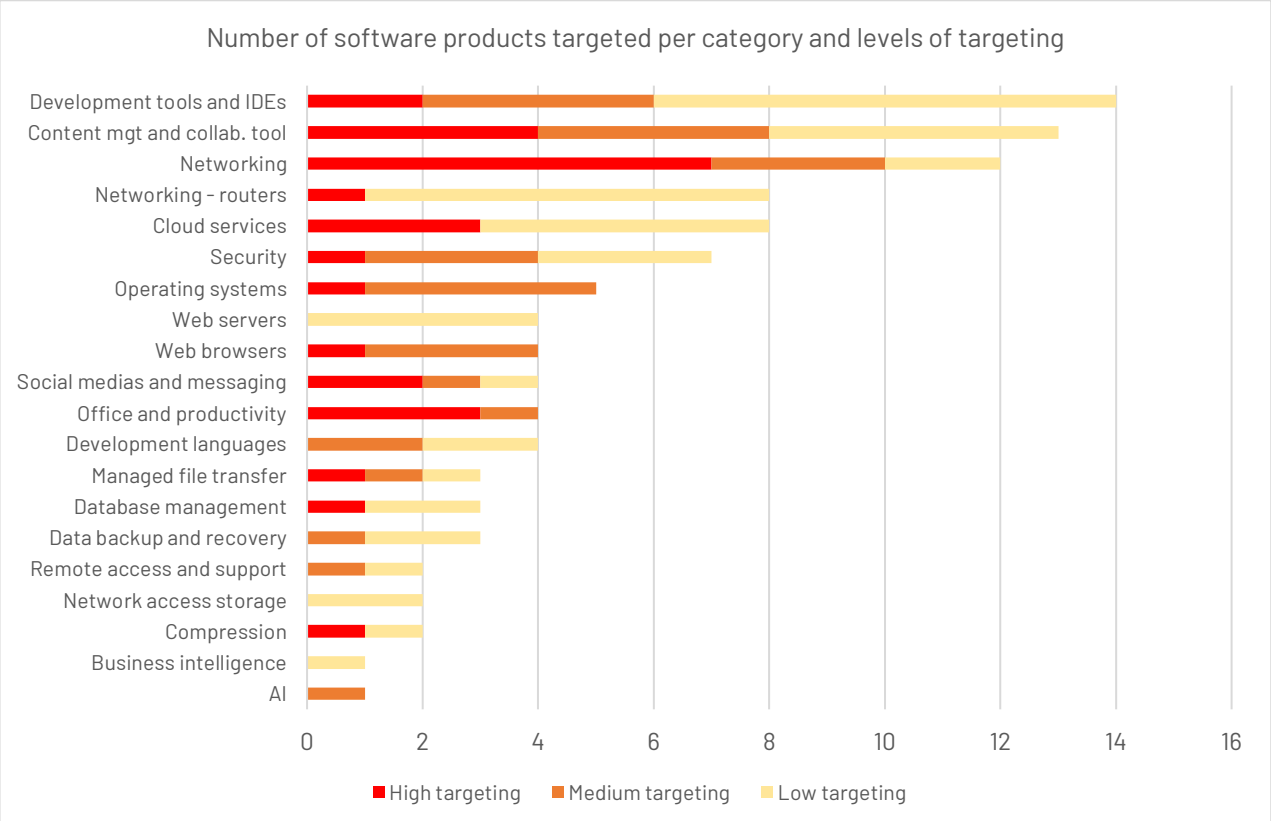


Figure 4 – Software products targeting

In the paragraphs below, we analyse some of the most targeted categories of software products.

Networking. There are many types of networking products (such as connectivity, load balancing, routing, firewall and VPN products). As these are usually part of any entity's internet exposure, networking products offer an ideal initial access path for threat actors. In 2023, we noticed a number of opportunistic or persistent threats (the latter usually state-sponsored), attempting to exploit vulnerable internet-exposed networking software products. Here are some notable examples:

- In May, Fortinet's FortiOS operating system was exploited through CVE-2023-27997, possibly as a zero-day[iv].
- In October, Cisco IOS XE devices were massively targeted through the CVE-2023-20198 vulnerability[v].
- In October, Mandiant reported that the CVE-2023-4966 vulnerabilities impacting Citrix NetScaler ADC and NetScaler Gateway appliances had been exploited as a zero-day in August 2023[vi].

Development tools and integrated development environments (IDE). Such products are ideal targets in some forms of supply-chain attacks. Targeting development tools or platforms can offer threat actors a possibility to easily trojanise software developed with these tools. Threat actors can also create malicious packages for programming languages in order to spread malware serving different purposes (cryptomining, backdoor features, etc.). Here are some notable examples:

- In December, the US CISA warned that the Russian Foreign Intelligence Service (SVR) was exploiting TeamCity globally. TeamCity is a software to manage and automate software compilation, building, testing, and releasing[vii].
- In December, the ESET cyber security company reported about several malicious Python projects being distributed via PyPI, the official Python package repository[viii].

Security. Attackers can target security software to better defeat or bypass security controls. This includes password management software, anti-virus, SIEMs, as well as endpoint protection software. In the case of password management software, threat actors often reuse stolen passwords in further attacks against additional victims. Here are some examples:

- 1Password, a popular password management platform used by over 100.000 businesses, suffered a security incident after hackers gained access to its Okta ID management tenant[ix].
- Hackers stole 4,4 million US dollars in cryptocurrency using private keys and passphrases stored in stolen LastPass databases[x].
- In August 2023, The US CISA and the Norwegian National Cyber Security Centre (NCSC-NO) released a joint advisory about threat actors exploiting Ivanti EPMM vulnerabilities CVE-2023-35078 and CVE-2023-35081[xi].

