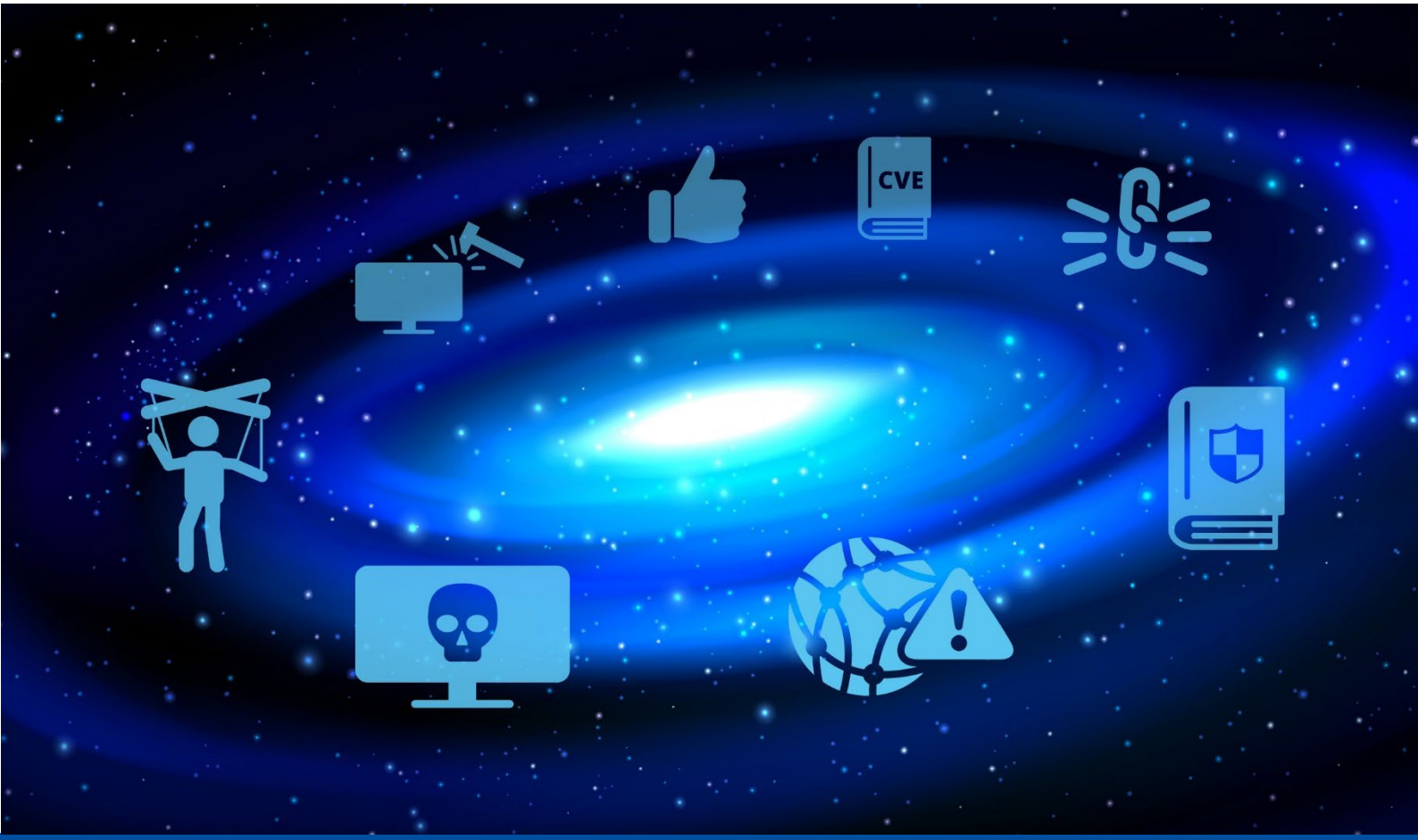
EUROPEAN UNION AGENCY
FOR CYBERSECURITY



ENISA THREAT LANDSCAPE 2023

July 2022 to June 2023

OCTOBER 2023

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure, and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

CONTACT

To contact the authors, please use etl@enisa.europa.eu
For media enquiries about this paper, please use press@enisa.europa.eu.

EDITORS

Ifigeneia Lella, Eleni Tsekmezoglou, Marianthi Theocharidou, Erika Magonara, Apostolos Malatras, Rossen Svetozarov Naydenov, Cosmin Ciobanu – European Union Agency for Cybersecurity

CONTRIBUTORS

Claudio Ardagna, Stephen Corbiaux, Koen Van Impe, Radim Ostadal

ACKNOWLEDGEMENTS

We would like to thank the Members and Observers of the ENISA ad hoc Working Group on Cyber Threat Landscapes for their valuable feedback and comments in validating this report. We would also like to thank the ENISA Advisory Group and the National Liaison Officers network for their valuable feedback.

We would also like to thank the EEAS Strategic Communication Task Forces and Information Analysis Division (SG. STRAT.2) for sharing the data on information manipulation and revising and contributing to the chapter on information manipulation.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-645-3, DOI: 10.2824/782573

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The ENISA Threat Landscape (ETL) report, now in its eleventh edition, plays a crucial role in understanding the current state of cybersecurity mainly within the European Union (EU). It provides valuable insights into emerging trends in terms of cybersecurity threats, threat actors' activities as well as vulnerabilities and cybersecurity incidents. Accordingly, the ETL aims at informing decisions, priorities and recommendations in the field of cybersecurity. It identifies the top threats and their particularities, threat actors' motivations and attack techniques, as well as provides a deep-dive insight on particular sectors along with a relevant impact analysis. The work has been supported by ENISA's ad hoc Working Group on Cybersecurity Threat Landscapes (CTL).

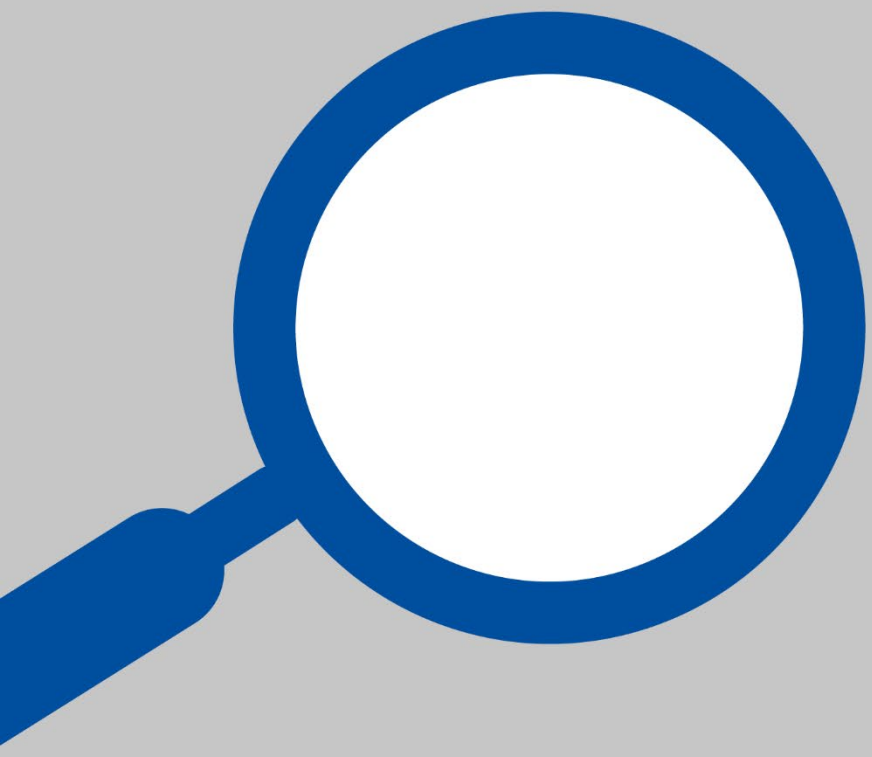
In the latter part of 2022 and the first half of 2023, the cybersecurity landscape witnessed a significant increase in both the variety and quantity of cyberattacks and their consequences. The ongoing war of aggression against Ukraine continued to influence the landscape. Hacktivism has expanded with the emergence of new groups, while ransomware incidents surged in the first half of 2023 and showed no signs of slowing down. The prime threats identified and analysed include:

- Ransomware
- Malware
- Social engineering
- Threats against data
- Threats against availability: Denial of Service
- Threat against availability: Internet threats
- Information manipulation and interference
- Supply chain attacks

For each of the identified threats, we determine impact, motivation, attack techniques, tactics and procedures to map relevant trends and propose targeted mitigation measures. During the reporting period, key findings include:

- **DDoS and ransomware rank the highest among the prime threats**, with social engineering, data related threats, information manipulation, supply chain, and malware following.
- A **noticeable rise was observed in threat actors professionalizing their as-a-Service programs**, employing novel tactics and alternative methods to infiltrate environments, pressure victims, and extort them, advancing their illicit enterprises.
- **ETL 2023 identified public administration as the most targeted sector** (~19%), followed by targeted individuals (~11%), health (~8%), digital infrastructure (~7%) and manufacturing, finance and transport.
- **Information manipulation has been as a key element of Russia's war of aggression against Ukraine** has become prominent.
- **State-nexus groups maintain a continued interest on dual-use tools** (to remain undetected) and on trojanising known software packages. **Cybercriminals increasingly target cloud infrastructures, have geopolitical motivations in 2023 and increased their extortion operations**, not only via ransomware but also by directly targeting users.
- **Social engineering attacks grew significantly in 2023** with Artificial Intelligence (AI) and new types of techniques emerging, but phishing still remains the top attack vector.

The key findings and judgments in this assessment are based on multiple and publicly available resources which are provided in the references used for the development of this document. The report is mainly targeted at strategic decision-makers and policy-makers, while also being of interest to the technical cybersecurity community.



1. THREAT LANDSCAPE OVERVIEW

In its eleventh edition, the ENISA Threat Landscape (ETL) report offers a broad overview of the cybersecurity threat landscape. Over time, the ETL has served as a crucial tool for comprehending the present state of cybersecurity within the European Union (EU), furnishing insights into trends and patterns. This, in turn, has guided pertinent decisions and prioritisation of actions and recommendations. The ETL report combines strategic and technical elements, catering to both technical and non-technical audiences. The ETL 2023 report has been validated and supported by the ENISA ad hoc Working Group on Cybersecurity Threat Landscapes (CTL)[1] and the ENISA National Liaison Officers (NLO) Network.

Throughout the latter part of 2022 and the initial half of 2023, there was a notable escalation in cybersecurity attacks, setting new benchmarks in both the variety and number of incidents, as well as their consequences. The ongoing war of aggression against Ukraine remains a significant factor shaping the cybersecurity landscape. The phenomenon of hacktivism has seen steady expansion, marked by the emergence of numerous new groups. Concurrently, it was observed that a rise of ransomware groups took place, with the first half of 2023 witnessing an unprecedented surge in ransomware incidents, a trend that shows no signs of abating.

Additional focus was concentrated on the various kinds of impacts cyber threats have in critical sectors, including the sectors listed in the Network and Information Security Directive 2 (NISD 2). Interesting insights may be drawn from the particularities and insight of each sector when it comes to the threat landscape, as well as potential interdependencies and areas of significance. ENISA is following up by developing sectorial threat landscapes, diving deeper into the elements of each sector and providing targeted insight.

The ETL 2023 report follows the same customary approach, drawing from diverse open-source data and cyber threat intelligence sources. It pinpoints significant threats, discerns emerging trends and offers practical high-level strategies for mitigating risk. This year's ETL continues to use the officially endorsed ENISA Cyber Security Threat Landscape Methodology[2], which was released in 2022. The ENISA CTL Methodology serves as a foundational framework for the transparent and systematic creation of comprehensive cybersecurity threat landscapes, spanning horizontal, thematic, and sector-specific perspectives. This process is characterised by rigorous data collection and analysis procedures.

1.1 PRIME THREATS

A series of cyber threats emerged and materialised during the reporting period. According to the findings detailed in this report, the ENISA Threat Landscape 2023 report highlights and directs attention toward eight prime threat groups (refer to Figure 1). These particular threat groups have been singled out due to their prominence over the years, their widespread occurrence and the significant impact resulting from the realisation of these threats.

- **Ransomware**
  According to ENISA's Threat Landscape for Ransomware Attacks[3] report, ransomware is defined as a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the asset's availability. This action-agnostic definition is needed to cover the changing ransomware threat landscape, the prevalence of multiple extortion techniques and the various goals, other than solely financial gains, of the perpetrators. Ransomware has been, once again, one of the prime threats during the reporting period, with several high profile and highly publicised incidents.

- **Malware**
  Malware, also referred to as malicious code and malicious logic, is an overarching term used to describe any software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity or availability of a system.

[1] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes.
[2] https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology
[3] ENISA Threat Landscape for Ransomware Attacks https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks.

- **Social Engineering**
  Social engineering encompasses a broad range of activities that attempt to exploit human error or human behaviour with the objective of gaining access to information or services. It uses various forms of manipulation to trick victims into making mistakes or handing over sensitive or secret information. Users may be lured to open documents, files or e-mails, to visit websites or to grant access to systems or services. Although the lures and tricks used may abuse technology, they rely on a human element to be successful. This threat canvas consists mainly of the following attack vectors: phishing, spear-phishing, whaling, smishing, vishing, watering hole attack, baiting, pretexting, quid pro quo, honeytraps and scareware. While social engineering techniques are often used to gain initial access, they may also be used at later stages in an incident or breach. Notable examples are business e-mail compromise (BEC), fraud, impersonation, counterfeit and, more recently, extortion.

- **Threats against data**
  A data breach is defined in the GDPR as *any breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed* (article 4.12 GDPR). Technically speaking, threats against data can be mainly classified as data breach or data leak. Though often used as interchangeably concepts, they entail fundamentally different concepts that mostly lie in how they happen[4] [5]. Data breach is an intentional cyber-attack brought by a cybercriminal with the goal of gaining to unauthorised access and release sensitive, confidential or protected data. In other words, a data breach is a deliberate and forceful attack against a system or organisation with intention to steal data. Data leak is an event (e.g. misconfigurations, vulnerabilities or human errors) that can cause the unintentional loss or exposure of sensitive, confidential or protected data (intentional attacks are sometimes referred to as data exposure).

- **Threats against availability: Denial of Service**
  Availability is the target of a plethora of threats and attacks, among which DDoS stands out. DDoS targets system and data availability and, though it is not a new threat, it plays a significant role in the cybersecurity threat landscape[6] [7]. Attacks occur when users of a system or service are not able to access relevant data, services or other resources. This can be accomplished by exhausting the service and its resources or overloading the components of the network infrastructure[8].

- **Threats against availability: Internet threats**
  Threats to Internet availability refer to intentional or unintentional disruptions of Internet or electronic communications that result in Internet outages, blackouts, shutdowns or censorship. Internet disruptions can be due to government-directed Internet shutdowns, cyclones, massive earthquakes, power outages, cable cuts, cyberattacks, technical problems and military actions. These threats are diversifying and growing, having reached a new record in this reporting period and having caused huge monetary loss to national economies.

- **Information Manipulation**
  Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. FIMI can be carried out by state or non-state actors, including their proxies inside and outside of their own territory, whereas in this report we study the threat regardless of its origin.

- **Supply Chain Attacks**
  A supply chain attack targets the relationship between organisations and their suppliers[9]. For this ETL report we use the definition as stated in the ENISA Threat Landscape for Supply Chain Attacks[10] in which an attack is considered to have a supply chain component when it consists of a combination of at least two attacks. For an attack to be classified as a supply chain attack, both the supplier and the customer have to be targets. SolarWinds was one of the first revelations of this kind of attack and showed the potential impact of supply chain attacks. It

[4] https://blog.f-secure.com/data-breach-and-data-leak-whats-the-difference .
[5] https://www.upguard.com/blog/data-breach-vs-data-leak#:~:text=Simply%20put%2C%20a%20data%20leak,Apps%20data%20leak%20in%202021
[6] Federal Office for Information Security (BSI), The State of IT Sec in Germany, September 2020.
[7] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020.
[8] CISA, Understanding Denial-of-Service Attacks, November 2019. https://www.uscert.gov/ncas/tips/ST04-015.
[9] https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.
[10] ENISA Threat Landscape for Supply Chain Attacks https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.

was observed that threat actors are continuing[11] to feed on this source to conduct their operations and gain a foothold within organisations, to benefit from the widespread impact and large victim base of such attacks.