Content management and collaboration tool. Some of the content management systems and collaboration tools are accessible via the internet, while some others are implemented for internal use only. Attackers targeting internet-facing products might want to exploit the breach to gather personal information from the visitors. They may also attempt to steal their identity by redirecting them to sites that download malware onto their devices. Another option is using the breached server to send spam or dangerous content, or using it as a stepping stone to move laterally in the organisation. The breach of an internal-only collaboration software product would usually allow an attacker get access to sensitive information. Here are some notable examples of incidents:

- Cyber security firm Sucuri found that more than 17.000 WordPress websites were compromised in September 2023 with a malware known as Balada Injector[xii].
- In October, the US CISA warned that threat actors were exploiting Atlassian Confluence CVE-2023-22515 for initial access to networks[xiii].
- In July, Microsoft detected targeted attacks by Secret Blizzard (KRYPTON, UAC-0003) targeted Microsoft Exchange servers with PowerShell Desired State Configuration (DSC) to deliver various second-stage payloads including the DeliveryCheck backdoor[xiv].
- April, Mandiant reported on supply-chain attack that affected 3CX Desktop App software and attributed the attack to a North Korea linked threat actor[xv].

Cloud services. Organisations, including Union entities, rely increasingly on cloud computing. According to Eurostat[xvi], in 2023, 45,2% of EU enterprises purchased cloud services. The most purchased cloud services in 2023 were e-mail services (82,7%), followed by storage services for files (68,0%), and office software (66,3%). Security software applications (61,0%), finance or accounting software applications (51,6%) and hosting for the enterprise's database (43,0%) were also popular. In the vicinity of Union entities, we noticed a large variety of attacks exploiting flaws in cloud software or architectures but also targeting cloud services providers. Here is a short selection of notable attacks:

- In July, Microsoft reported about a China-linked threat actor, tracked as STORM-0558, forging authentication tokens with a stolen Azure Active Directory key, and gaining access to e-mails from an estimated number of 25 organisations[xvii].
- In July, UNC4899, a North Korea-linked threat actor targeted JumpCloud, a zero-trust directory platform service used for identity and access management, in a supply chain compromise affecting customers[xviii].
- In October, Microsoft reported about a campaign where attackers gained access and elevated permissions on a Microsoft SQL Server instance deployed in an Azure Virtual Machine (VM)[xix].

2.2 Product vendors

While tracking attacks targeting software products used or likely to be used by our constituents, we noticed various levels of criticality for exploited vulnerabilities. In the table below, we indicate vendors which had critical vulnerabilities affecting one or several of their products. These were exploited as zero-days or n-days by state-sponsored threat actors or cybercrime groups. The exploitation campaigns were opportunistic or targeted. After initial access, we noticed some threat actors starting further exploitation (such as installing webshells or conducting lateral movement). In other cases, we assess that the threat actors either did not find the target interesting or were focussed on selling access to third parties.

We assess that these vendors were particularly targeted for different reasons:

- Some of their products are used in almost all IT environments (such as Microsoft environments) or are very popular for particular use cases (such as WordPress for website content management).
- Several of these products must be exposed on the internet to operate, and therefore any flaw in them would offer ideal opportunities for initial access.
- Some vendors have a track record of poor security management.

Vendors	Products	Notable CVEs
Fortinet	FortiOS SSL-VPN, FortiWeb, FortiNAC, FortiGate	CVE-2022-42475, CVE-2023-27997, CVE-2023-33308, CVE-2022-39952
Ivanti	Endpoint Mobile Manager (also known as MobileIron Core)	CVE-2023-35078, CVE-2023-35082
Microsoft	Azure, Exchange Server, SQL server	CVE-2023-29332, CVE-2021-34473, CVE-2021-34523, and CVE-2021-31207
Citrix	Citrix Netscaler Gateway, Citrix Netscaler ADC	CVE-2023-3519, CVE-2023-4966
Zimbra	Zimbra Collaboration Suite	CVE-2023-29381, CVE-2023-29382
WordPress	WordPress (multiple plugins)	CVE-2023-5360, CVE-2023-28121
VMWare	VMWare ESXi, Vmware Aria Operations, vRealize Log Insight	CVE-2023-20887, CVE-2022-31704
MoveIT	Progress MoveIT Transfer	CVE-2023-34362, CVE-2023-35708
Cisco	Cisco routers	CVE-2023-20198
Atlassian	Confluence	CVE-2023-22518
Google	Chrome	CVE-2023-7024

Table 1 – Notable exploited products per vendor

3. Spearphishing attacks

In 2023, spearphishing remained the predominant initial access method for state-sponsored and cybercrime groups seeking to infiltrate target networks. This sophisticated form of phishing involved highly targeted and personalised e-mail campaigns, meticulously crafted to deceive specific individuals within organisations. In Union entities or their vicinity, as well, spearphishing was the most observed method to attempt initial access. We have analysed 177 such attacks, that we found notable.

3.1 EU affairs lures

A number of adversaries used specific lures related to EU affairs, in their attempts to deceive users in our vicinity. Some threat actors sent spearphishing e-mails containing malicious attachments, links, or decoy PDF files that originally were internal or publicly available documents related to EU policies. Some examples of leveraged EU affairs themes include the following (but did not necessarily target the mentioned organisations):

- Swedish Presidency of the Council of the European Union[xx]
- EU - Community of Latin American and Caribbean States (CELAC) Summit
- Working Party of Foreign Relations Counsellors (RELEX)
- EU LegisWrite (a European Commission editing program)[xxi].

In recent years, 2023 was the first time that we observed so many attacks in a short period of time (a few months) being directly linked to the EU political consultation and decision-making structure. Interestingly, one of the adversaries known to use EU political lures for spearphishing, the China-linked threat actor Mustang Panda, has been using this tactic since at least 2022[xxii].

To make the spearphishing message even more credible, the attackers often impersonated staff members of Union entities or of the public administration of EU countries. These attacks targeted not only Union entities but also public administration in EU countries. This shows a significant interest by some adversaries to gather information related to various EU political matters.