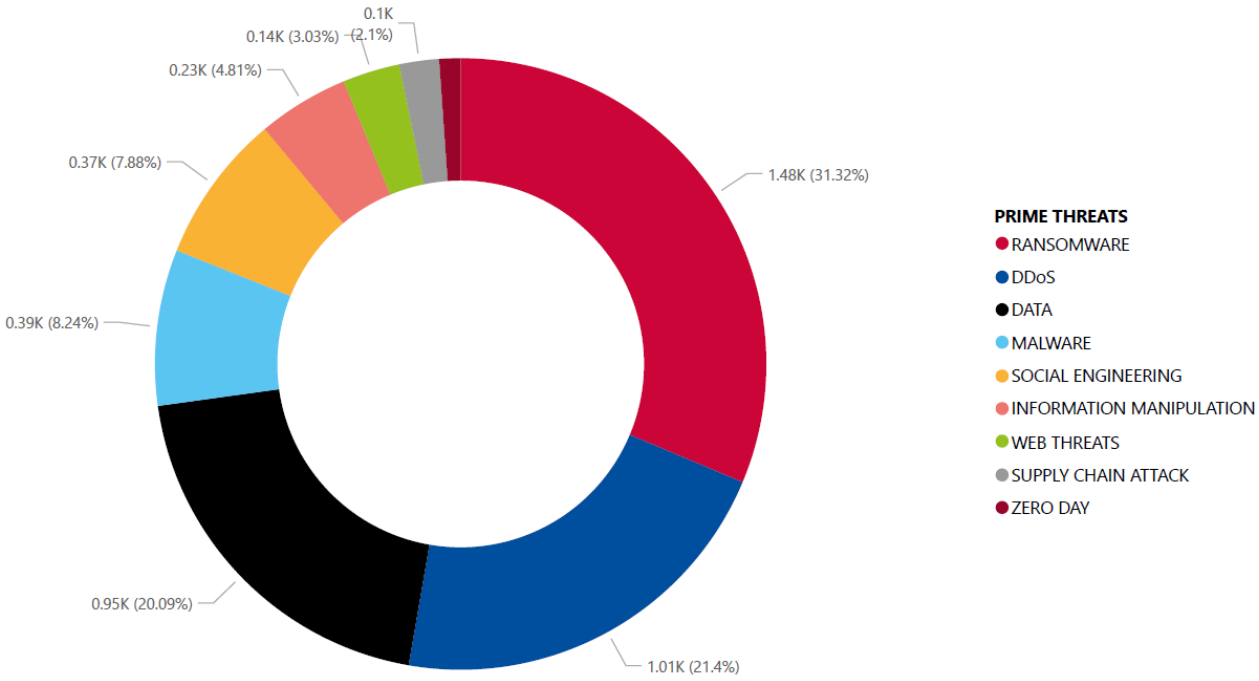
Figure 1: ENISA Threat Landscape 2022 - Prime threats

It should be noted that the aforementioned threats involve categories and refer to collections of diverse types of threats that have been consolidated into the eight areas mentioned above. Each of the threat categories is further analysed in a dedicated chapter in this report, which elaborates on its particularities and provides more specific information on findings, trends, attack techniques and mitigation vectors.

In the following figure it can be seen that ransomware and DDoS attacks were the most reported forms of attack during the reporting period and accounted for nearly half of the observed events followed by threats related to data. Moreover, we need to stress out that in several cases incidents involved more than one threat category and were thus analysed in the context of all respective categories. Given that the ETL is based on publicly available information and the fact that such information might not always provide the full picture, in certain cases incidents were not able to be classified into any threat category.

[11] Accenture Cyber Threat Intelligence Report https://www.accenture.com/ae-en/insights/security/cyber-threat-intelligence.

Figure 2: Breakdown of analysed incidents by threat type (July 2022 till June 2023)



1.2 KEY TRENDS

The list below summarises the main trends observed in the cyber threat landscape during the reporting period. Further details and analysis on the trends may be found throughout the various chapters that comprise the ENISA threat landscape of 2023.

- **Ransomware and threats against availability ranked at the top during the reporting period.**
- **Resourceful threat actors have been observed to misuse legitimate tools** primarily to prolong their cyber espionage operations . Their aim was to evade detection for as long as possible and obscure their activities by using widely available software from most systems which makes it more challenging for defenders to identify them. Maximizing their chances of success when it comes to an intrusion by not arousing victim' suspicions
- **Geopolitics continue to have a strong impact on cyber operations.**
- **Several threat actors further professionalised**[12] [13] their As-a-Service programmes. They not only used novel tactics and methods to infiltrate environments but also delved into alternative approaches to pressure and extort victims, all the while advancing their illicit enterprises.
- **By Using Extortion Only Techniques** criminal organisations have been progressively blending extortion methods that almost invariably incorporate some form of data theft. Double extortion has witnessed a notable rise, with certain groups even relying solely on the act of stealing information.
- **Increased operations by law enforcement,** such as the takedown of Hive ransomware group's IT infrastructure or Trickbot.
- **Cl0p rose** in the first half of 2023 with the weaponisation of two zero-days.
- **One of the biggest malware threats is still information stealers** such as Agent Tesla, Redline Stealer and FormoBook.
- **There is a steady decline in classic mobile malware**, with adware remaining in numbers of occurrences the most prevalent threat to mobile devices while in terms of impact spyware can be seen as the most prevalent threat to mobile devices.

[12] PWC - Cyber Threats 2022: A Year in Retrospect - https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/pdf/2022-year-in-retrospect-report.pdf.
[13] Group IB - Hi-Tech Crime Trends 2022/2023 – https://go.group-ib.com/hubfs/report/protected/group-ib-hi-tech-crime-trends-2022-2023-en.pdf.

- **Hacktivists are increasingly claiming[14] that they target OT environments** but public reporting indicate they often[15] **overestimate** or **do not substantiate** their claims.
- **Phishing is once again the most common vector** for initial access. But a new model of social engineering is also emerging, an approach that consists of **deceiving victims in the physical world**.
- **Business e-mail compromise (BEC, VEC) remains** one of the attacker's favourite means for obtaining financial gain.
- **The move from Microsoft macros to ISO , Onenote and LNK files is continuing,** a shift towards the use of LNK and ISO/ZIP files as well as Onenote files in response to Microsoft's macro changes.
- **Data compromise increased in 2023**. There was a rise in data compromises leading up to 2021, and although this trend remained relatively stable in 2022, it began to increase once more in 2023.
- **There has been a Surge in AI Chatbots impacting the cybersecurity threat landscape.** The disruptive impact and the exponential adoption of generative artificial intelligence chatbots such as OpenAI ChatGPT, Microsoft Bing and Google Bard are changing the way in which we work, live and play, all built around data sharing and analysis.
- **DDoS attacks are getting larger and more complex, are moving towards mobile networks and IoT and are being used in the context of** being used in support of additional means in the context of a conflict**.**
- **Internet shutdowns are at an all-time high.** Internet availability threats are keeping up their momentum, especially in the post-covid era, due to the increasing reliance of human activities and society on Internet technologies.
- **Information manipulation is a key element of Russia's war of aggression against Ukraine**. Information manipulation has been an essential and well-established component of Russia's security strategies[16] [17]. The number of analysed events for the reporting period has also grown significantly.
- **'Cheap fakes' and AI-enabled manipulation of information** continues to be a cause for concern. In the past months, the debate on the use of AI to manipulate information has heated up both within and beyond the circle of industry professionals.
- **Threat groups have an increased interest in supply chain attacks and exhibit an increasing capability by using employees as entry points.** Threat actors will continue to target employees with elevated privileges, such as developers or system administrators

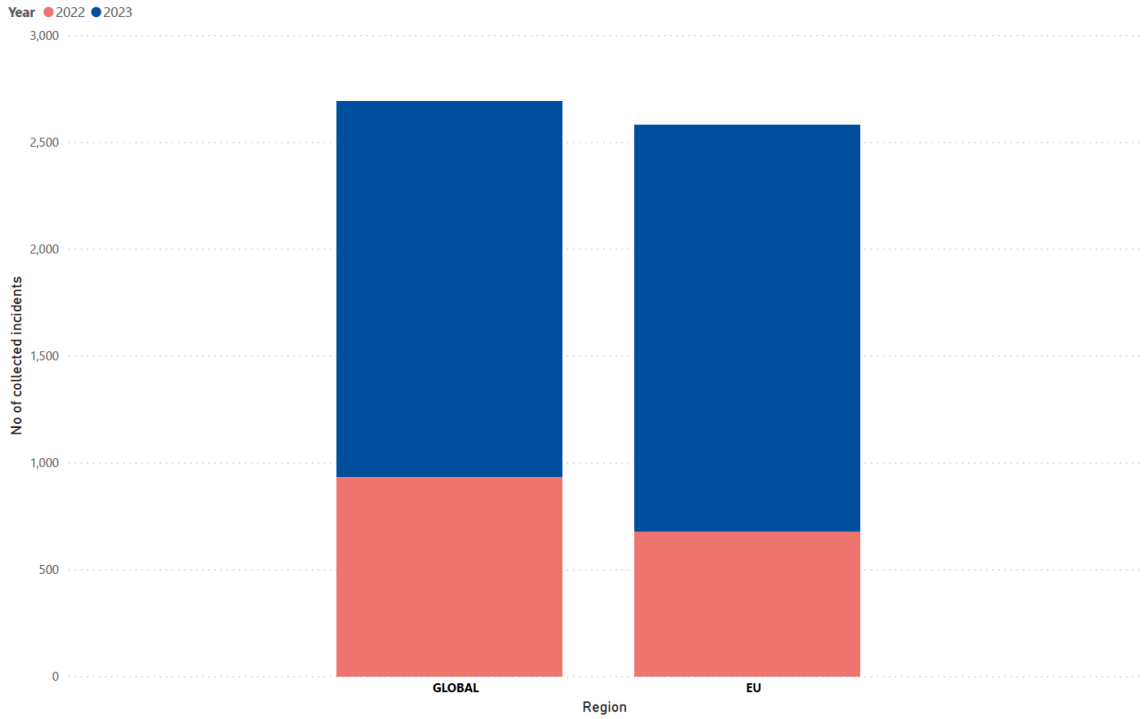
1.3 EU PRIME THREATS

Cyberattacks continue to increase on the global scale; however, ENISA's scope is primarily focused on EU member states and thus more emphasis is placed on the EU landscape.

Figure 3 makes it evident that, starting from the first half of 2023, both global (i.e. non-EU) and EU events have shown a relevant increase. However, it is important to note that the number of events observed can be influenced by various factors. An uptick in reported cyberattacks does not necessarily imply an actual increase in number of attacks or the strength of their impacts. This rise could be attributed to media or public attention being focused on specific events for a certain period, resulting in more incidents being documented in open-source intelligence (OSINT) channels or threat actors claiming victims in their sites or telegram channels with no real impact on those victims.

[14] Mandiant - We (Did!) Start the Fire: Hacktivists Increasingly Claim Targeting of OT Systems - https://www.mandiant.com/resources/blog/hacktivists-targeting-ot-systems.
[15] Claroty - Hacktivist Group Claims Ability to Encrypt an RTU Device – https://claroty.com/team82/blog/hacktivist-group-claims-ability-to-encrypt-an-rtu-device.
[16] No Water's Edge: Russia's Information War and Regime Security (2023, Carnegie Endowment for International Peace).
[17] https://raport.valisluureamet.ee/2023/en/russian-armed-forces/1-3-russia-continues-to-look-for-a-weak-link-in-ukrainian-cyberspace/.

Figure 3: Break down of Global and EU events (July 2022 – June 2023)



Furthermore, as ENISA enhances its cyber threat intelligence capabilities, we anticipate an increase in the number of observable cyber incidents in the future. Consequently, this should help mitigate the observational bias mentioned previously and contribute to higher-quality and more informative findings.

Throughout the reporting period, EU Member States continued to be affected by the ongoing geopolitical crisis, with a growing number of threat actors directing their efforts against both public and private organisations. These kinds of events more often fall under the DDoS threat (chapter 8) with little to no impact in most of the cases reported through OSINT. Ransomware attacks have also increased (chapter 4) in the EU.

ENISA observed approximately 2 580 incidents, with an additional 220 incidents specifically targeting two or more EU Member States (labelled 'EU') as it can be seen in Figure 4 which shows a timeline of when the events where first reported through the OSINT channels. In addition, throughout this iteration of the ETL it can be seen that Ransomware and DDoS still remain the two prime threats for the EU as shown in Figure 5.

Figure 4: Timeline of EU events (count of number of observed incidents per month)

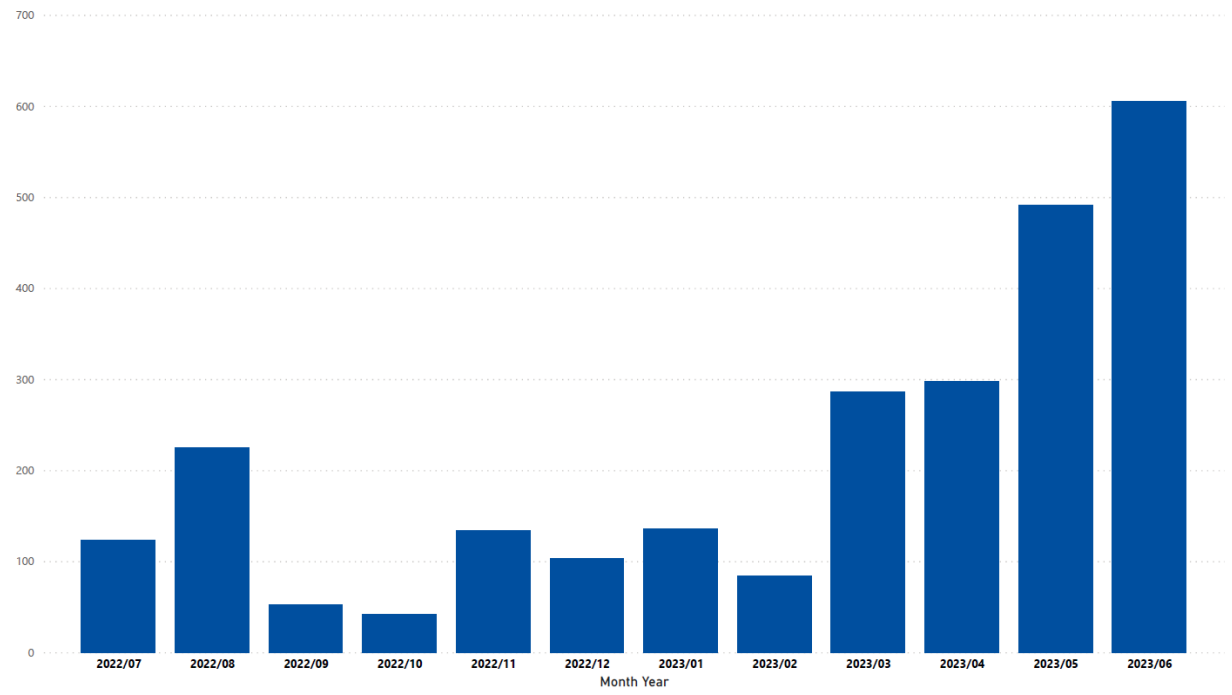
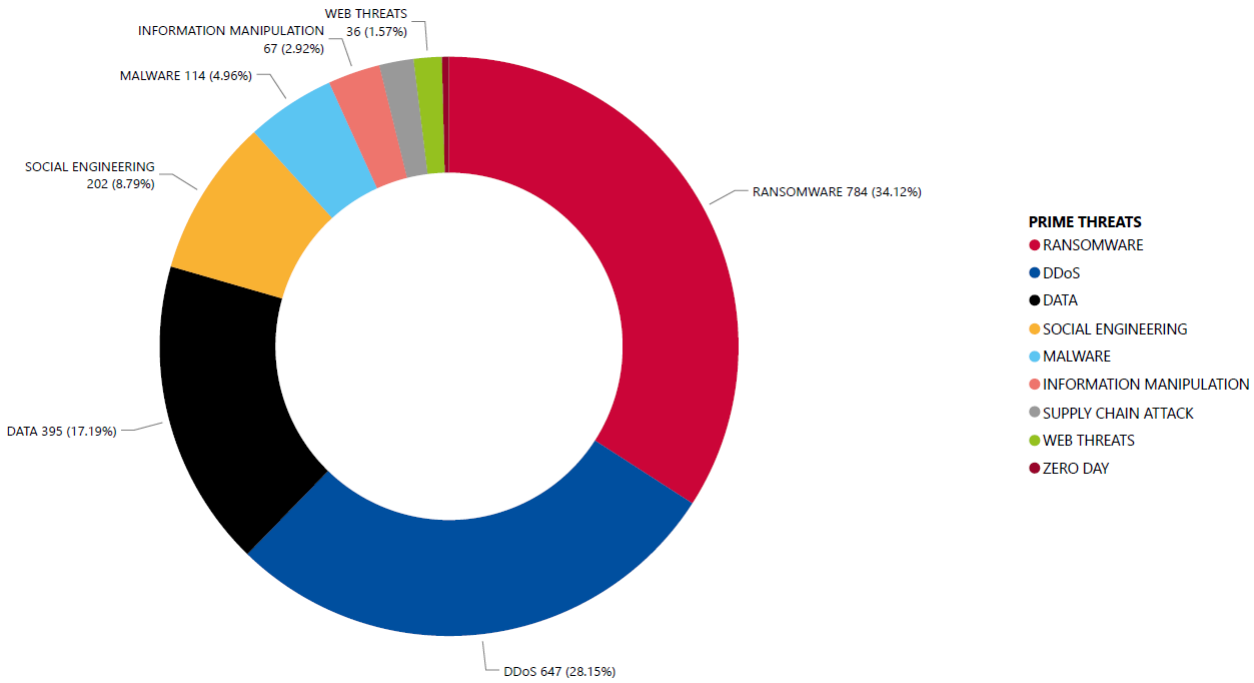