3.2 A diversity of tactics

Beside spearphishing attacks using EU affairs lures, we also noticed different forms of spearphishing tactics:

- Attackers targeted Union entities with e-mail thread hijacking or attempted to phish by reusing old conversations. This implies that an account participating in the threat had at some point been compromised.
- Several Union entities received phishing e-mails that impersonated the CEO of a company. The company was a contractor for the Union entities.
- One Union entity reported targeted e-mails and WhatsApp messages impersonating a head of Unit of the entity.
- Several Union entities received e-mails containing a link to a page that masqueraded as an official portal of another entity.
- The Head of a Union entity was targeted with a smishing (SMS phishing) attack attempting to deliver mobile spyware.

We could not always determine the motive of these attacks. We assess that they could have been of a cybercriminal nature, or with a cyberespionage purpose. These tactics are not new, and, in all the cases reported to us, the attacks were not successful. However, the diversity of tactics, especially when the social engineering component is well prepared, makes it difficult for organisations to counter all variations of spearphishing.

3.3 Reconnaissance and social engineering

The observations above show that, whatever the goal of the attack was, the threat actors dedicated time and resources in preparatory phases such as reconnaissance and social engineering. Reconnaissance involves gathering intelligence about Union entities: the role of certain staff members, their contact lists, the documents or information they usually share with their stakeholders. Social engineering manipulates human psychology, and in the context of spearphishing against Union entities, social engineering aims to craft believable deceptive messages by leveraging information acquired from previous attacks or exposed on unsecured IT assets to increase the likelihood of successful infiltration.

3.4 Spearphishing via multiple platforms

It is also important to recognise that spearphishing extends beyond traditional e-mail platforms, as threat actors also target diverse communication channels such as messaging apps and social media. When the spearphishing attack is executed via messaging, the goal of the threat actor is to infect targeted mobile devices; indeed, these devices are often less controlled than the personal computers and servers administered by Union entities. Maintaining awareness of these evolving tactics is paramount for individuals and organisations, in order to reinforce and adapt their defences, and to safeguard against the expanding scope of spearphishing attacks.

3.5 Spearphishing and information operations

We observed that spearphishing attacks sometimes served as integral components within broader information operations, enabling threat actors to compromise specific targets, gather sensitive data, and manipulate public perception. In orchestrated campaigns, these attacks were followed by tactics such as hack and leak, leveraging stolen information for strategic dissemination, influencing narratives, and furthering the objectives of the overall disinformation effort. We assess that spearphishing operations executed as a preamble, to feed information operations constitute a major threat to Union entities, especially in view of the upcoming EU elections of May 2024.

3.6 Most active spearphishing threat actors

Against Union entities or their vicinity, the two most active threat actors in spearphishing operations were Mustang Panda and APT29, respectively attributed by reliable sources to China and Russia. We assess that both threat actors launched at least 15 waves of spearphishing attacks against EU targets in 2023. In some cases, the attacks were also targeting organisations in non-EU countries. In many of these attacks, the targeted organisations were public administrations, especially in the diplomatic sector. We also noticed spearphishing attacks by four additional groups of likely Russian origin and one group of likely Chinese origin. There were also waves attributed to a likely Iranian threat actor.

4. Sectors

We identified 25 sectors of interest to Union entities and track attacks targeting those sectors. Given the high number of Union entities and the diversity of EU policies, these sectors are varied in nature. Attacks targeting specific sectors usually have particular motives which we will discuss below.

While monitoring attacks on specific sectors, it's often challenging to determine if the attacks were deliberately targeting that sector or if they were opportunistic. Cybercriminals typically target sectors opportunistically to monetise breaches by selling access or stealing valuable information. However, certain sectors are also prime targets for cyberespionage, where threat actors aim to steal information for disruptive operations or for hacktivism purposes.

It is also important to keep in mind which sectors are likely to be targeted following a change in geopolitical circumstances around the world (e.g. Russia's war on Ukraine, Israel-Hamas conflict, etc.). In fact, often when the sectoral targeting is deliberate and motivated, it comes in retaliation to wider circumstances. We can take Russia's war on Ukraine as an example, where the diplomatic and defence sectors became prime targets, namely for cyberespionage reasons.

In our records, the public administration sector is the most targeted, with 33% of MAIs focusing on it. Since Union entities are all public administrations, the report will not delve into public administration as a separate sector. Instead, our analysis focuses on other sectors for which we recorded at least 10 MAIs in 2023. The number of recorded MAIs is given by sector, without implying a direct targeting of Union entities in that sector.