Figure 5: EU breakdown of number of threats by threat group

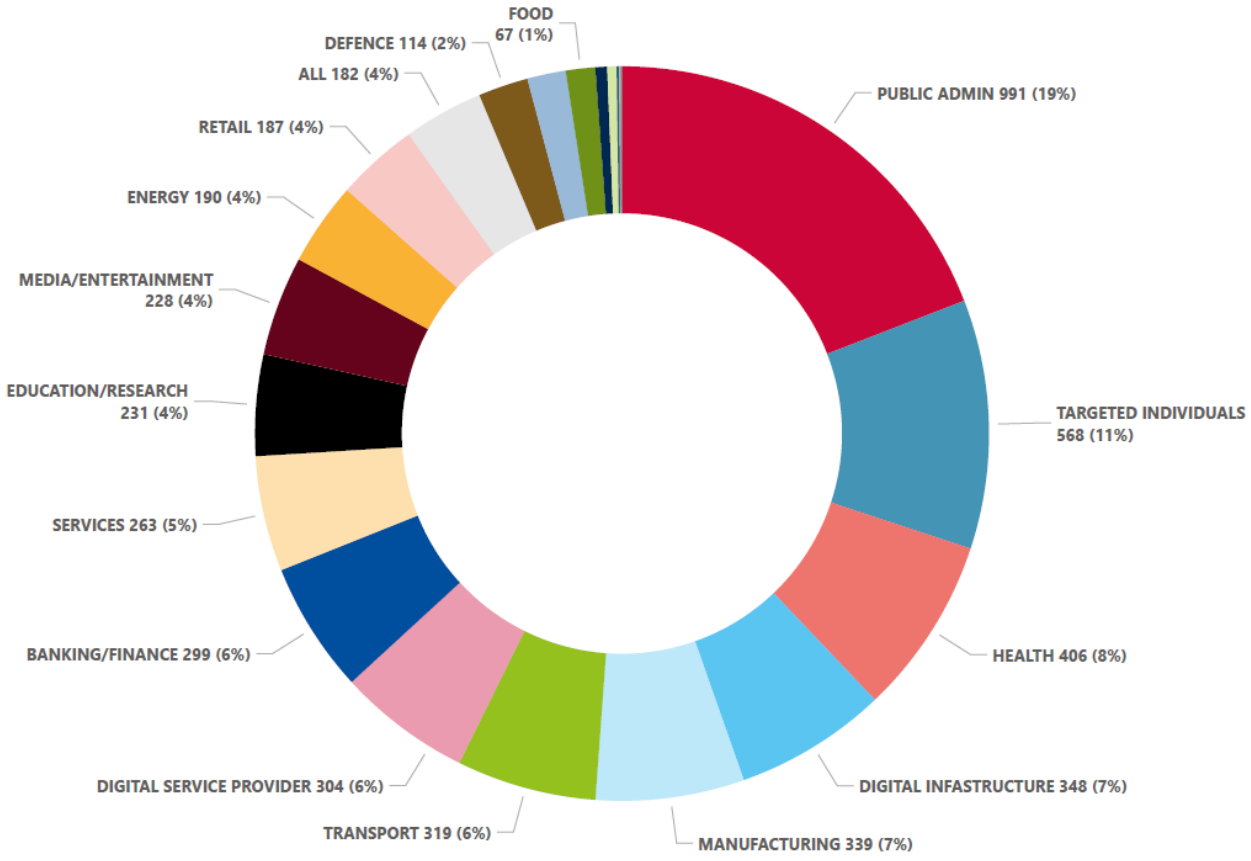


1.4 SECTORAL ANALYSIS

Cyber threats transcend the boundaries of specific industries or sectors, exerting their influence across a broad spectrum of areas. This phenomenon is a tribute to the pervasive nature of digital interconnectivity in today's world. As demonstrated by the following figures, it becomes apparent that threat actors spare no sectors from their targeting endeavours, reinforcing the notion that no sector remains unaffected by their actions.

The sectors analysed in this report in general follow the classification of the sector categories of the Network and Information Security Directive (NIS2)[18]. There are however some deviations, derived by the sample used, as it may include events affecting sectors beyond the scope of the NIS2 directive. Examples include Defence, Education[19], Media and entertainment, the Retail sectors and more. We have also grouped under the term 'Digital service provider', the sectors listed in NIS2 as ICT service management (MSPs and MSSPs) and Digital providers. There is also a separate category, labelled as 'all sectors' which is used when events have a global effect across sectors. During the analysis, a lot of other sectors were identified that relate to various services that are not currently within the scope of the NIS2 directive. These include consulting services, legal services, hospitality services etc, and are grouped under the category 'Services'.

Figure 6: Targeted sectors per number of incidents (July 2022 - June 2023)



During this reporting period in the overall global landscape, we have again observed a large number of events (Figure 6) targeting organisations in the public administration (19%) and health (8%) sectors. Events targeting digital infrastructure (7%) and digital service providers (6%) form a substantial portion of the events observed. These are events that affect more than one sector due to the reliance of the other sectors on these two sectors. We also observed a considerable number of events targeting civil society and not necessarily a particular sector (these are labelled as 'Targeted individuals' and amount to 11% of the events observed). They consist of social engineering or

[18] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2555.
[19] The education sector was coupled in our sample with the research sector, as they are often intertwined. While the research sector is considered in the scope of the NIS2 directive, educational organisations are not included.

information manipulation campaigns. The manufacturing, transport and finance sectors all faced around 6% of the events each throughout the reporting period.

The prime threat was ransomware and it appears to target the entire range of the sectors (Figure 7). The most targeted sectors were manufacturing (14% out of ransomware events), health (13%), public administration (11%) and services (9%).

These are followed by DDoS attacks and data-related threats. Thirty-four per cent of the DDoS attacks targeted public administration, followed by the transport (17%) and banking/finance sectors (9%). Data related threats targeted all sectors, with the ones that hold personal information being more affected. These included public administration (16%) and health (10%) as well as targeted individuals (15%).

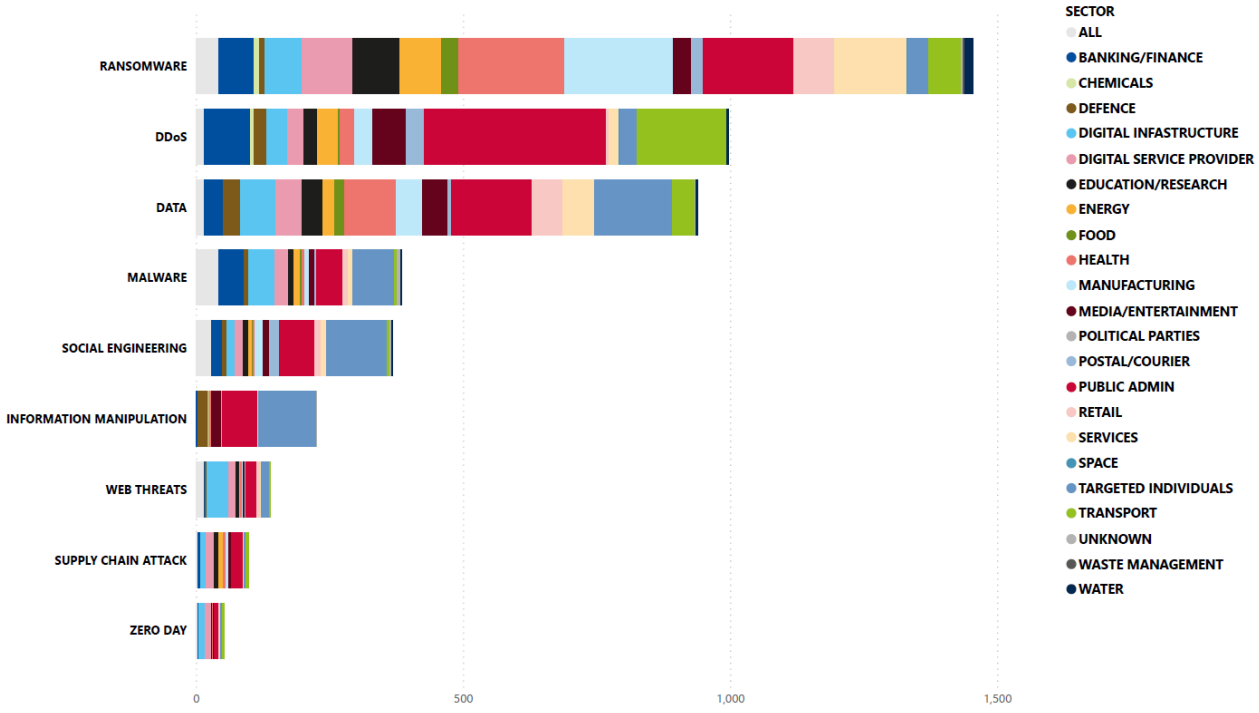
One fifth of the events involving as malware affected the general public (targeted individuals, 20%), followed by malware infections in public administration (13%), digital infrastructure (13%), banking and finance (12%) and digital service providers (7%). All sectors were targeted by 11% of the reported malware infections.

Out of the observed events related to social engineering, 30% were aimed at the general public, 18% at public administration and 8% at all sectors. Likewise, information manipulation campaigns targeted individuals (47%), public administration (29%), followed by the defence (9%) and media/entertainment (8%) sectors.

As expected, threats against the availability of the Internet primarily affected digital infrastructure (28%) and digital service providers (10%). Public administration (15%), individuals (10%) and 'all sectors' (11%) were also affected, as they are dependent on digital infrastructure and services.

Supply chain attacks affected public administration (21%) and involved primarily the digital service providers (16%), digital infrastructure (10%) and energy (9%) sectors. Likewise, the exploitation of vulnerabilities was associated with events targeting digital service providers (25%), digital infrastructures (23%) and public administration (15%), and they affected all sectors (8%) and targeted individuals (8%) to a greater degree.

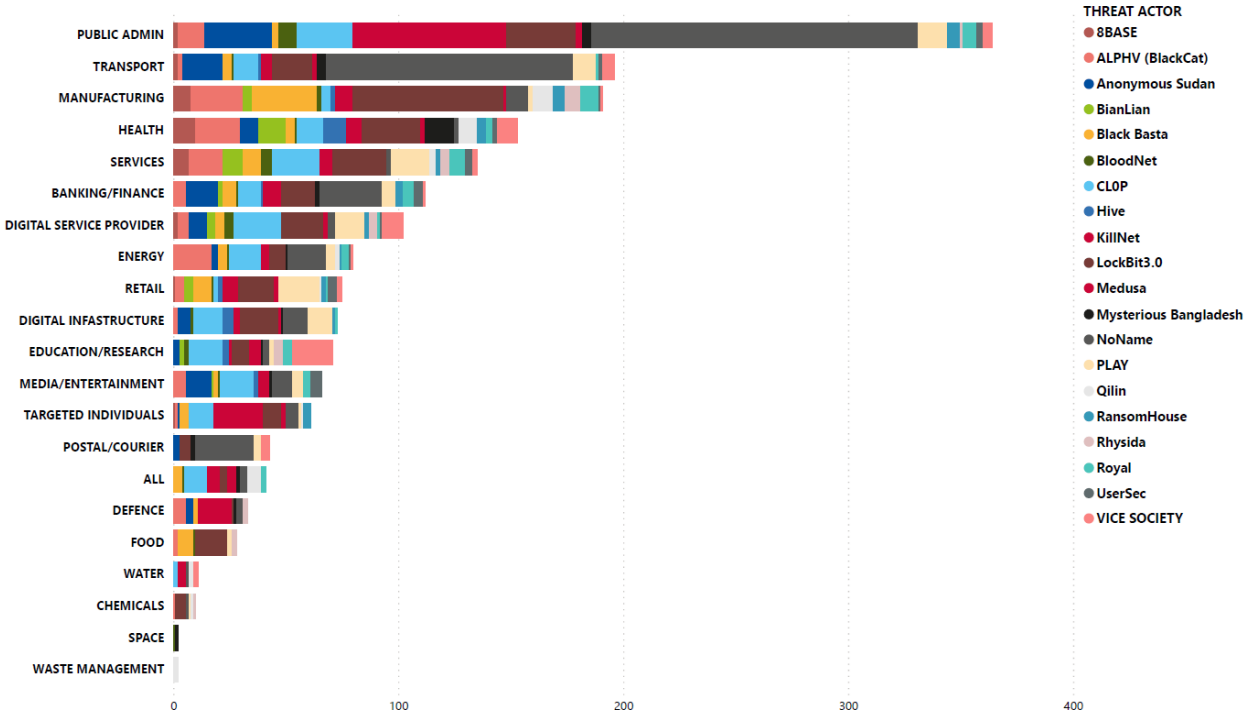
Figure 7: Observed events related to prime ETL threats in terms of the affected sector



In the breakdown of the top 20 'active' threat actors during the reporting period, the trend that activity by actors is often sector-agnostic becomes evident once more, as nearly all these threat actors are dispersed across various

sectors. This can be further be seen when dealing with cybercriminals (chapter 2) as they are assessed to be opportunistic by nature.

Figure 8: Threat actor by sector



1.5 IMPACT ASSESSMENT

In this iteration of ENISA's threat landscape we have again included an assessment of the impacts of the events observed. We followed a qualitative process of impact analysis in order to identify the consequences of an event. Due to the fact that information related to the impact of cyberattacks is often not available or made public, determining and assessing the effect following an incident entails a level of assumption in which a certain degree of subjectivity cannot be avoided. This in itself makes the argument for improving the process of incident reporting in the EU, an aspect that is reflected in the NIS2 Directive and an area where ENISA will continue its efforts in the coming years.

In the context of this ETL report, we defined and applied the following types of impact.

- **Digital impact** refers to damaged or unavailable systems, corrupted data files or exfiltration of data or some announced malicious intrusion.
- **Economic impact** refers to the direct financial loss incurred, the damage to national security that can be caused due to the loss of important material or a ransom demand.
- **Social impact** refers to any effect on the general public or to a widespread disruption that could have an impact on society (e.g. incidents disrupting the national health system of a country, leakage of any data concerning the general public's IDs, social security numbers, addresses etc.).
- **Reputational impact** refers to the potential for negative publicity or an adverse public perception of the entity that has been the victim of a cyber incident.
- **Physical impact** refers to any kind of injury or harm to employees, customers or patients.
- **Psychological impact** refers to any kind of confusion, discomfort, frustration, worry or anxiety caused to employees, customers or patients, or the general public.

The events collected were classified according to these six types of impact by applying internal ENISA experience and expertise. It is quite interesting to note that, in most of the events collected, some kind of digital impact was identified as seen in Figure 9. Digital impact was observed in one of three ways: evidence of downtime (often associated with hacktivist DDoS events, regardless of their brevity) reported by relevant vendors, data breaches or explicitly mentioned by the sources being monitored.