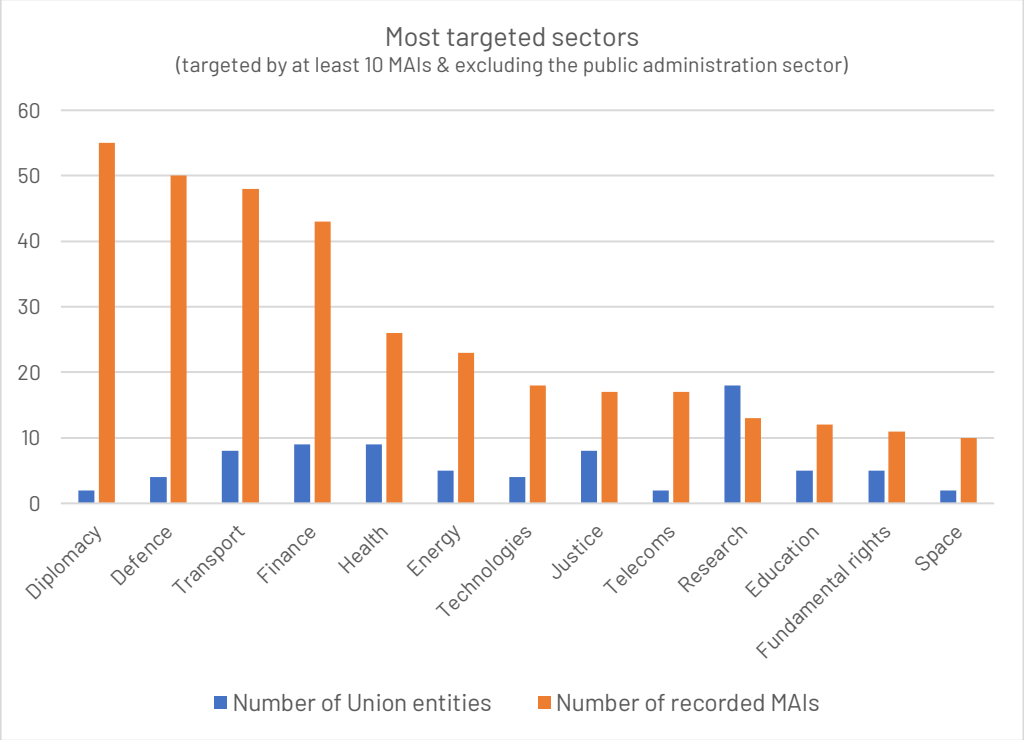


Figure 5 – Most targeted sectors and number of Union entities

In the sub-chapters below, we analyse the particular attractiveness of a subset of these sectors.

4.1 Diplomacy

The diplomatic sector includes activities related to a country's diplomatic affairs, such as its embassies, consulates, and foreign ministries. It is highly targeted, particularly for cyberespionage, due to the strategic information accessible to diplomatic instances and staff. Threat actors targeting this sector in the EU likely aim to steal information concerning EU policies and international strategy.

Some publicly known attacks are given below:

- Russia-linked APT29 targeting EU governments assisting Ukraine in the context of the war in Ukraine, more specifically their diplomatic entities[xxiii].
- Spearphishing attacks by Russia-linked APT29 targeted Polish diplomatic missions of Poland[xxiv].
- China-linked Mustang Panda targeted diplomatic missions of NATO countries[xxv].

4.2 Defence

The defence sector, akin to diplomacy, holds crucial geopolitical importance and is a prime target for cyberespionage. Recent events like Russia's war on Ukraine have heightened the defence sector's appeal to threat actors interested in understanding European defence support to Ukraine. Additionally, it's considered critical infrastructure for countries' sovereignty and the EU's security efforts. Investments in defence policy and industry have increased, including through initiatives like the Common Security and Defence Policy and the European Defence Industrial Strategy. This sector encompasses both public and private entities, such as defence ministries and industries.

Some publicly known attacks are given below:

- Iran-linked Peach Sandstorm targeted defence organisations worldwide[xxvi].
- The threat actor Void Rabisu targeted EU military personnel working on gender equality initiatives (in a separate campaign, they have also used the NATO summit as spearphishing lures[xxvii]).
- Russia-linked threat actors claimed to have stolen information on UK military and intelligence sites[xxviii].

4.3 Transport

The transport sector, encompassing aviation, maritime, rail, and road activities, is crucial infrastructure due to its diverse mobility functions, including civilian, commercial, and military operations. It is susceptible to two main types of targeting: cyberespionage, particularly in aviation and maritime subdomains, and disruption, due to the significant consequences it can entail.

Some publicly known attacks are given below:

- Russia-linked threat actor exploited a Microsoft vulnerability to target, among others, transport sector in Europe[xxix].
- APT35 targeted critical infrastructure in European countries, including in the transport sector[xxx].
- China-linked Volt Typhoon targeted US critical infrastructure, including in the transport sector[xxxi].

4.4 Finance

The finance sector is interconnected with various sectors and susceptible to different threats like cybercrime and cyberespionage. Attacks on this sector are typically opportunistic, driven by financial gain. Common attack types include data leaks, ransomware, and cyberespionage. Additionally, supposed hacktivist attacks like DDoS often target finance websites.

Some publicly known attacks are given below:

- Several pro-Russia supposed hacktivists conducted DDoS attacks on financial systems.
- China-linked Mustang Panda targeted finance sector in Europe, Asia, and the United States[xxxii].
- Russia-linked Winter Vivern targeted several sectors, including financial, in a long-term cyberespionage campaign[xxxiii].

4.5 Health

The health sector, deemed critical infrastructure due to its societal importance, includes hospitals, medical centres, and health organisations. Attacks on this sector are typically opportunistic, often driven by financial motives, though there's been a rise in supposed hacktivist attacks. Ransomware is the most common cybercriminal attack targeting this sector.

Some publicly known attacks are given below:

- Killnet, the pro-Russia supposed hacktivist group targeted hospitals in Europe with DDoS[xxxiv].
- North Korea-linked Lazarus Group launched a campaign targeting healthcare entities in Europe and the United States[xxxv].
- Philippines state health organisation victim of Medusa ransomware gang was struggling to recover[xxxvi].

4.6 Energy

The energy sector includes traditional industries like petroleum, natural gas, and nuclear, as well as renewables like hydropower and solar. Attacks on this sector typically aim to disrupt energy production or distribution, potentially impacting citizens, or are hacktivist DDoS attacks which aim to gain media attention.

Some publicly known attacks are given below:

- Russia-linked threat actor exploited a Microsoft vulnerability to target, among others, the energy sector in Europe[xxxvii].
- Unknown threat actor breaches 22 energy companies in Denmark, disrupting the operations of the targeted facilities[xxxviii].

4.7 Technology

The technology sector encompasses digital infrastructure, IT companies, and technology development industries. It faces various attacks, including financially motivated cybercrime, espionage, and prepositioning (potentially for future disruptive attacks). It's also a prime target for supply-chain attacks, where threat actors target technology companies to compromise their software products or services and potentially affect their customers.