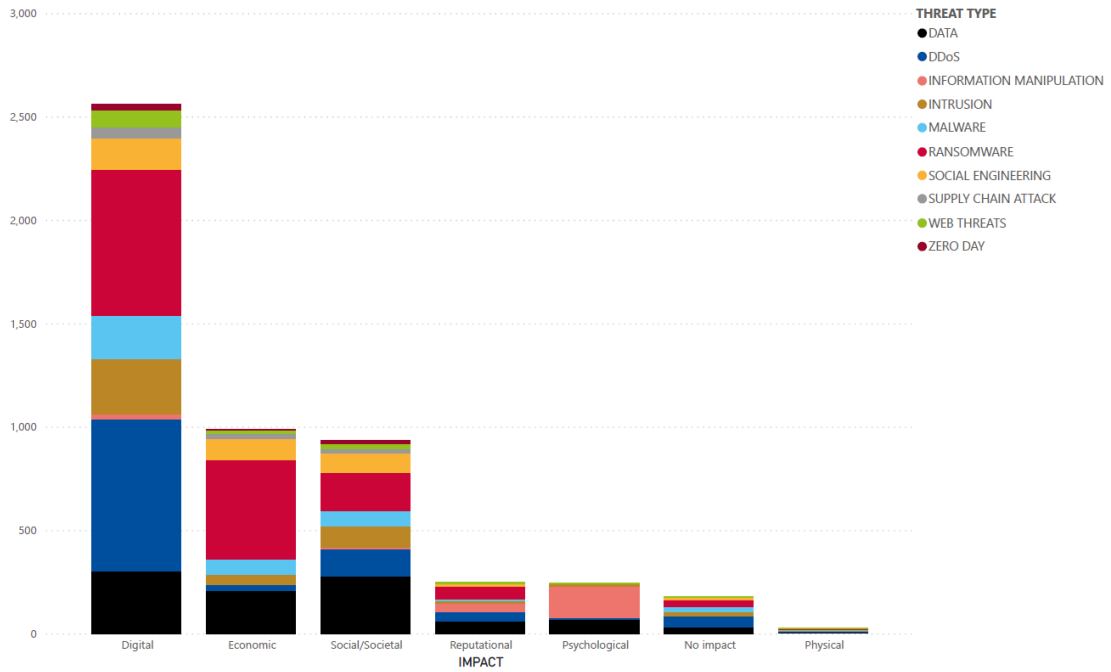
Approximately one fifth of the events collected (19%) were evaluated as having an economic impact but this assessment is based on the information available at the time of the analysis. Ransomware and DDoS incidents took centre stage due to the financial gains sought by the threat actors or due to economic losses caused by disruptions in manufacturing or in the provision of services (public administration, services, banking and finance). During the assessment, it often remained uncertain whether ransoms were actually paid, so we included such information in the assessment only when available. Data breaches were also considered to have an economic impact, primarily due to legal obligations (e.g. fines due to GDPR violations) that could arise or due to the profit made by the attackers from selling the acquired data, which were personal or proprietary information. This was observed primarily in the health and manufacturing sectors, as well as public administration, services and targeted individuals.

We assessed social impact (18%) when analysing events with a significant effect on the general public and citizens, either due to the leak of personal information or due to disruptions of services. These were mainly observed when citizens were targeted directly or indirectly when events (ransomware, DDoS) were associated with public administration and health sectors. The social impact referred mainly to the inability of the citizens to access important services provided by these two sectors.

However, it is important to highlight that the assessment of reputational, psychological and physical impacts was particularly challenging. This was due to the limited time between the incident taking place and our analysis, or due to the fact that such impacts could not be assessed solely from open sources. Reputational impact was mostly associated with ransomware, data breaches or leaks, with DDoS and information manipulation. Psychological impact was observed when examining events of information manipulation and data leaks of personal information.

Another noteworthy observation was the rarity of events categorised as having ‘No impact’; this suggests a possible hypothesis that media or the affected parties may exaggerate their impact when reporting cyber incidents.

Figure 9: Threat type breakdown by Impact



1.6 MOTIVATION

Understanding the enemy and the motivation behind a cybersecurity incident or targeted attack is important because it can determine what an adversary is after. Knowing the motives can help organisations determine and prioritise what to protect and how to protect it. It also provides an idea of the intents of attackers and helps entities focus their efforts in defence on the most likely attack scenario for any particular asset.

For all the above reasons, ETL 2023 has for the second year included an assessment of the motivation behind the incidents observed during the reporting period. For this purpose, five distinct kinds of motivation that can be linked to threat actors have been defined:

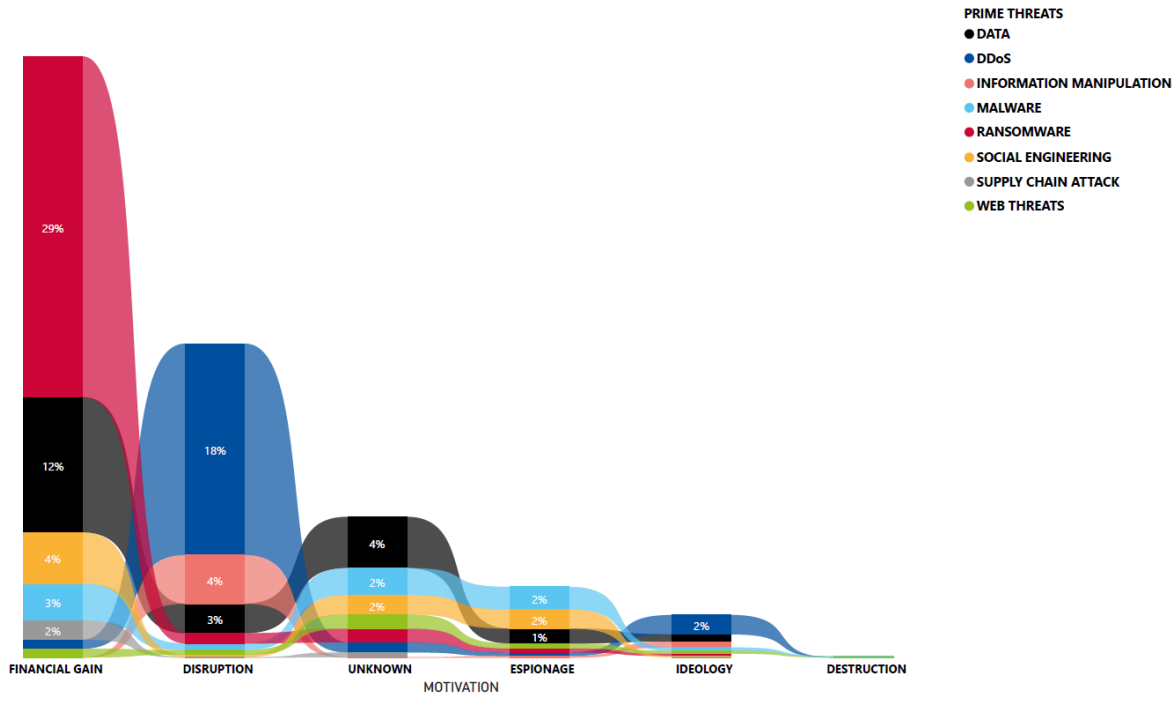
- **Financial gain**: any financially related action (carried out by mostly cybercrime groups);
- **Espionage**: gaining information on IP (Intellectual Property), sensitive data, classified data (mostly executed by state-sponsored groups);
- **Disruption**: any disruptive action done in the name of geopolitics (mostly carried out by state-sponsored groups);
- **Destruction**: any destructive action that could have irreversible consequences;
- **Ideological**: any action backed up with an ideology behind it (such as hacktivism).

It is apparent that in the majority of cases the primary threats can be attributed to one or more motivations, with certain motivations emerging as more dominant than others. Within the realm of Ransomware attacks, while the primary motivation typically revolves around financial gain, there is a small percentage where a disruptive motive also plays a role.

For a considerable number of the events we have gathered, the motivation behind them remains unclear. This lack of clarity could be due to either limited or undisclosed information or the victims themselves being unaware of the underlying motive.

Following financial gain as the top motivation, the second most common motive was disruption. While over half of these cases can be attributed to various DDoS attacks that occurred throughout the reporting period, information manipulation was also a sizeable portion of this category.

Figure 10: Motivation of threat actors per threat category



1.7 METHODOLOGY

The ENISA Cybersecurity Threat Landscape (CTL) methodology[20] was used to produce the ETL 2023 report. The methodology was published in July 2022.

The ENISA Threat Landscape (ETL) 2023 report is based on information from open sources, mainly of a strategic nature and ENISA's own Cyber Threat Intelligence (CTI) capabilities. It covers more than one sector, technology and context. The report aims to be industry and vendor agnostic. It references or cites the work of various security researchers, security blogs and news media articles throughout the text in multiple footnotes to validate findings and statements. The time span of the ETL 2023 report is July 2022 to June 2023 and is referred to as the 'reporting period' throughout the report.

During the reporting period, ENISA gathered a list of major incidents as they appeared in open sources through situational awareness. This list serves as the foundation for identifying the list of prime threats and the source material for several trends and statistics in the report.

Subsequently, an in-depth desk research of available literature from open sources such as news media articles, expert opinion, intelligence reports, incident analysis and security research reports was conducted by ENISA and external experts. Note that many intelligence and research reports are written on the basis of a January to December year, contrary to the ETL's reporting period which is from July to June. Through continuous analysis, ENISA derived trends and points of interest. The key findings and judgments in this assessment are based on multiple and publicly available resources which are provided in the references used for the development of this document.

Within the report, we differentiate between what has been reported by our sources and what is our assessment. When conducting an assessment, we convey probability by using words that express an **estimate of probability**[21].

When we refer to threat actors in this report, we use the naming convention used by the company revealing the campaign, as well as a number of synonyms[22] commonly used in the industry.

1.8 STRUCTURE OF THE REPORT

The ENISA Threat Landscape (ETL) 2023 has maintained the core structure of previous ETL reports for highlighting the prime cybersecurity threats in 2023. Those familiar with previous versions will observe that the current editions now incorporate the CVE landscape within chapters that offer an overview of the most significant CVEs identified during the reporting period. ENISA considers this inclusion to be crucial because it sheds light on yet another facet of what threat actors can exploit, as highlighted in Chapter 3. This addition also underscores the significance of vulnerability disclosure and timely patching.

This report is structured as follows:
Chapter 2 explores the trends related to threat actors
Chapter 3 includes a CVE landscape, as observed during the reporting period;
Chapter 4 discusses major findings, incidents and trends regarding ransomware;
Chapter 5 presents major findings, incidents and trends regarding malware;
Chapter 6 describes major findings, incidents and trends regarding social engineering;
Chapter 7 highlights major findings, incidents and trends regarding threats against data (data breach, data leak);
Chapter 8 discusses major findings, incidents and trends regarding threats against availability (denial of service);
Chapter 9 presents major findings, incidents and trends regarding threats against availability (internet threats);
Chapter 10 underlines the importance of hybrid threats and describes major findings, incidents and trends regarding information manipulation;
Chapter 11 focuses on major findings, incidents and trends regarding supply chain attacks.
Annex A presents the techniques commonly used for each threat, based on the MITRE ATT&CK® framework;
Annex B presents recommendations and security controls that might add to the mitigation of the threats.

[20] ENISA Cybersecurity Threat Landscape (CTL) methodology, July 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology.
[21] MISP estimative language https://www.misp-project.org/taxonomies.html#_estimative_language.
[22] MISP Galaxies and Clusters https://github.com/MISP/misp-galaxy.

2. THREAT ACTOR TRENDS

Cyber threat actors are an integral component of the threat landscape. These are entities that aim to conduct malicious acts by taking advantage of existing vulnerabilities with the intention of harming their victims. Understanding how threat actors think and act as well as their motivations and goals are essential for a more robust management of cyber threats and better responses to incidents. Monitoring the latest developments concerning the tactics and techniques used by threat actors to achieve their objectives and staying up-to-date with the long-term trends in motivations and targets is crucial for an efficient defence in today's cybersecurity ecosystem.

Moreover, understanding the trends related to threat actors, their motivations and their targets assists greatly in planning cybersecurity defences and mitigation strategies. It is an integral part of the overall assessment of threats since it allows security controls to be prioritised and a dedicated strategy based on potential impact and the likelihood that threats will materialise to be developed. Not understanding threat actors and how they operate creates a significant knowledge gap in cybersecurity because analysing threats without considering the motivations and goals may lead to inefficient defences or, in some cases, not being able to protect at all.

Cyber threat actors and their modus operandi are inevitably influenced by geopolitical events. A sizeable number of operations have been monitored, during the reporting period, where the actions of some cybercriminals, state-nexus threat groups and hacktivists have their roots in geopolitical developments. In general, at least state-nexus groups and hacktivists, regardless of motivation or agenda, can be triggered into action by these events.

In this section, we explore the trends related to threat actors. This assessment does not provide an exhaustive list of all trends during the reporting period but rather a high-level view of the significant trends observed at a strategic level. We focus on the motives of threat actors, their impact, and targeting. Their evolution is also assessed.

For the ETL 2023 report, we consider once more the following four categories of cybersecurity threat actors:

- **State-nexus threat groups**,
- **Cybercriminals**,
- **Hackers-for-hire**,
- **Hacktivists**.

State-nexus threat groups, often referred to as Advanced Persistent Threats or APTs, are in general well-funded, resourced and display advanced capabilities. Their objective is primarily espionage and revenue generation, sometimes directed by the military, intelligence or state control apparatus of their country. And although the techniques they employ might not always be that novel, their motivation and planning allow them to execute large-scale, advanced, targeted and long-term operations. State-nexus groups often spend considerable time investigating their targets to identify weaknesses and entry points, and they focus on stealth and avoiding operational mistakes. State-nexus groups do not only target other states. They can also target other organisations for sensitive data or conduct operations to obtain funding for their country.

The objective of **cybercriminals** is financial gain or profits in general. Their attacks are opportunistic and indiscriminate and they target the data or infrastructure that has the highest impact on the operations of victims. They can steal directly from victims, can extort the victim or can monetise the information stolen from victims. Cybercrime actors often use social engineering and employ multiple different methods for monetising their access to organisations. More recently, cybercrime actors have shown an increased level of collaboration and professionalisation, making them a force to be reckoned with.

Hackers-for-hire actors contribute to the professionalisation of the cybercrime market and they also provide services to state-nexus groups. The hacker-for-hire actors can lower the barrier to gain access to the criminal market such as, for example, with Ransomware-as-a-Service (RaaS). They also play a key role in the market that thrives on selling

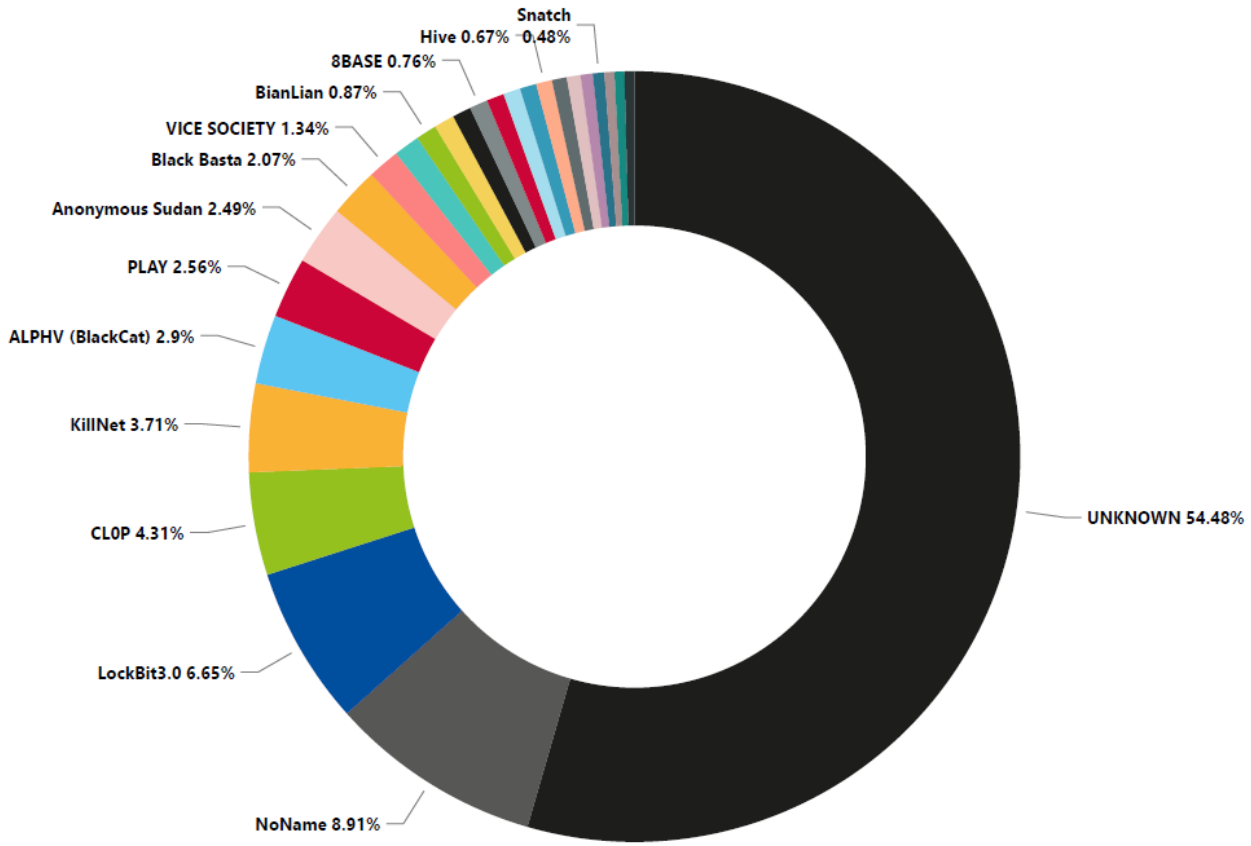
access to environments (so called Initial Access Brokers or IAB), either because the threat actor is tasked or because of opportunistic reasons.