Some publicly known attacks are given below:

- Russia-linked APT29 targeted several sectors, including technology and IT services[xxxix]. This threat actor often works with supply-chain attacks and has created some of the biggest incidents related to it, such as for Microsoft in 2023, or for SolarWinds in 2020.
- A threat actor named Earth Estries was found conducting a cyberespionage campaign against technology industries in Germany, the United States, and others[xl].
- Agonizing Serpens targeted Israeli technology sector, to steal information and then deploy wipers[xli].

5. Ransomware

In 2023, ransomware remained the predominant cybercrime activity, globally. In this chapter, we are providing a synthetic overview of the ransomware threat in our constituency, an analysis of ransomware attacks in Europe, and a focus on some major ransomware operations.

5.1 Union entities

In our constituency, although we didn't detect any significant ransomware breach, we made two notable observations. First, we continued to detect routine attempts to deliver malware (mostly via phishing attacks). A possible malware infection could lead to ransomware incidents (via an infection chain). It could also give a foothold on Union entities systems for access brokers reselling access to ransomware groups. All such attempts, in 2023 remained generally unsuccessful. Second, we observed a single case of limited ransomware infection affecting a system in a testing environment. Interestingly, the initial access vector was the exploitation of a vulnerable, internet-exposed server.

5.2 Europe

In Europe, based on information from open sources and data leak sites (DLS), we noticed activity by at least 55 ransomware operations and a total of 906 victims. The activity of the various groups is very heterogeneous:

- One ransomware operation, Lockbit, accounts for 25% of the total cases.
- Just 20 groups have claimed ten or more victims each.
- These 20 groups account for more than 87% of the cases.

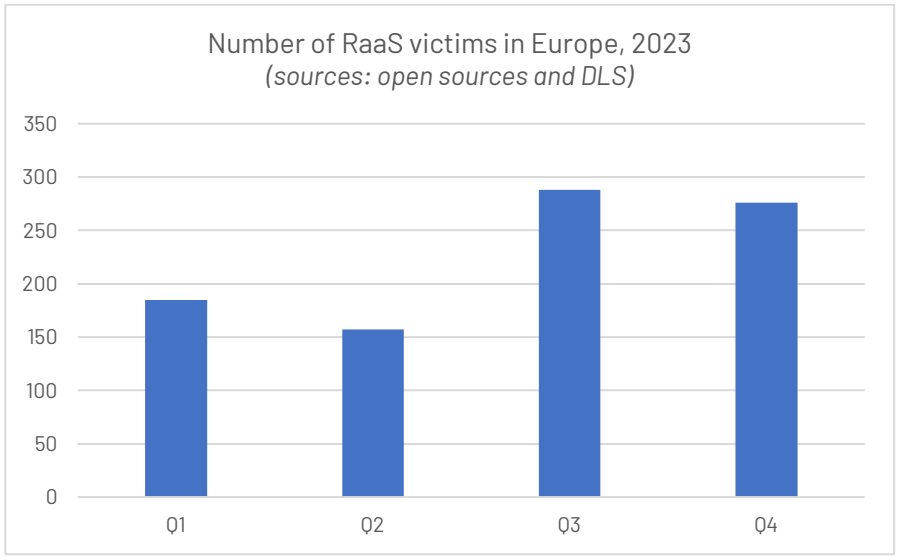


Figure 6 – Number of ransomware victims in Europe

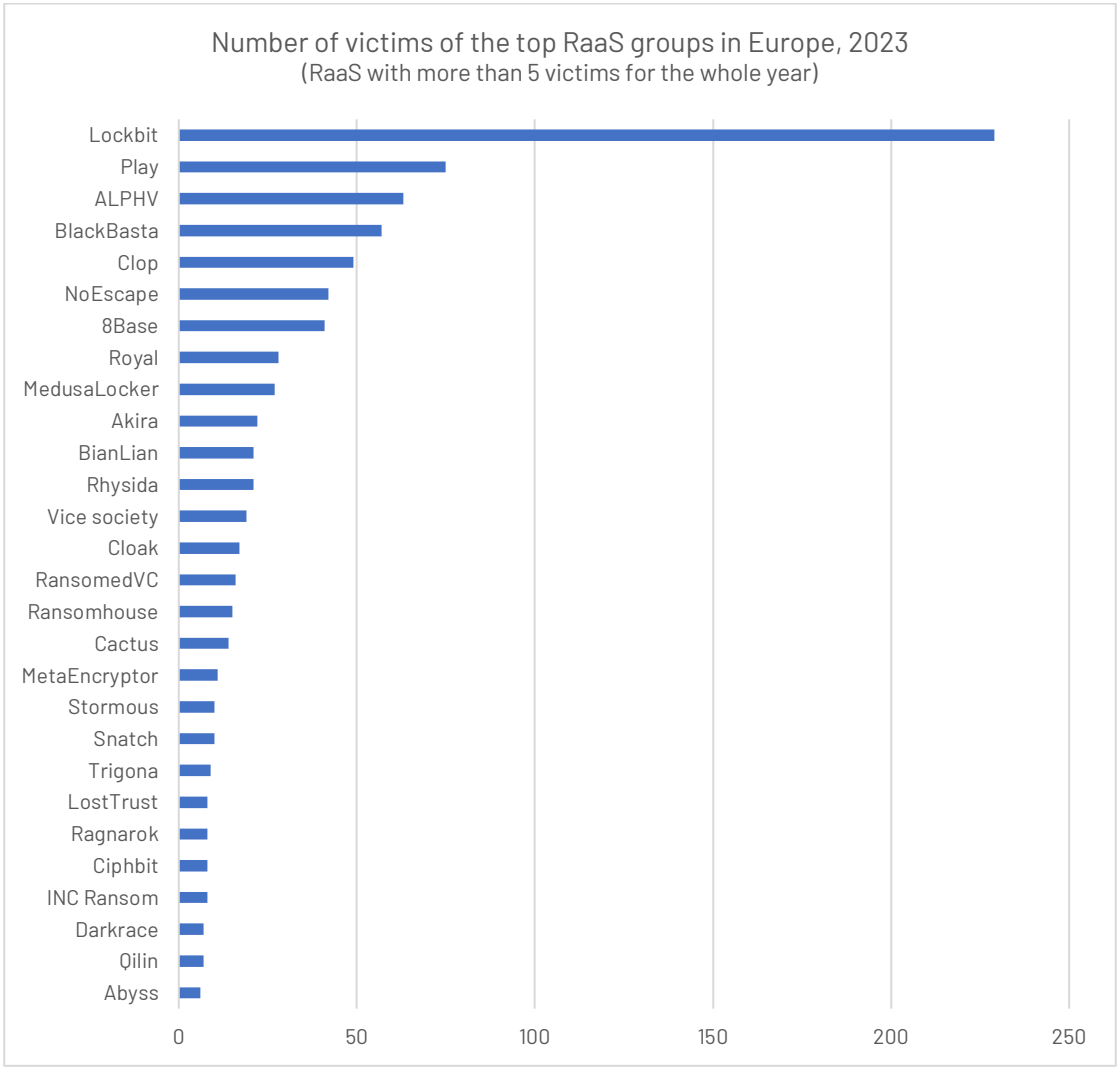


Figure 7 – Most active ransomware in Europe

Lockbit has been the main ransomware group in Europe, maintaining around 65 victims per quarter, with signs of organisational challenges[xlii]. Other groups like Play, AlphaV, and BlackBasta remained active, while newcomers like 8Base and NoEscape replaced others like Royal and Vice Society.

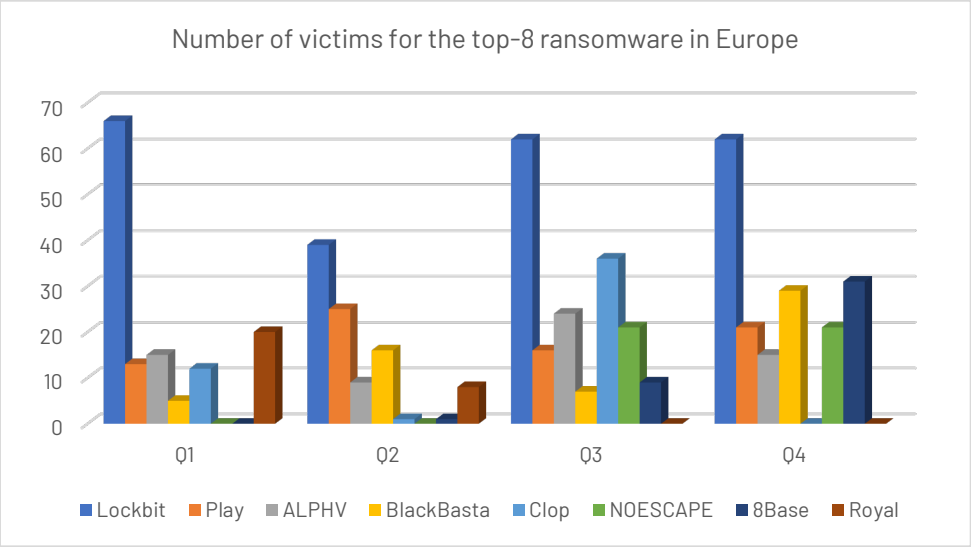


Figure 8 – Evolution of top-8 ransomware in Europe

Regarding country targeting, in Europe, the UK was the most attacked country, closely followed by Germany, France, Italy, and Spain, with these results staying almost stable for all the period of 2023. Ranking of countries match the respective size of their economy. Since RaaS operations mainly target opportunistically, the more companies there are in a country, the bigger attack surface this country presents.

Regarding sectoral targeting, the manufacturing sector was the hardest hit, with attacks increasing over each quarter. The same trend was observed in the legal and professional services, construction and engineering, and retail sectors. Although also targeted, the technology, education, and healthcare sectors showed a diminishing number of attacks as the year progressed.