Lastly, we cover the **hacktivists.** Hacktivists are not as well-resourced as the other threat actors but are often fuelled by strong motivations. Their objectives often involve disruption and they use hacking to affect some form of political or social change. Hacktivists groups are truly diverse and vary heavily in skillsets and capabilities. In addition, hacktivist threat actors are sometimes leveraged by state-nexus groups for information manipulation and interference operations or other forms of intrusion campaigns.

As an attentive reader you probably noticed we did not include the insider threat actor as one of the prime threat actors in this ETL. We excluded this threat actor because of the exceptionally small number of publicly reported incidents. Despite the fact that there are programmes that highlight the need to focus on the mitigation of insider threats[23], organisations remain reluctant to share details of these incidents. This does certainly not imply that the risk of a malicious insider is deemed of lesser significance. On the contrary, insiders remain the most efficient way to gain access to the internals of an organisation and, as such, they are sometimes used (knowingly or unknowingly) by state-sponsored or cybercrime actors for initial access to a victim's environment.

Over the course of the reporting period, we have pinpointed the 25 most active threat actors overall for our collected data. It is worth highlighting that a significant majority of the events we gathered have not been attributed to any specific threat actor, which underscores the challenges associated with accurate attribution.

Figure 11: 25 Most attributed Threat actors during the reporting period



[23] CISA Insider Threat Mitigation https://www.cisa.gov/topics/physical-security/insider-threat-mitigation.

2.1 STATE-NEXUS GROUP TRENDS

2.1.1 Misuse of Legitimate tools

It was observed that state-nexus groups have a continued interest in the misuse of these legitimate tools. This should not come as a surprise. Their objective is to **remain undetected** as long as possible and by using software commonly found on most systems they make it harder for defenders to spot their activities. Additionally, by leveraging these tools they have a better chance of **hiding their identities**. Where traditionally the use of specific tools was an element for attribution or the linking of related campaigns, this becomes much harder with dual-use tools.

According to multiple reports, the most common application is hijacking legitimate[24] [25] [26] tools (**Living Off the Land Binaries or LOLBins**) and using[27] [28] [29] [30] **freely available software**. A type of dual-use tools now seen more frequently than before are the **Command and Control (C2)** and **post exploitation frameworks**. These frameworks are commonly used by offensive security teams but also by actors with malicious intentions. This trend is not limited to state-nexus groups only; there is also an increase for cybercrime threat actors. Cobalt Strike remains[31] [32] amongst the most popular frameworks, but due to its widespread use in high-profile attacks there is an increased focus on detecting[33] its activity. This results in actors looking at alternatives[34] [35]. And although LOLBins, freely available software and post-exploitation frameworks, are not new, finding state-nexus groups relying on them is becoming more common. It is highly likely that this trend will continue, making detection and attribution harder.

2.1.2 Trojanising known software packages

. A trend, primarily exhibited by actors associated with North Korea and Russia[36], is to **trojanise**[37] [38] [39] **known software packages** and convince targets to use this software. These are not supply chain attacks as actors do not target software suppliers but rely on **social engineering** to convince victims to install software that has not been delivered through normal software delivery mechanisms. It is likely that trojanised software will remain part of state-nexus campaigns relying on social engineering.

2.1.3 Targeting edge devices for easy access

Misuse of legitimate tools and trojanised software have one aspect in common: in general, there is a form of **interaction with a victim** and consequently a higher chance of detection. To avoid this, actors show[40] [41] an increased interest in **edge devices**. This is also not limited to state-nexus groups; cybercrime actors have jumped on this bandwagon as well. The advantage is obvious. In most cases these devices lack in-depth detection and are not a prime subject for security monitoring. In addition, edge devices have a less frequent patch cycle and can suffer from misconfigurations, making them an easy target altogether. It is very unfortunate, though, that organisations get breached by devices they acquired for improving their protection. The primary type of targeted edge devices are **e-**

[24] People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection - https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF.
[25] EclecticIQ - Three Cases of Cyber Attacks on the Security Service of Ukraine and NATO Allies, Likely by Russian State-Sponsored Gamaredon - https://blog.eclecticiq.com/three-cases-of-cyber-attacks-on-the-security-service-of-ukraine-and-nato-allies-likely-by-russian-state-sponsored-gamaredon.
[26] Microsoft - Volt Typhoon targets US critical infrastructure with living-off-the-land techniques – https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.
[27] Meta - Meta's Adversarial Threat Report, Second Quarter 2022 - https://about.fb.com/news/2022/08/metas-adversarial-threat-report-q2-2022/.
[28] ESET - APT activity report T3 2022 - https://www.welivesecurity.com/wp-content/uploads/2023/01/eset_apt_activity_report_t32022.pdf.
[29] Microsoft - Nation-state threat actor Mint Sandstorm refines tradecraft to attack high-value targets - https://www.microsoft.com/en-us/security/blog/2023/04/18/nation-state-threat-actor-mint-sandstorm-refines-tradecraft-to-attack-high-value-targets/.
[30] People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices – https://media.defense.gov/2022/Jun/07/2003013376/-1/-1/0/CSA_PRC_SPONSORED_CYBER_ACTORS_EXPLOIT_NETWORK_PROVIDERS_DEVICES_TLPWHITE.PDF.
[31] Red Canary 2023 Threat Detection Report - https://redcanary.com/resources/guides/threat-detection-report/.
[32] Sophos - The Phantom Menace: Brute Ratel remains rare and targeted - https://news.sophos.com/en-us/2023/05/18/the-phantom-menace-brute-ratel-remains-rare-and-targeted/.
[33] NVISO - Cobalt Strike: Decrypting Traffic - https://blog.nviso.eu/series/cobalt-strike-decrypting-traffic/.
[34] Cybereason - Sliver C2 Leveraged by Many Threat Actors - https://www.cybereason.com/blog/sliver-c2-leveraged-by-many-threat-actors.
[35] Google - Threat Horizons April 2023 – https://services.google.com/fh/files/blogs/gcat_threathorizons_full_apr2023.pdf.
[36] Mandiant - Trojanised Windows 10 Operating System Installers Targeted Ukrainian Government - https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government.
[37] Microsoft - ZINC weaponising open-source software – https://www.microsoft.com/en-us/security/blog/2022/09/29/zinc-weaponizing-open-source-software/.
[38] ReversingLabs - ZetaNile: Open-source software trojans from North Korea - https://www.reversinglabs.com/blog/zetanile-open-source-software-trojans-from-north-korea.
[39] ESET - APT activity report T3 2022 – https://www.welivesecurity.com/wp-content/uploads/2023/01/eset_apt_activity_report_t32022.pdf.
[40] Recorded Future 2022 Annual Report - https://www.osintme.com/wp-content/uploads/2023/03/Recorded_Future_Annual_Report.pdf.
[41] Mandiant - Move, Patch, Get Out the Way: 2022 Zero-Day Exploitation Continues at an Elevated Pace - https://www.mandiant.com/resources/blog/zero-days-exploited-2022.

mail gateways, including Microsoft Exchange[42] [43] [44] [45], Zimbra[46] [47] and Barracuda[48]. Threat actors[49] [50] [51] [52] [53] also focus on **network equipment**, such as router firewalls and VPN hardware, to gain access to environments.

Given the wide range of edge devices, their crucial role in the infrastructure of organisations and sometimes their lack of protection and monitoring measures, it is highly likely that they will remain a prime target for exploitation and initial access. It is also likely that popular file transfer solutions will become interesting targets for state-nexus groups.

2.1.4 Use of known vulnerabilities or leveraging zero-days

The trend towards targeting vulnerabilities in edge devices shows that state-nexus groups have an appetite for using **old vulnerabilities** as well as relying **on zero-days**[54], often as a way to gain **initial access**. The focus on the next new threat, 'the unknown risk', should not make us forget[55] that there are still a lot of older vulnerabilities that can be exploited. Threat actors do not have to invest in zero-days as there are many known (and unpatched)[56] [57] [58] vulnerabilities available for abuse. And although Log4Shell has been declared[59] an endemic, it remains[60] [61] a significant threat for organisations. It is highly likely state-nexus groups will continue abusing new and older vulnerabilities and they will continue to drive the exploitation of vulnerabilities.

2.1.5 Targeting individuals

State-sponsored actors increasingly had, in their crosshairs, **employees** in key positions, **politicians**, government **officials**, **journalists, security researchers** or **activists**. They target these individuals not only via traditional spear phishing e-mails but also via social networks.

[42] Intrinsec - APT27 – One Year To Exfiltrate Them All: Intrusion In-Depth Analysis - https://www.intrinsec.com/apt27-analysis.
[43] XRATOR - BackdoorDiplomacy APT Group Targets Middle Eastern Telecoms in Espionage Campaign - https://www.conquer-your-risk.com/2023/03/01/backdoordiplomacy-apt-group-targets-middle-eastern-telecoms-in-espionage-campaign/.
[44] Microsoft - Analysing attacks using the Exchange vulnerabilities CVE-2022-41040 and CVE-2022-41082 - https://www.microsoft.com/en-us/security/blog/2022/09/30/analyzing-attacks-using-the-exchange-vulnerabilities-cve-2022-41040-and-cve-2022-41082/.
[45] CISA – Microsoft Releases Guidance on Zero-Day Vulnerabilities in Microsoft Exchange Server – https://www.cisa.gov/news-events/alerts/2022/09/30/microsoft-releases-guidance-zero-day-vulnerabilities-microsoft.
[46] WithSecure - No Pineapple! –DPRK Targeting of Medical Research and Technology Sector - https://labs.withsecure.com/publications/no-pineapple-dprk-targeting-of-medical-research-and-technology-sector.
[47] Proofpoint - Exploitation is a Dish Best Served Cold: Winter Vivern Uses Known Zimbra Vulnerability to Target Webmail Portals of NATO-Aligned Governments in Europe - https://www.proofpoint.com/us/blog/threat-insight/exploitation-dish-best-served-cold-winter-vivern-uses-known-zimbra-vulnerability.
[48] Mandiant - Barracuda ESG Zero-Day Vulnerability (CVE-2023-2868) Exploited Globally by Aggressive and Skilled Actor, Suspected Links to China - https://www.mandiant.com/resources/blog/barracuda-esg-exploited-globally.
[49] CISA – APT28 exploits known vulnerability to carry out reconnaissance and deploy malware on Cisco routers – https://www.cisa.gov/sites/default/files/2023-04/apt28-exploits-known-vulnerability-to-carry-out-reconnaissance-and-deploy-malware-on-cisco-routers-uk.pdf.
[50] Censys - CVE-2017-6742 Actively Exploited SNMP Vulnerability on Cisco Routers - https://censys.io/cve-2017-6742-actively-exploited-snmp-vulnerability-on-cisco-routers/.
[51] Checkpoint – The Dragon Who Sold His Camaro: Analysing Custom Router Implant – https://research.checkpoint.com/2023/the-dragon-who-sold-his-camaro-analyzing-custom-router-implant/.
[52] Microsoft – Volt Typhoon targets US critical infrastructure with living-off-the-land techniques – https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.
[53] Mandiant - Suspected Chinese Threat Actors Exploiting FortiOS Vulnerability (CVE-2022-42475) - https://www.mandiant.com/resources/blog/chinese-actors-exploit-fortios-flaw
[54] Mandiant - Move, Patch, Get Out the Way: 2022 Zero-Day Exploitation Continues at an Elevated Pace - https://www.mandiant.com/resources/blog/zero-days-exploited-2022.
[55] Darkreading – The Problem of Old Vulnerabilities – and What to Do About It – https://www.darkreading.com/vulnerabilities-threats/the-problem-of-old-vulnerabilities-and-what-to-do-about-it.
[56] CISA - Top CVEs Actively Exploited By People's Republic of China State-Sponsored Cyber Actors - https://media.defense.gov/2022/Oct/06/2003092365/-1/-1/0/Joint_CSA_Top_CVEs_Exploited_by_PRC_cyber_actors_.PDF.
[57] Google TAG – Continued cyber activity in Eastern Europe observed by TAG – https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/.
[58] Microsoft Threat Intelligence - https://twitter.com/MsftSecIntel/status/1654610012457648129.
[59] CSRB - Review of the December 2021 Log4j Event - https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf.
[60] Cisco Talos - Lazarus and the tale of three RATs - https://blog.talosintelligence.com/lazarus-three-rats/.
[61] CISA - Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester - https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-320a.

A long running pretext[62] [63] [64] [65] is impersonating recruiters[66] [67] or journalists[68] [69] and using LinkedIn to setup initial communications. Some actors even used phone calls or video chats to persuade[70] victims into participating in propaganda. It is very likely we will continue to see state-nexus groups targeting individuals. Either because this provides an easier way to bypass corporate defences, because individuals might be more off-guard when engaged outside their professional context or because it is used in relation to campaigns of information manipulation.

2.1.6 Information manipulation and interference operations

Targeting individuals is only the start of an approach that was refined further during information manipulation and interference operations. Often, these operations are **complementary**[71] **to traditional kinetic attacks** and are executed via different internet services at once. There is no single playbook[72] which complicates the possibilities for discovery and their application is wide-spread[73] [74] [75]. One problem[76] in addressing these threats is '**linkage blindness'**, where different governments and organisations look at different facets, no institution is positioned to take responsibility for adopting a comprehensive approach.

Although campaigns associated with the Russia-Ukraine war are **high**[77] **in volume**, they are of **low quality**[78]**.** Their goal[79] [80], often, is to undermine the Ukrainian government, fracture international support for Ukraine and maintain domestic support for the war. Some campaigns are amplified[81] [82] by overt state-backed media or Russian embassies while others are linked to private actors. A common theme[83] [84] [85] [86] is to **launder messages** via local media brands, Non-Governmental Organisations (NGOs) and shell companies and using an extensive range of intermediaries[87]. The operations associated with China[88] [89] are resembling[90] [91] [92] more and more those employed by Moscow. In some

[62] Sekoia - Peeking at Reaper's surveillance operations - https://blog.sekoia.io/peeking-at-reaper-surveillance-operations-against-north-korea-defectors/.
[63] ESET – Who's swimming in South Korean waters? Meet ScarCruft's Dolphin – https://www.welivesecurity.com/2022/11/30/whos-swimming-south-korean-waters-meet-scarcrufts-dolphin/.
[64] HRW - Iran: State-Backed Hacking of Activists, Journalists, Politicians - https://www.hrw.org/news/2022/12/05/iran-state-backed-hacking-activists-journalists-politicians.
[65] Microsoft - Disrupting SEABORGIUM's ongoing phishing operations - https://www.microsoft.com/en-us/security/blog/2022/08/15/disrupting-seaborgiums-ongoing-phishing-operations/.
[66] Microsoft - ZINC weaponising open-source software - https://www.microsoft.com/en-us/security/blog/2022/09/29/zinc-weaponizing-open-source-software/.
[67] ReversingLabs – ZetaNile: Open-source software trojans from North Korea – https://www.reversinglabs.com/blog/zetanile-open-source-software-trojans-from-north-korea.
[68] Mandiant - APT42: Crooked Charms, Cons and Compromises - https://www.mandiant.com/media/17826.
[69] Proofpoint – Above the Fold and in Your Inbox: Tracing State-Aligned Activity Targeting Journalists, Media – https://www.proofpoint.com/us/blog/threat-insight/above-fold-and-your-inbox-tracing-state-aligned-activity-targeting-journalists.
[70] Proofpoint - Do not Answer That! Russia-Aligned TA499 Beleaguers Targets with Video Call Requests - https://www.proofpoint.com/us/blog/threat-insight/dont-answer-russia-aligned-ta499-beleaguers-targets-video-call-requests.
[71] Mandiant - M-Trends 2023: Cybersecurity Insights From the Frontlines - https://www.mandiant.com/resources/blog/m-trends-2023.
[72] Meta – Recapping Our 2022 Coordinated Inauthentic Behaviour Enforcements – https://about.fb.com/news/2022/12/metas-2022-coordinated-inauthentic-behavior-enforcements/.
[73] Meta - Quarterly Adversarial Threat Report - https://about.fb.com/wp-content/uploads/2023/02/Meta-Quarterly-Adversarial-Threat-Report-Q4-2022.pdf.
[74] Euronews - Turkey's disinformation election: Fake videos and wildly misleading claims - https://www.euronews.com/2023/05/16/turkeys-disinformation-election-fake-videos-and-wildly-misleading-claims.
[75] EU DisinfoLab - Landscape publications - https://www.disinfo.eu/publications/.
[76] Cardiff University – The Ghostwriter Campaign – https://www.cardiff.ac.uk/__data/assets/pdf_file/0005/2699483/Ghostwriter-Report-Final.pdf.
[77] Meta - Removing Coordinated Inauthentic Behaviour from China and Russia - https://about.fb.com/news/2022/09/removing-coordinated-inauthentic-behavior-from-china-and-russia/.
[78] Meta – Meta's Adversarial Threat Report, Fourth Quarter 2022 – https://about.fb.com/news/2023/02/metas-adversarial-threat-report-q4-2022/.
[79] How the Russian Influence Operation on Twitter Weaponized Military Narratives - https://papers.academic-conferences.org/index.php/iccws/article/view/985/982.
[80] Google TAG - Fog of war: how the Ukraine conflict transformed the cyber threat landscape - https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/.
[81] Meta - Quarterly Adversarial Threat Report - https://about.fb.com/wp-content/uploads/2022/11/Quarterly-Adversarial-Threat-Report-Q2-2022-1.pdf.
[82] Google TAG - Ukraine remains Russia's biggest cyber focus in 2023 - https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/.
[83] Google TAG - Prigozhin interests and Russian information operations - https://blog.google/threat-analysis-group/prigozhin-interests-and-russian-information-operations/.
[84] Qurium - Under the hood of a Doppelgänger - https://www.qurium.org/alerts/under-the-hood-of-a-doppelganger/.
[85] EC - 26-04-2023 09:00 ING2 votes and exchange of views - https://www.europarl.europa.eu/committees/en/ing2-votes-and-exchange-of-views/product-details/20230421CHE11608.
[86] EU DisinfoLab - Doppelganger – Media clones serving Russian propaganda - https://www.disinfo.eu/doppelganger/.
[87] Olga Lautman - Dossier Center Investigation: Prigozhin's Cyber Troops - https://olgalautman.substack.com/p/dossier-center-investigation-prigozhins.
[88] IRSEM - Chinese influence operations - https://www.irsem.fr/report.html.
[89] Recorded Future - 2022 Annual Report - https://www.osintme.com/wp-content/uploads/2023/03/Recorded_Future_Annual_Report.pdf.
[90] The Record - Meta: Chinese disinformation network was behind London front company recruiting content creators - https://therecord.media/china-disinformation-meta-london-new-media-europe.
[91] Mandiant - Pro-PRC 'HaiEnergy' Information Operations Campaign Leverages Infrastructure from Public Relations Firm to Disseminate Content on Inauthentic News Sites - https://www.mandiant.com/resources/blog/pro-prc-information-operations-campaign-haienergy.
[92] CFR - China's Growing Attempts to Influence U.S. Politics - https://www.cfr.org/article/chinas-growing-attempts-influence-us-politics.

cases,[93] this **Russification**[94] even amplified the Russian narratives, directly or indirectly. Iran[95] [96] [97] has well established its efforts in using influence operations complementarity with traditional cyber operations, possibly to **compensate for its shortcomings** in cyberattack capabilities.