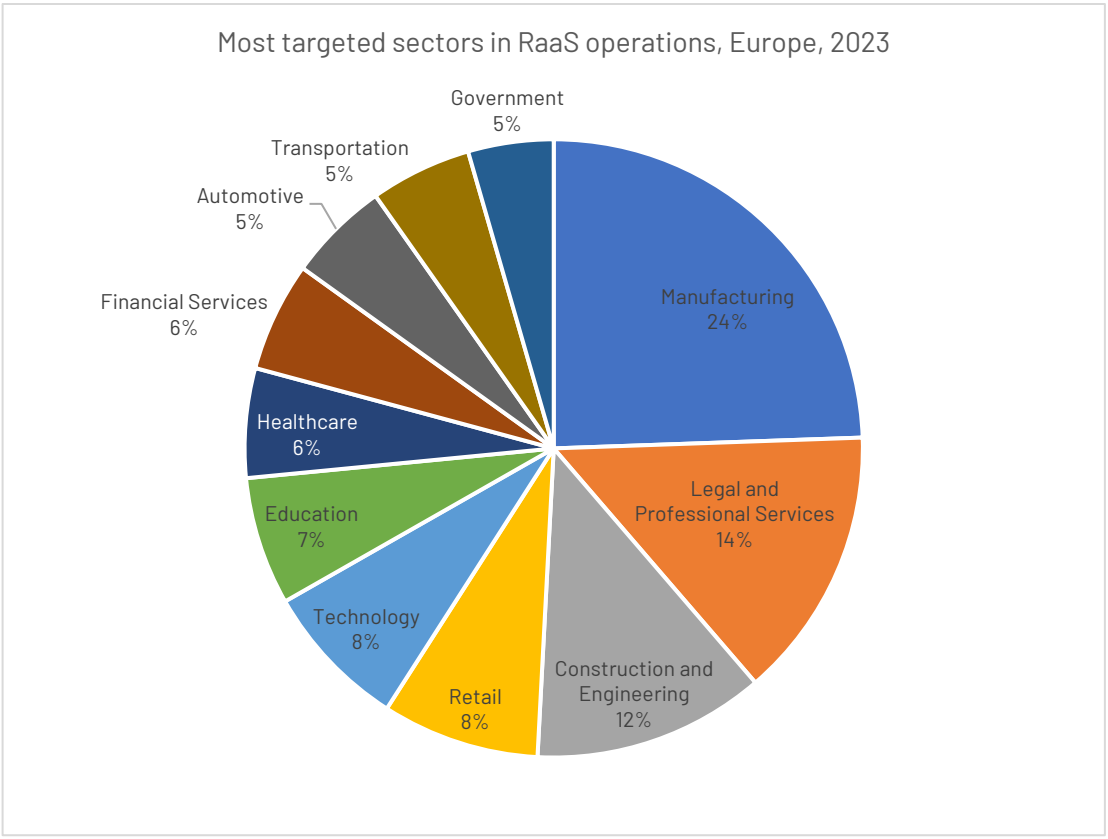


Figure 9 – Most targeted sectors by ransomware in Europe

5.3 Top 3 RaaS operations in Europe

Lockbit. In 2022, LockBit emerged as the most widespread ransomware variant. By 2023, the group targeted organisations across all sectors in Europe, showcasing their opportunistic approach and potential impact on any organisation. According to BlackBerry, LockBit is a cybercriminal group with Russian ties. The malware,

part of the LockerGoga and MegaCortex families, is self-spreading and utilises common on-device tools like Windows PowerShell and SMB for encryption, data exfiltration, and propagation. Notable LockBit attacks in Europe in 2023 include:

- In February, Lockbit listed the UK Royal Mail on their DLS and threatened to publish data. The British postage and courier company's ability to dispatch parcels and letters to international recipients ground to a halt in January, following the attack[xliii].
- In February, LockBit claimed the compromise of Aguas do Porto, a Portuguese municipal water company. Lockbit threatened to release exfiltrated data[xliv].
- A Lockbit ransomware attack on December 24, 2023, disrupted emergency services at three German hospitals. While patient treatment continued with some restrictions, emergency care became unavailable, and patients were redirected to other hospitals[xlv].

Play. The Play ransomware operation, likely originating in Latin America around mid-2022, gains access through reused or illicitly obtained accounts, exposed RDP servers, and exploiting vulnerable Fortinet systems. They adapt tactics with evolving vulnerabilities, such as ProxyNotShell and Microsoft Exchange Server Remote Code Execution. They escalate privileges using Mimikatz and add accounts to privileged groups like Domain Administrators. Their toolkit includes Cobalt Strike SystemBC, a SOCKS5 Tor proxy, and the Empire post-exploitation framework. In 2023, there were around 76 attacks against European entities, mainly targeting the manufacturing, construction, and engineering sectors, with significant cases in the UK, Germany, France, and the Netherlands.

Black Basta. Black Basta ransomware, originating from Russia, targets prominent organizations in Europe and North America across various industries since April 2022. It's suspected to be connected to the Conti Group and potentially Fin7 due to similar tactics. Initial access is gained through spearphishing, buying access, or exploiting vulnerabilities like PrintNightmare and Follina. Affiliates move laterally, steal data, and deploy ransomware, using a double-extortion scheme. They expanded to ESXi systems in 2022 with version 2.0. Despite disruptions to associated malware, Black Basta remains a persistent threat. In 2023, at least 57 operations targeted European entities, mainly in the manufacturing sector, with most cases in Germany, and additional ones in the UK and the Netherlands.

Annexe - Software products heatmap

AI	Business intelligence	Cloud Services	Content management and collaboration tool	Compression	Data Backup and Recovery	Database Management	Development Languages	Development Tools and IDEs	Managed file transfer	Networking	Networking - Routers	Network Access Storage	Office and Productivity	Operating Systems	Remote Access and Support	Security	Social medias and messaging	Web Browsers	Web Servers
ChatGPT	Qlik Sense	Amazon Web Services	3CX Desktop App	7zip	ConnectWise R1Soft Server Backup	Microsoft SQL server	GNU C library	Adobe ColdFusion	GoAnywhere	VMWare ESXi	Asus router	QNAP NAS device	Adobe Acrobat Sign	Android OS	AnyDesk	1password	Facebook	Apple Safari	Apache Tomcat
		Google Cloud	Atlassian Confluence	WinRAR	Veeam Backup and Recovery	MySQL server	NPM library	Apache ActiveMQ	MOVEit	Cacti	Cisco router	Zyxel NAS device	Microsoft Outlook	iOS	Teamviewer	Barracuda Email Security Gateway	Mastodon	Google Chrome	Google webserver
		JumpCloud	Atlassian Jira		Veritas Backup Exec	Redis	Python library	Apache Strut	WS_FTP server	Cisco IOS XE	D-Link router		PaperCut	Linux		Emsisoft anti-virus	Signal	Microsoft Edge	IIS server
		Microsoft Azure	Joomla				Packagist	Docker		Cisco VPN	DrayTek Vigor router		Zoho ManageEngine	macOS		Ivanti Endpoint Mobile Manager	Telegram	Mozilla Firefox	Nginx
		Microsoft 365	Microsoft Streaming Service					Github		Citrix Netscaler ADC	Juniper router			Microsoft Windows		Keepass			
		ownCloud	Microsoft Teams					JetBrains TeamCity		Citrix Netscaler Gateway	NETGEAR router					LastPass			
		VMware Cloud Foundation	Microsoft Exchange Server					Kubernetes		F5 BIG-IP	TP-Link router					Microsoft OAuth			
		Western Digital My Cloud	Oracle E-Business Suite					Microsoft Powerapps		Fortinet - FortiGate	Ubiquiti router								
			Roundcube					Mocky		Fortinet- FortiOS									
			SharePoint					Notepad++		Fortinet - FortiWeb									
			WordPress plugin					Oracle Weblogic server		VMware Aria Operations for Networks									
			Zimbra					Progress Telerik server		VMware vRealize Log Insight									
			Zoom					Progress Telerik UI											
								Visual Studio Code extension											