We expect that state-nexus campaigns of information manipulation, sometimes side-by-side with traditional cyber and kinetic attacks will further increase in volume. It is likely that state-nexus groups will continue setting up fake news outlets or similar things to distribute their narratives, and it is highly likely they will continue the use of social media to amplify their messages. Considering geopolitical tensions, we can already observe that campaigns associated with China will have an impact in the sphere of European media[98].

2.1.7 Activities fuelled by geopolitical events

A shortcoming raised by influence campaigns is 'linkage blindness' as stated earlier. Related to this problem is that defenders can sometimes be anchored in their 'cyber' world, without considering how geopolitical changes influence cyber-activities.

Obviously, the Russian war against Ukraine is a key topic for state-nexus groups, more specifically those that are associated with Russia. Between each phase[99] of Russian cyber offensive events, the attacks decreased in coordination and technical sophistication, but increased in number of attackers and targets. With this emphasis on **speed** the **risk for errors** increases tremendously, introducing **spill-over risk**[100] and unintentional spread beyond the original target. **Intelligence collection** remains[101] a prime source for anticipating geopolitical events, especially by targeting[102] [103] [104] [105] [106] [107] [108] [109] [110] diplomatic services, private and public military organisations, think-tanks, humanitarian organisations, IT companies and critical infrastructure. What is remarkable is that more mundane lures, such as fake Windows update mails, remained[111] effective as well. The disruption[112] [113] of the Snake malware network gave a substantial blow to the espionage capabilities of actors associated with Russia. Although the malware itself is relatively old (first appearance early 2004[114]), the dismantling of its operations certainly had negative strategical and operational effects. Groups associated with North Korea and Iran used the war between Russia and

[93] Recorded Future - 2022 Annual Report - https://www.osintme.com/wp-content/uploads/2023/03/Recorded_Future_Annual_Report.pdf.
[94] Per Concordiam – War by Narrative? – https://perconcordiam.com/war-by-narrative/.
[95] Microsoft – Rinse and repeat: Iran accelerates its cyber influence operations worldwide – https://blogs.microsoft.com/on-the-issues/2023/05/02/dtac-iran-cyber-influence-operations-digital-threat/.
[96] Microsoft - Iran turning to cyber-enabled influence operations for greater effect - https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/05/Iran-turning-to-cyber-enabled-influence-operations-for-greater-effect-05022023.pdf.
[97] Foreignpolicy - How Albania Became a Target for Cyberattacks - https://foreignpolicy.com/2023/03/25/albania-target-cyberattacks-russia-iran/.
[98] My Tea's not cold - An overview of China's cyber threat - Sekoia.io Blog
[99] Recorded Future - 2022 Annual Report - https://www.osintme.com/wp-content/uploads/2023/03/Recorded_Future_Annual_Report.pdf.
[100] Council - Declaration by the High Representative on behalf of the EU on malicious cyber activities conducted by hackers and hacker groups in the context of Russia's aggression against Ukraine - https://www.consilium.europa.eu/en/press/press-releases/2022/07/19/declaration-by-the-high-representative-on-behalf-of-the-european-union-on-malicious-cyber-activities-conducted-by-hackers-and-hacker-groups-in-the-context-of-russia-s-aggression-against-ukraine/.
[101] Crowdstrike - CrowdStrike 2023 Global Threat Report - https://www.crowdstrike.com/global-threat-report/.
[102] CERT-EU – Russia's war on Ukraine – One year of cyber operations – https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CERT-EU-1YUA-CyberOps.pdf.
[103] TheRecord - Russia-backed hacker group Gamaredon attacking Ukraine with info-stealing malware - https://therecord.media/russia-backed-hacker-group-gamaredon-attacking-ukraine-with-info-stealing-malware.
[104] BlackBerry – Gamaredon Leverages Microsoft Office Docs to Target Ukraine Government and Military – https://blogs.blackberry.com/en/2022/11/gamaredon-leverages-microsoft-office-docs-to-target-ukraine-government.
[105] Cisco - Gamaredon APT targets Ukrainian government agencies in new campaign - https://blog.talosintelligence.com/gamaredon-apt-targets-ukrainian-agencies/.
[106] BlackBerry - Gamaredon (Ab)uses Telegram to Target Ukrainian Organisations - https://blogs.blackberry.com/en/2023/01/gamaredon-abuses-telegram-to-target-ukrainian-organizations.
[107] Gov.pl – Espionage campaign linked to Russian intelligence services – https://www.gov.pl/web/baza-wiedzy/espionage-campaign-linked-to-russian-intelligence-services.
[108] Mandiant - You Can't Audit Me: APT29 Continues Targeting Microsoft 365 - https://www.mandiant.com/resources/blog/apt29-continues-targeting-microsoft.
[109] Palo Alto – Unit42 – Russian APT29 Hackers Use Online Storage Services, DropBox and Google Drive – https://unit42.paloaltonetworks.com/cloaked-ursa-online-storage-services-campaigns/.
[110] Blackberry - NOBELIUM Uses Poland's Ambassador's Visit to the US to Target EU Governments Assisting Ukraine - https://blogs.blackberry.com/en/2023/03/nobelium-targets-eu-governments-assisting-ukraine.
[111] RedPacket Security - APT28 Targets Ukrainian Government Entities with Fake 'Windows Update' Emails - https://www.redpacketsecurity.com/apt-targets-ukrainian-government-entities-with-fake-windows-update-emails/.
[112] DOJ - Justice Department Announces Court-Authorised Disruption of the Snake Malware Network Controlled by Russia's Federal Security Service - https://www.justice.gov/usao-edny/pr/justice-department-announces-court-authorized-disruption-snake-malware-network.
[113] CISA - Hunting Russian Intelligence 'Snake' Malware - https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a.
[114] https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-129a

Ukraine as a theme for intelligence seeking campaigns[115] [116] and groups associated with China used[117] the EU sanctions against Russia as a lure in their campaigns.

It is very likely that campaigns of espionage by actors associated with Russia will persist[118], possibly pivoting to **support domestic production capabilities** or increasing **retaliation** against those that express solidarity with Ukraine. It is likely that other state-sponsored groups will leverage the same theme.

Apart from espionage, Russia associated actors continued using **destructive wipers** for sabotage, with some campaigns[119] [120] aligning with kinetic military actions. State-nexus groups also deployed[121] ransomware, traditionally associated with cybercrime.

2.1.8 Sustained activity by threat actors associated with China

Chinese state-sponsored groups have traditionally been active[122] in targeting China's rival territorial claimants, but after the war on Ukraine started there is an increased targeting and Russian[123] entities. The objective and motivation of these campaigns[124] [125] [126] [127] [128] is mostly **espionage** and **information theft** from a diverse range of sectors, including financial bodies, telecommunications[129], government agencies, critical infrastructure[130] and military organisations. An important change is the **outspoken statements** from official organisations[131] [132] [133] [134] [135] [136] to consider China as an immense threat.

Given the elevation[137] [138] of key security officials into top leadership bodies (Politburo) in China, it is very likely that the volume of espionage campaigns run by groups associated with China is only going to increase in the near future. It is also highly likely that the information gained during these campaigns will be used for economic benefit, pre-positioning for future attacks and to fine-tune **campaigns of information manipulation** to steer their narrative.

2.1.9 Financial gain interwoven with state-nexus activities

[115] Sentinel One - Kimsuky Evolves Reconnaissance Capabilities in New Global Campaign - https://www.sentinelone.com/labs/kimsuky-evolves-reconnaissance-capabilities-in-new-global-campaign/.
[116] Microsoft - Iran turning to cyber-enabled influence operations for greater effect - https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/05/Iran-turning-to-cyber-enabled-influence-operations-for-greater-effect-05022023.pdf.
[117] BlackBerry - Mustang Panda Uses the Russian-Ukrainian War to Attack Europe and Asia Pacific Targets - https://blogs.blackberry.com/en/2022/12/mustang-panda-uses-the-russian-ukrainian-war-to-attack-europe-and-asia-pacific-targets.
[118] Recorded Future – 2022 Annual Report – https://www.osintme.com/wp-content/uploads/2023/03/Recorded_Future_Annual_Report.pdf.
[119] https://www.eset.com/int/business/resource-center/reports/eset-apt-activity-report-t2-2022/.
[120] ESET – ESET Research: Russian APT groups, including Sandworm, continue their attacks against Ukraine with wipers and ransomware – https://www.eset.com/gr-en/about/newsroom/press-releases/eset-research-russian-apt-groups-including-sandworm-continue-their-attacks-against-ukraine-with-wipe-3/.
[121] Microsoft - New 'Prestige' ransomware impacts organisations in Ukraine and Poland - https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/.
[122] Recorded Future – 2022 Annual Report – https://www.osintme.com/wp-content/uploads/2023/03/Recorded_Future_Annual_Report.pdf.
[123] Sentinel One - Targets of Interest | Russian Organisations Increasingly Under Attack By Chinese APTs - https://www.sentinelone.com/labs/targets-of-interest-russian-organizations-increasingly-under-attack-by-chinese-apts/.
[124] AttackIQ - Emulating the Politically Motivated Chinese APT Mustang Panda - https://www.attackiq.com/2023/03/23/emulating-the-politically-motivated-chinese-apt-mustang-panda/.
[125] Trend Micro – Pack it Secretly: Earth Preta's Updated Stealthy Strategies – https://www.trendmicro.com/fr_fr/research/23/c/earth-preta-updated-stealthy-strategies.html.
[126] The Hacker News - Chinese Hackers Target Government Officials in Europe, South America, and Middle East - https://thehackernews.com/2022/09/chinese-hackers-target-government.html.
[127] ESET - MQsTTang: Mustang Panda's latest backdoor treads new ground with Qt and MQTT - https://www.welivesecurity.com/2023/03/02/mqsttang-mustang-panda-latest-backdoor-treads-new-ground-qt-mqtt/.
[128] Cisco Talos - Mustang Panda deploys a new wave of malware targeting Europe - https://blog.talosintelligence.com/mustang-panda-targets-europe/.
[129] CERT-EU – Cyber Security Brief (March 2023) – https://cert.europa.eu/static/MEMO/2023/TLP-CLEAR-CB-23-04.pdf.
[130] Microsoft - Volt Typhoon targets US critical infrastructure with living-off-the-land techniques - https://www.microsoft.com/en-us/security/blog/2023/05/24/volt-typhoon-targets-us-critical-infrastructure-with-living-off-the-land-techniques/.
[131] BBC - China: MI5 and FBI heads warn of 'immense' threat - https://www.bbc.com/news/world-asia-china-62064506.
[132] ITPro – MI5 to establish new security agency to counter Chinese hacking, espionage – https://www.itpro.com/business/policy-legislation/370238/mi5-establish-security-agency-counter-chinese-hacking-espionage.
[133] People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection - https://media.defense.gov/2023/May/24/2003229517/-1/-1/0/CSA_Living_off_the_Land.PDF.
[134] CISA - People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection - https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a.
[135] BUZA - China: Declaration by the Minister for Foreign Affairs on behalf of the Belgian Government urging Chinese authorities to take action against malicious cyber activities undertaken by Chinese actors - https://diplomatie.belgium.be/en/news/declaration-minister-foreign-affairs-malicious-cyber-activities.
[136] ENISA - Sustained Activity by Threat Actors-Joint Publication - https://www.enisa.europa.eu/publications/sustained-activity-by-specific-threat-actors-joint-publication.
[137] Axios - Xi's new inner circle emphasizes security and loyalty - https://www.axios.com/2022/10/25/xi-inner-circle-security-loyalty-china.
[138] SCMP - Politburo member Chen Wenqing to step up to China's top security job - https://www.scmp.com/news/china/politics/article/3197708/politburo-member-chen-wenqing-step-chinas-top-security-job.

Traditionally, campaigns associated with North Korea have had since 2014 a dual motivation, espionage and financial gain, often via cryptocurrency. It is highly likely[139] [140], given the explosive growth of cryptocurrency and the economic impact of sanctions, that they will continue to undertake **financial theft** on behalf of the government, sometimes including laundering[141] crypto through legitimate services. Groups associated with North Korea[142] [143] [144] [145] [146] have also shifted to the **collection of intelligence**, mostly via **tailored social engineering campaigns**. And where historically their targeting was regionally focused, they are including targets **outside**[147] [148] [149] **their region**. It is expected that groups associated with North Korea will continue to focus on cryptocurrency but will also include the collection of intelligence, as a means of bypassing the effects of the international sanctions imposed on the regime.

2.1.10 Disruption of public services and critical infrastructure

Attacks causing disruption are not only started because of geopolitical events, they can also be due to retaliation. This was painfully demonstrated[150] [151] when groups associated with Iran started a disruptive attack against the Albanian government, most likely in retaliation because Iran suffered of an earlier attack[152] by an Iranian dissident group headquartered in Albania. The 'hack, lock and leak' approach was applied[153] [154] on multiple occasions by actors associated with Iran. A common method is the **exploitation** of vulnerabilities for initial access and **hiding** in the environment for a prolonged period of time; then the tasking of the final objectives is **shared** between different (Iranian) groups.

We expect that actors associated with Iran will continue to undertake disruptive campaigns, most often via the exploitation of vulnerabilities.

2.1.11 Novel techniques

During the reporting period there were reports of novel attack techniques that require resources typically associated with state-nexus groups. These techniques [155] targeted the Unified Extensible Firmware Interface (UEFI firmware), which, if successful, would allow an actor to have full control over the operating system (OS) boot process and thus capable of disabling OS security mechanisms. Although the discovery indicates that malware targeting UEFI firmware is not a myth, practical implementation remains difficult. It is unlikely we will see this being used by state-nexus groups in the very near future.

2.2 CYBERCRIME ACTOR TRENDS

2.2.1 Using valid accounts for initial access

Although not a novel technique, abusing valid accounts for initial access remained[156] successful for cybercrime actors during the reporting period. Especially notable were **misconfigured** accounts or those with **weak passwords**. And

[139] PWC - 2022 Year in retrospect - https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/pdf/2022-year-in-retrospect-report.pdf.
[140] Mandiant - M-Trends 2023 - https://www.mandiant.com/resources/blog/m-trends-2023.
[141] Wired - North Korea Is Now Mining Crypto to Launder Its Stolen Loot - https://www.wired.com/story/north-korea-apt43-crypto-mining-laundering/.
[142] Mandiant - APT43: North Korean Group Uses Cybercrime to Fund Espionage Operations - https://mandiant.widen.net/s/zvmfw5fnjs/apt43-report.
[143] Packt – Kimsuky – the notorious North Korean APT – https://security.packt.com/kimsuky-notorious-north-korean/.
[144] Sentinel One - Kimsuky | Ongoing Campaign Using Tailored Reconnaissance Toolkit - https://www.sentinelone.com/labs/kimsuky-ongoing-campaign-using-tailored-reconnaissance-toolkit/.
[145] Ahnlab - Kimsuky Group's Phishing Attacks Targeting North Korea-Related Personnel - https://asec.ahnlab.com/en/52970/.
[146] Sentinel One - Kimsuky Strikes Again | New Social Engineering Campaign Aims to Steal Credentials and Gather Strategic Intelligence - https://www.sentinelone.com/labs/kimsuky-new-social-engineering-campaign-aims-to-steal-credentials-and-gather-strategic-intelligence/.
[147] BfV - Joint Cyber Security Advisory (Deutsch) - https://www.verfassungsschutz.de/SharedDocs/publikationen/DE/wirtschafts-wissenschaftsschutz/2023-03-20-sicherheitshinweis-cyberaktivitaeten.html.
[148] The Record - North Korean APT group 'Kimsuky' targeting experts with new spearphishing campaign - https://therecord.media/north-korea-apt-kimsuky-attacks.
[149] North Korea Using Social Engineering to Enable Hacking of Think Tanks, Academia, and Media - https://media.defense.gov/2023/Jun/01/2003234055/-1/-1/0/JOINT_CSA_DPRK_SOCIAL_ENGINEERING.PDF.
[150] Microsoft - Microsoft investigates Iranian attacks against the Albanian government - https://www.microsoft.com/en-us/security/blog/2022/09/08/microsoft-investigates-iranian-attacks-against-the-albanian-government/.
[151] Group IB – Hi-Tech Crime Trends 2022/2023 https://go.group-ib.com/hubfs/report/protected/group-ib-hi-tech-crime-trends-2022-2023-en.pdf.
[152] Jerusalem Post - Mossad blamed for cyberattack on Tehran municipality - https://www.jpost.com/middle-east/article-708830.
[153] Microsoft - Profiling DEV-0270: PHOSPHORUS' ransomware operations - https://www.microsoft.com/en-us/security/blog/2022/09/07/profiling-dev-0270-phosphorus-ransomware-operations/.
[154] Microsoft – MERCURY and DEV-1084: Destructive attack on hybrid environment – https://www.microsoft.com/en-us/security/blog/2023/04/07/mercury-and-dev-1084-destructive-attack-on-hybrid-environment/.
[155] ESET - BlackLotus UEFI bootkit: Myth confirmed - https://www.welivesecurity.com/2023/03/01/blacklotus-uefi-bootkit-myth-confirmed/.
[156] Cisco - Quarterly Report: Incident Response Trends in Q3 2022 - https://blog.talosintelligence.com/quarterly-report-incident-response-trends-in-q3-2022/.

although multi-factor authentication (MFA) stops a lot of these attacks, it is not bulletproof. This was demonstrated[157] by actors **intercepting MFA** codes, harassing users with an overload of push notifications, abusing accounts waiting to be enrolled for MFA or by device code[158] phishing or session cookie theft[159]. We expect that credentials remain a focal point for cybercrime actors. Despite technical protective measures, cybercrime actors have found ways around them.

2.2.2 Misuse of Legitimate tools

The abundance of **Remote Monitoring and Management (RMM)** software has also gained[160] the attention of cybercrime actors. An advisory[161] from CISA highlights how this software allows attackers to blend in with normal operations and the risks this entails. It is highly likely we will continue to see cybercrime (and state-nexus groups) make use of RMM software. This stresses the need for organisations to review their lists of running software and identify unauthorised RMM software, as well as monitor the access logs of their authorised software.

Cybercrime actors keep relying on **Living Off the Land Binaries (LOLBins)**, some even[162] using BitLocker to do the encryption. These actors increasingly have an interest in tools commonly used by offensive security teams, such as **Command and Control (C2) frameworks**. But whereas state-nexus groups are more reluctant to use a new framework, cybercrime actors will **adapt much faster**. They observe which techniques are successful and then include them in their arsenal. Once one group starts using a tool, it is quickly taken up by other groups. Threat actors used pirated copies[163] of commercial C2 frameworks, frameworks[164] written in GoLang or relied on open-source post-exploitation frameworks. Cobalt Strike was[165] still the preferred framework. We expect that LOLBins and offensive security tools will remain part of the cybercrime actor's toolset. They have proven to be highly successful, both in achieving their goals and for blending in with normal activities, and there are no signs this is going to change soon.

Another trend was '**bring your own vulnerable driver**' to disable **security products**. The vulnerable driver does not need to be present on the system; it is put there by the threat actor. Since these signed and trusted drivers run with kernel-level privileges, even behaviour-based detections can be bypassed. And although vendors tried to address the problem, it remains a successful[166] [167] [168] [169] [170] [171] technique to evade detection. Actors can also **directly target**[172] [173] security products for gaining access to victims. It is highly likely that threat actors will further analyse security products and look for ways on how to reconfigure or disable them or use these tools in unexpected ways to their advantage.

2.2.3 Use of non-traditional programming languages

[157] Microsoft – DEV-1101 enables high-volume AiTM campaigns with open-source phishing kit – https://www.microsoft.com/en-us/security/blog/2023/03/13/dev-1101-enables-high-volume-aitm-campaigns-with-open-source-phishing-kit/.
[158] Red Canary - 2023 Threat Detection Report - https://redcanary.com/resources/guides/threat-detection-report/.
[159] mrd0x.com - Attacking With WebView2 Applications - https://mrd0x.com/attacking-with-webview2-applications/.
[160] DFIR Report - 2022 Year in Review - https://thedfirreport.com/2023/03/06/2022-year-in-review/.
[161] CISA - Protecting Against Malicious Use of Remote Monitoring and Management Software - https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-025a.
[162] Arctic Wolf - Chiseling In: Lorenz Ransomware Group Cracks MiVoice And Calls Back For Free - https://arcticwolf.com/resources/blog/lorenz-ransomware-chiseling-in/.
[163] Sophos - BlackCat ransomware attacks not merely a byproduct of bad luck - https://news.sophos.com/en-us/2022/07/14/blackcat-ransomware-attacks-not-merely-a-byproduct-of-bad-luck.
[164] Cisco Talos - Talos Takes 126: Year in Review – Threat Landscape Edition – https://blog.talosintelligence.com/talos-takes-126-year-in-review-threat-landscape-edition/.
[165] DFIR Report - 2022 year in review - https://thedfirreport.com/2023/03/06/2022-year-in-review/.
[166] Trend Micro - Ransomware Actor Abuses Genshin Impact Anti-Cheat Driver to Kill Antivirus - https://www.trendmicro.com/en_us/research/22/h/ransomware-actor-abuses-genshin-impact-anti-cheat-driver-to-kill-antivirus.html.
[167] Cybernews - Bringing your own vulnerable driver attack technique is becoming popular among threat actors - https://cybernews.com/security/bring-your-own-vulnerable-driver-attack/.
[168] FourCore - Exploit Party: Bring Your Own Vulnerable Driver Attacks - https://fourcore.io/blogs/bring-your-own-vulnerable-driver-attack.
[169] TrendMicro - BlackCat Ransomware Deploys New Signed Kernel Driver – https://www.trendmicro.com/en_us/research/23/e/blackcat-ransomware-deploys-new-signed-kernel-driver.html.
[170] VMware - Bring Your Own Backdoor: How Vulnerable Drivers Let Hackers In - https://blogs.vmware.com/security/2023/04/bring-your-own-backdoor-how-vulnerable-drivers-let-hackers-in.html.
[171] Crowdstrike - SCATTERED SPIDER Exploits Windows Security Deficiencies with Bring-Your-Own-Vulnerable-Driver Tactic in Attempt to Bypass Endpoint Security – https://www.crowdstrike.com/blog/scattered-spider-attempts-to-avoid-detection-with-bring-your-own-vulnerable-driver-tactic/.
[172] Checkpoint Rorschach – A New Sophisticated and Fast Ransomware - https://research.checkpoint.com/2023/rorschach-a-new-sophisticated-and-fast-ransomware/.
[173] Google TAG – Magniber ransomware actors used a variant of Microsoft SmartScreen bypass – https://blog.google/threat-analysis-group/magniber-ransomware-actors-used-a-variant-of-microsoft-smartscreen-bypass/.

Cybercrime actors increasingly use[174] non-traditional languages. This is partially done to make their malware **cross-platform**, with a higher return on investment. Another advantage is that it can make the **analysis** much **harder**. Not necessarily from a technical point of view but from a lack of hands-on expertise with languages such as Rust[175] or Go[176]. Non-traditional programming languages sometimes bring **better performance** and memory management also. For cybercrime actors, this means their malware will be more reliable and faster. In addition, Go libraries are statically linked, which means all necessary libraries are included in the compiled binary. This makes files larger, which might be beneficial, given that some malware scanners are optimised for speed and could ignore larger files. The use of non-traditional programming languages will further find its way into the toolset of cybercrime actors and also, it is likely, into the toolset of state-nexus groups.

2.2.4 Role of cloud infrastructure

It will come as no surprise that cybercrime actors continue to use cloud infrastructure. In most cases cloud infrastructure is part of **social engineering** campaigns[177] [178] [179] to distribute spear phishing mails with links to file-sharing services in the cloud. Apart from the availability and low cost there is an additional advantage: it enables **blending in** with what is 'normal' within organisations. Also, they do not have to worry about their domains being blocklisted, as cloud services are often already allowlisted. This is not only advantageous for delivering malware but they can also use them for Command and Control (C2) communications.

Cybercrime actors turn to the cloud infrastructure of potential victims to cause harm, primarily by abusing cloud **misconfigurations**[180] [181]. Due to the complexity of securing a cloud tenant, it is not surprising that miscreants often 'discover' features neglected[182] by organisations. We expect that cybercrime actors will continue to use cloud infrastructure to support their campaigns, as well as targeting the cloud infrastructure of organisations. This will not only include the organisations' systems, storage and networks running in the cloud, but also the management consoles of these cloud infrastructures.

2.2.5 Old tricks remain a guarantee for success

Whereas non-traditional programming languages are a rather novel technique, there are still old techniques that remain successful as well. Search engine optimisation (SEO) poisoning and **malvertising** dates back many years and has sparked a new interest[183] [184] amongst cybercrime actors. The FBI issued a warning[185] that criminals[186] [187] [188] are using search engine advertisement services to impersonate brands and direct users to sites that host ransomware and steal login credentials and other financial information. Criminal gangs leverage the advantages of **advertisement platforms**, such as traffic distribution and traffic filtering, to **tune their campaigns**. It is likely that cybercrime actors will continue to use advertisement platforms to target specific sets of users.

[174] Cisco Talos - Talos Takes 126: Year in Review - Threat Landscape Edition - https://blog.talosintelligence.com/talos-takes-126-year-in-review-threat-landscape-edition/.
[175] BlackBerry – Global Intelligence Report – https://www.blackberry.com/content/dam/bbcomv4/global/pdf/0408-Threat-ReportV17.pdf.
[176] BlackBerry - BianLian Ransomware Encrypts Files in the Blink of an Eye - https://blogs.blackberry.com/en/2022/10/bianlian-ransomware-encrypts-files-in-the-blink-of-an-eye.
[177] Trend Micro - Earth Preta Spear-Phishing Governments Worldwide – https://www.trendmicro.com/en_us/research/22/k/earth-preta-spear-phishing-governments-worldwide.html.
[178] Google TAG - Continued cyber activity in Eastern Europe observed by TAG - https://blog.google/threat-analysis-group/continued-cyber-activity-in-eastern-europe-observed-by-tag/.
[179] Sentinel One – WIP26 Espionage | Threat Actors Abuse Cloud Infrastructure in Targeted Telco Attacks – https://www.sentinelone.com/labs/wip26-espionage-threat-actors-abuse-cloud-infrastructure-in-targeted-telco-attacks/.
[180] Crowdstrike - CrowdStrike 2023 Global Threat Report - https://www.crowdstrike.com/global-threat-report/.
[181] Tenable – 2022 threat landscape report – https://www.tenable.com/cyber-exposure/tenable-2022-threat-landscape-report.
[182] Mandiant - SIM Swapping and Abuse of the Microsoft Azure Serial Console: Serial Is Part of a Well Balanced Attack - https://www.mandiant.com/resources/blog/sim-swapping-abuse-azure-serial.
[183] Red Canary - 2023 Threat Detection Report – https://redcanary.com/resources/guides/threat-detection-report/.
[184] Crowdstrike - https://www.crowdstrike.com/cybersecurity-101/attack-types/seo-poisoning/.
[185] FBI – Cyber Criminals Impersonating Brands Using Search Engine Advertisement Services to Defraud Users – https://www.ic3.gov/Media/Y2022/PSA221221.
[186] BlackBerry - Wave of Magniber Ransomware Attacks Hitting EU: What to Know - https://blogs.blackberry.com/en/2023/01/magniber-ransomware-hits-eu.
[187] Microsoft - DEV-0569 finds new ways to deliver Royal ransomware, various payloads - https://www.microsoft.com/en-us/security/blog/2022/11/17/dev-0569-finds-new-ways-to-deliver-royal-ransomware-various-payloads/.
[188] Bleeping Computer - SharkBot malware sneaks back on Google Play to steal your logins - https://www.bleepingcomputer.com/news/security/sharkbot-malware-sneaks-back-on-google-play-to-steal-your-logins/.

USBs also had[189] [190] a resurgence by groups that are **financially motived**. We expect attacks via USB to be used in targeted attacks, but they are unlikely to be used in widespread campaigns.

Another relatively old technique that remains[191] [192] lucrative is **cryptojacking**, demonstrated by the announcement[193] [194] from AstraLocker that it will **cease ransomware operations** and **switch to cryptojacking** operations. But this success comes at a price, at least from the cybercrime actor point of view. Law enforcement are increasingly[195] **treating virtual assets like any other asset** from a legal perspective, easing their seizure. Although not advanced in nature, criminals will continue to seek novel ways for deploying cryptojacking, their source of income, on the infrastructure of unsuspecting victims.

2.2.6 Fight back from law enforcement agencies

A major trend observed during this reporting period is that there are increasingly more **legal actions taken against cybercrime actors**. One such action making the news is the operation[196] [197] [198] against the **Hive** ransomware gang. Investigators were able to uncover operational details about the group and eventually slipped inside the group's infrastructure. And although this operation sends a message to cybercrime actors, it is to be expected that some of their members will lay low for a while and reappear[199] under new handles. The Hive group was not the only gang having an unfortunate day in the cybercrime trenches. The Dutch National Police, in collaboration with a private company, tricked[200] the DeadBolt ransomware gang into handing over 155 decryption keys by faking ransom payments. German Regional Police in cooperation with Ukrainian National Police arrested[201] members of the DoppelPaymer ransomware operation. The DoppelPaymer attacks were enabled by the prolific **Emotet** botnet. This botnet had been disrupted by law enforcement in early 2021 but reporting indicates it had been reactivated[202] [203] [204] multiple times during this reporting period.