Exploitation level	Definition
Low	Product targeted in one attack in our vicinity
Medium	Product targeted in at least two attacks in our vicinity
High	Product targeted in significant attacks | exploited by APT groups

[i] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a

[ii] https://therecord.media/nobelium-hacking-group-stealing-credentials

[iii] https://www.cert.europa.eu/static/files/TLP-CLEAR-JointPublication-23-01.pdf

[iv]https://www.securityweek.com/fortinet-warns-customers-of-possible-zero-day-exploited-in-limited-attacks/

[v] https://vulnera.com/newswire/massive-cyberattack-targets-cisco-ios-xe-devices-through-cve-2023-20198-exploitation/

[vi] https://www.mandiant.com/resources/blog/session-hijacking-citrix-cve-2023-4966

[vii] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a

[viii] https://www.welivesecurity.com/en/eset-research/pernicious-potpourri-python-packages-pypi/

[ix]https://www.bleepingcomputer.com/news/security/1password-discloses-security-incident-linked-to-okta-breach/

[x] https://www.bleepingcomputer.com/news/security/lastpass-breach-linked-to-theft-of-44-million-in-crypto/

[xi]https://www.cisa.gov/news-events/alerts/2023/08/01/cisa-and-international-partner-ncsc-no-release-joint-cybersecurity-advisory-threat-actors-exploiting

[xii]https://blog.sucuri.net/2023/10/balada-injector-targets-unpatched-tagdiv-plugin-newspaper-theme-wordpress-admins.html

[xiii] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-289a

[xiv] https://twitter.com/msftsecintel/status/1681695399084539908?s=12&t=tDVP3ULf1Ou5szxCQAKqjA

[xv] https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise

[xvi] https://ec.europa.eu/eurostat/web/products-eurostat-news/internet/ddn-20231208-1

[xvii]https://www.microsoft.com/en-us/security/blog/2023/07/14/analysis-of-storm-0558-techniques-for-unauthorized-email-access/

[xviii] https://www.mandiant.com/resources/blog/north-korea-supply-chain

[xix] https://www.microsoft.com/en-us/security/blog/2023/10/03/defending-new-vectors-threat-actors-attempt-sql-server-to-cloud-lateral-movement/

[xx] https://research.checkpoint.com/2023/chinese-threat-actors-targeting-europe-in-smugx-campaign/

[xxi] https://blogs.blackberry.com/en/2023/03/nobelium-targets-eu-governments-assisting-ukraine

[xxii]https://blog.eclecticiq.com/mustang-panda-apt-group-uses-european-commission-themed-lure-to-deliver-plugx-malware

[xxiii] https://blogs.blackberry.com/en/2023/03/nobelium-targets-eu-governments-assisting-ukraine

[xxiv] https://www.gov.pl/attachment/48cb27d1-5a31-46fe-9a18-aedbed03ed5f

[xxv] https://www.gov.pl/attachment/48cb27d1-5a31-46fe-9a18-aedbed03ed5f

[xxvi] https://www.microsoft.com/en-us/security/blog/2023/09/14/peach-sandstorm-password-spray-campaigns-enable-intelligence-collection-at-high-value-targets/

[xxvii] https://www.trendmicro.com/en_us/research/23/j/void-rabisu-targets-female-leaders-with-new-romcom-variant.html

[xxviii] https://www.csoonline.com/article/650994/russia-linked-attackers-hit-uk-ministry-of-defence-leak-security-data.html

[xxix] https://msrc.microsoft.com/blog/2023/03/microsoft-mitigates-outlook-elevation-of-privilege-vulnerability/

[xxx] https://www.bitdefender.com/blog/businessinsights/unpacking-bellaciao-a-closer-look-at-irans-latest-malware

[xxxi]https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/

[xxxii] https://www.mandiant.com/resources/blog/infected-usb-steal-secrets

[xxxiii] https://www.sentinelone.com/labs/winter-vivern-uncovering-a-wave-of-global-espionage/

[xxxiv] https://securityaffairs.com/141695/cyber-warfare-2/killnet-hit-dutch-european-hospitals.html

[xxxv] https://www.infosecurity-magazine.com/news/lazarus-internet-healthcare/

[xxxvi] https://therecord.media/philippines-state-health-insurer-struggles-with-ransomware

[xxxvii]https://msrc.microsoft.com/blog/2023/03/microsoft-mitigates-outlook-elevation-of-privilege-vulnerability/

[xxxviii] https://therecord.media/danish-energy-companies-hacked-firewall-bug

[xxxix]https://www.microsoft.com/en-us/security/blog/2023/08/02/midnight-blizzard-conducts-targeted-social-engineering-over-microsoft-teams

[xl]https://www.trendmicro.com/en_us/research/23/internet/earth-estries-targets-government-tech-for-cyberespionage.html

[xli] https://unit42.paloaltonetworks.com/agonizing-serpens-targets-israeli-tech-higher-ed-sectors/

[xlii] https://analyst1.com/ransomware-diaries-volume-3-lockbits-secrets/

[xliii] https://therecord.media/lockbit-ransomware-group-threatens-royal-mail-data-leak-deadline

[xliv] https://securityaffairs.com/142477/cyber-crime/lockbit-water-utility-aguas-do-porto.html

[xlv] https://www.bleepingcomputer.com/news/security/lockbit-ransomware-disrupts-emergency-care-at-german-hospitals/