Law enforcement agencies are not only chasing ransomware gangs, those behind **crime markets** and forums are also a target. Pompomurin, the administrator of BreachForums was arrested[205] [206]. Europol reported on the takedown[207] of Genesis Market, a marketplace selling stolen credentials. Those thinking of swapping forum

[189] Red Canary - 2023 Threat Detection Report - https://redcanary.com/resources/guides/threat-detection-report/.
[190] Kroll - Q3 2022 Threat Landscape: Insider Threat, The Trojan Horse of 2022 - https://www.kroll.com/en/insights/publications/cyber/threat-intelligence-reports/q3-2022-threat-landscape-insider-threat-trojan-horse.
[191] Mandiant - M-Trends 2023 - https://www.mandiant.com/resources/blog/m-trends-2023
[192] SonicWall - 2023 SonicWall Cyber Threat Report - https://www.sonicwall.com/2023-cyber-threat-report/.
[193] The Register - AstraLocker ransomware reportedly closes doors to pursue cryptojacking – https://www.theregister.com/2022/07/06/astralocker-ransomware-shutters-operations/.
[194] Bitdefender - AstraLocker Gang Abandons Ransomware, Switches to Cryptojacking - https://www.bitdefender.com/blog/hotforsecurity/astralocker-gang-abandons-ransomware-switches-to-cryptojacking/.
[195] Europol - Cryptocurrencies key to tackling organised crime – Europol and Basel Institute on Governance - https://www.europol.europa.eu/media-press/newsroom/news/cryptocurrencies-key-to-tackling-organised-crime-%E2%80%93-europol-and-basel-institute-governance.
[196] Europol - Cybercriminals stung as HIVE infrastructure shut down - https://www.europol.europa.eu/media-press/newsroom/news/cybercriminals-stung-hive-infrastructure-shut-down.
[197] BlackBerry - Hive Ransomware: $100 Million in Profits, Then the FBI Hid Inside Their Network - https://blogs.blackberry.com/en/2023/01/hive-ransomware-100-million-in-profits-then-the-fbi-hid-inside-their-network.
[198] DOJ - US Department of Justice Disrupts Hive Ransomware Variant - https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant.
[199] DarkReading - Effects of the Hive Ransomware Group Takedown - https://www.darkreading.com/vulnerabilities-threats/effects-of-the-hive-ransomware-group-takedown.
[200] Sophos - When cops hack back: Dutch police fleece DEADBOLT criminals (legally!) - https://nakedsecurity.sophos.com/2022/10/21/when-cops-hack-back-dutch-police-fleece-deadbolt-criminals-legally/.
[201] Europol - Germany and Ukraine hit two high-value ransomware targets - https://www.europol.europa.eu/media-press/newsroom/news/germany-and-ukraine-hit-two-high-value-ransomware-targets.
[202] Bleeping Computer - Emotet botnet now pushes Quantum and BlackCat ransomware - https://www.bleepingcomputer.com/news/security/emotet-botnet-now-pushes-quantum-and-blackcat-ransomware/.
[203] Proofpoint - A Comprehensive Look at Emotet's Fall 2022 Return - https://www.proofpoint.com/us/blog/threat-insight/comprehensive-look-emotets-fall-2022-return.
[204] Cryptolaemus1 – https://twitter.com/Cryptolaemus1/status/1587792659275448320.
[205] KrebsonSecurity - Feds Charge NY Man as BreachForums Boss 'Pompompurin' - https://krebsonsecurity.com/2023/03/feds-charge-ny-man-as-breachforums-boss-pompompurin/.
[206] Flashpoint - Another One Bites the Dust: The (Apparent) End of Breach Forums - https://flashpoint.io/blog/end-of-breach-forums/.
[207] Europol - Takedown of notorious hacker marketplace selling your identity to criminals - https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-notorious-hacker-marketplace-selling-your-identity-to-criminals.

conversation to dedicated **messaging services** are also out of luck. The Dutch national police shut down[208] Exclu, a criminal messaging service. This follows earlier actions against Sky ECC[209] and EncroChat[210].

Another arrow shot by law enforcement was right to the heart of **DDoS** operations. Europol[211] reported a take down against fifty of the world's biggest booter services. And although DDoS attacks might not sound as exciting as attacks via deepfakes, they have effectively lowered the entry barrier into cybercrime. So, any take-down, including those against DDoS-friendly hosters[212] has its effect on the cybercrime scene. The UK's National Crime Agency even went further[213] [214]. Their 'Operation PowerOFF' used fake Cybercrime-as-a-Service sites to attract the attention of individuals considering a career in crime. Anyone who attempted to register then received a friendly follow-up call warning them not to get into crime.

The playing field remains uneven though. Cybercriminals have no limits[215] in terms of sharing resources and know-how, whereas law-enforcement agencies have difficulties finding sufficient resources to do their job.

2.2.7 Deepfakes and AI

Artificial intelligence, and the uncertainties associated with Large Language Models (LLMs) have received a lot of attention lately. The cybersecurity world is no stranger to it either as AI, deepfakes and alike seem like a perfect fit for realistic and targeted social engineering attacks. Europol warned[216] about the potential misuse of artificial intelligence-powered chatbot ChatGPT in phishing attempts, information manipulation and cybercrime. And one should not forget that there are still plenty of older techniques, requiring much less effort and still providing good results for criminality. That is not to say that threat actors with the **resources and determination** to make use of the technology will ignore it altogether. This technology can certainly be used for highly targeted and specialised (but also high cost) campaigns.

2.2.8 Using extortion-only techniques

Criminal groups increasingly combined[217] extortion techniques and almost always included some form of **information stealing**. **Double extortion** increased[218] [219] [220], with some groups relying[221] solely on stealing information. Threat actors also combined double extortion with **other ways** of making the lives of victims more miserable. Examples include setting up a replica[222] of a victim's site on a typosquatted domain and using it to publish stolen data or combining malware with a clipboard stealer[223], replacing information on cryptocurrency transactions on the clipboard with transaction details chosen by the criminals. Other groups turned their attention to **backup software**, such as Veeam[224] [225]. After all, if you locked and stole information from a victim, destroying their backups is an additional way to cause despair. A more conservative approach is adding **DDoS** to the list. But DDoS is something that can come

[208] DarkReading - Exclu Shutdown Underscores Outsised Role Messaging Apps Play in Cybercrime - https://www.darkreading.com/endpoint/exclu-shutdown-underscores-outsized-apps-messaging-apps-role-in-cybercrime.
[209] BalkanInsight – Encrypted Phone Crack No Silver Bullet against Balkan Crime Gangs – https://balkaninsight.com/2022/04/25/encrypted-phone-crack-no-silver-bullet-against-balkan-crime-gangs/.
[210] Europol - Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe - https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe.
[211] Europol - Global crackdown against DDoS services shuts down most popular platforms - https://www.europol.europa.eu/media-press/newsroom/news/global-crackdown-against-ddos-services-shuts-down-most-popular-platforms.
[212] KrebsonSecurity – German Police Raid DdoS-Friendly Host 'FlyHosting' – https://krebsonsecurity.com/2023/03/german-police-raid-ddos-friendly-host-flyhosting/.
[213] NCA - NCA infiltrates cybercrime market with disguised DDoS sites - https://www.nationalcrimeagency.gov.uk/news/nca-infiltrates-cyber-crime-market-with-disguised-ddos-sites.
[214] Sophos – Cops use fake DdoS services to take aim at wannabe cybercriminals – https://nakedsecurity.sophos.com/2023/03/28/cops-use-fake-ddos-services-to-take-aim-at-wannabe-cybercriminals/.
[215] Interpol - https://www.interpol.int/content/download/19174/file/African%20Cyberthreat%20Assessment%20Report%202022-V2.pdf.
[216] Europol - The impact of Large Language Models on Law Enforcement - https://www.europol.europa.eu/cms/sites/default/files/documents/Tech%20Watch%20Flash%20-%20The%20Impact%20of%20Large%20Language%20Models%20on%20Law%20Enforcement.pdf.
[217] EclecticIQ – EclecticIQ Retrospective: A Look at the Themes & Events That Shaped the 2022 Cyber Landscape - https://blog.eclecticiq.com/eclecticiq-retrospect-a-look-at-the-themes-events-that-shaped-the-2022-cyber-landscape.
[218] Sonicwall - 2023 cyber threat report - https://www.sonicwall.com/2023-cyber-threat-report/.
[219] Red Canary - 2023 Threat Detection Report - https://redcanary.com/resources/guides/threat-detection-report/.
[220] Tenable - 2022 threat landscape report - https://www.tenable.com/cyber-exposure/tenable-2022-threat-landscape-report.
[221] Mandiant - MTrends 2023 - https://www.mandiant.com/resources/blog/m-trends-2023.
[222] Blackberry - Global Intelligence Report - https://www.blackberry.com/content/dam/bbcomv4/global/pdf/0408-Threat-ReportV17.pdf.
[223] Bleeping Computer - New clipboard hijacker replaces crypto wallet addresses with lookalikes - https://www.bleepingcomputer.com/news/security/new-clipboard-hijacker-replaces-crypto-wallet-addresses-with-lookalikes/.
[224] BlackBerry - The Curious Case of 'Monti' Ransomware: A Real-World Doppelganger - https://blogs.blackberry.com/en/2022/09/the-curious-case-of-monti-ransomware-a-real-world-doppelganger.
[225] SOCRadar – Veeam Fixes Critical Vulnerabilities in Backup & Replication Software – https://socradar.io/veeam-fixes-critical-vulnerabilities-in-backup-replication-software-cve-2022-26500-cve-2022-26501/.

back as a boomerang. During the reporting period, several leak sites were subjected to DDoS attacks[226], some even referring[227] [228] to a breach they had conducted earlier.

It is highly likely that cybercrime actors will stay focussed on information theft as the return on investment for these operations is more rewarding than merely locking up data. It is also to be expected that these actors will come up with new novel ways for extorting victims.

2.2.9 Ransomware activity

Ransomware revenues, although still substantial, **went down**[229] in 2022 according to reports by ChainAnalysis. That does not mean the number of attacks was down, it was due to victims refusing to pay. First and foremost, this can be associated with the increased level of awareness and improved maturity within organisations. Additionally, it may be explained by the fact that paying ransomware is legally riskier as it may be perceived as funding the criminal market. Another explanation is that because companies need to meet security and backup requirements to qualify for cyber insurance, they now have more capacity to recover from an attack, without the need to pay. Ransomware operators have added search functionality[230] to their leak sites. This increases **victimisation**, draws more visitors to their sites and brings attention to the stolen data. There was also a lot of competition[231] between various groups. We expect that ransomware operations will increasingly expose victims, sometimes as an additional way to put pressure and convince victims to pay.

And although the Conti group has dissolved, that does not mean their techniques[232] are no longer successful, partially because some of their gang **members remained active**[233] [234] [235] in the cybercrime world. Next to **copycatting techniques**, gangs are also looking at re-using **tooling** that proved to be successful. The leak of ransomware builders[236] [237] is used to update existing toolsets or by new groups to enter the market. It is very likely that the wide availability of these builders in combination with the as-a-service markets lowers the barriers to entry into the cybercrime market and leads to additional (but maybe short-lived) ransomware groups popping up.

Human-operated ransomware maintains[238] its position as one of the most impactful cyberattack trends world-wide. These attacks often exploit vulnerabilities, use valid accounts, take advantage of misconfigurations or rely on dual-use tools to find their ways to the crown jewels. It is also not uncommon that, as a means for evading defences, security products are reconfigured or disabled. It is likely we will continue to see human-operated ransomware in targeted attacks, by well-resourced cybercrime gangs. Those less resourced or skilful will likely revert to readily available tools, use the proven playbooks or buy their services from criminal markets.

2.3 HACKER-FOR-HIRE ACTOR TRENDS

2.3.1 Cybercrime market is booming

[226] Cisco Talos - Multiple ransomware data leak sites experience DDoS attacks, facing intermittent outages and connectivity issues - https://blog.talosintelligence.com/multiple-ransomware-data-leak-sites-experience-ddos-attacks-facing-intermittent-outages-and-connectivity-issues/.
[227] Bleeping Computer - LockBit claims ransomware attack on security giant Entrust, leaks data - https://www.bleepingcomputer.com/news/security/lockbit-claims-ransomware-attack-on-security-giant-entrust-leaks-data/.
[228] vx-underground - https://twitter.com/vxunderground/status/1561262483448512513.
[229] Chainanalysis – Ransomware Revenue Down As More Victims Refuse to Pay – https://blog.chainalysis.com/reports/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/.
[230] Bleeping Computer - Ransomware gang now lets you search their stolen data - https://www.bleepingcomputer.com/news/security/ransomware-gang-now-lets-you-search-their-stolen-data/.
[231] Sophos - Hive, LockBit and BlackCat Ransomware Gangs Consecutively Attack the Same Network, Sophos Reports - https://www.sophos.com/en-us/press/press-releases/2022/08/hive-lockbit-and-blackcat-ransomware-gangs-consecutively-attack-the-same-network.
[232] BlackBerry - The Curious Case of 'Monti' Ransomware: A Real-World Doppelganger - https://blogs.blackberry.com/en/2022/09/the-curious-case-of-monti-ransomware-a-real-world-doppelganger.
[233] Trend Micro - Conti Team One Splinter Group Resurfaces as Royal Ransomware with Callback Phishing Attacks - https://www.trendmicro.com/en_us/research/22/l/conti-team-one-splinter-group-resurfaces-as-royal-ransomware-wit.html.
[234] Vitali Kremez - https://twitter.com/VK_Intel/status/1557003350541242369.
[235] Mandiant - M-Trends 2023 - https://www.mandiant.com/resources/blog/m-trends-2023.
[236] Trend Micro – New Mimic Ransomware Abuses Everything APIs for its Encryption Process – https://www.trendmicro.com/en_us/research/23/a/new-mimic-ransomware-abuses-everything-apis-for-its-encryption-p.html.
[237] Bleeping Computer - TommyLeaks and SchoolBoys: Two sides of the same ransomware gang - https://www.bleepingcomputer.com/news/security/tommyleaks-and-schoolboys-two-sides-of-the-same-ransomware-gang/.
[238] Microsoft - Microsoft DART ransomware case study - https://learn.microsoft.com/en-us/security/ransomware/dart-ransomware-case-study.

The Initial Access Broker (IAB) market is booming[239] [240] [241] [242] [243], with a year-over-year growth in the number of groups and the volume of credentials for sale as per numerous reports. According to Google, this growth is[244] due to an increasing number of financially motivated threat actors targeting Ukraine, some with activities closely aligned with attackers backed by the Russian government.

The prime goods of this IAB market are **credentials**, primarily for VPN and RDP account takeovers or for credential stuffing attacks. Some credentials are obtained after exploiting[245] vulnerabilities, some are gathered after data leakage but the majority[246] is obtained by information or credential stealer malware. Prime examples are RedLine, Raccoon and Vidar. These stealers commonly find[247] their way to victim machines via **social engineering**, mostly phishing, some even via a paid distribution scheme relying on the Emotet and Qakbot botnets. Other campaigns lure users into downloading seemingly legitimate software, for example via **malvertising**. We expect that future social engineering campaigns to obtain credentials and install information stealers will further anticipate[248] new defensive measures to protect the abuse of credentials.

Historically a lot of phishing campaigns relied on document macros to get malware executed. The change[249] by Microsoft to disable Mark of the Web (MotW) by default and **block macros** coming from the Internet made this technique obsolete. Threat actors switched[250] [251] [252] to **compressed files**, **containers** and **LNK** shortcuts. And just as defenders started to adjust their detection methods, threat actors looked at other ways to trick users. Since 2023 there has been an upsurge[253] in the number of campaigns using **OneNote** documents for malware distribution. Similar to traditional Office documents, OneNote documents are delivered as email attachments but actors can also use URLs pointing to online documents. The spike in OneNote has dropped significantly since March 2023, most likely because Microsoft[254] introduced improved protection measures. This change in behaviour, switching from macros to compressed files and then to OneNote, is an example of the behaviour of threat actors who want to obtain initial access. Once a number of groups starts using new techniques, other groups quickly follow their example. This **rapid adoption of a new technique** was a key trend[255] observed during the reporting period.

In general, the cybercriminal ecosystem has experienced a monumental shift in activity and threat behaviour over the last year. Threat actors no longer use static, predictable attack chains to gain initial access, but rely and will keep on relying on dynamic, rapidly changing techniques. In addition, this ecosystem has been transformed into an industry, with a network of supporting services with proven and professionalised approaches to its operations.

2.3.2 Expansion of the As-a-Service model

Several threat actors further **professionalised**[256] [257] their As-a-Service programmes. Not only did they employ new tactics and techniques for gaining access to environments but they also explored **additional ways to coerce** and **extort** victims and **promote**[258] their businesses. Because these marketplaces are becoming increasingly

[239] Cisco Talos - What Old is New Again and What's Old is Me? - https://blog.talosintelligence.com/threat-source-012623/.
[240] CrowdStrike - 2023 Global Threat Report - https://www.crowdstrike.com/global-threat-report/.
[241] Mandiant – M-Trend 2023 – https ://www.mandiant.com/resources/blog/m-trends-2023.
[242] Kroll - Q3 2022 Threat Landscape: Insider Threat, The Trojan Horse of 2022 - https://www.kroll.com/en/insights/publications/cyber/threat-intelligence-reports/q3-2022-threat-landscape-insider-threat-trojan-horse.
[243] Group IB - Hi-Tech Crime Trends 2022/2023 - https://go.group-ib.com/hubfs/report/protected/group-ib-hi-tech-crime-trends-2022-2023-en.pdf.
[244] Google TAG - Initial access broker repurposing techniques in targeted attacks against Ukraine - https://blog.google/threat-analysis-group/initial-access-broker-repurposing-techniques-in-targeted-attacks-against-ukraine/.
[245] Group IB - Hi-Tech Crime Trends 2022/2023 - https://go.group-ib.com/hubfs/report/protected/group-ib-hi-tech-crime-trends-2022-2023-en.pdf.
[246] Recorded Future - 2022 Annual Report - https://www.osintme.com/wp-content/uploads/2023/03/Recorded_Future_Annual_Report.pdf.
[247] Sophos – 2023 Threat Report – https://www.sophos.com/en-us/content/security-threat-report.
[248] PWC - Cyber Threats 2022: A Year in Retrospect - https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/pdf/2022-year-in-retrospect-report.pdf.
[249] Microsoft - Macros from the internet will be blocked by default in Office - https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked.
[250] Red Canary – 2023 Threat Detection Report – https://redcanary.com/resources/guides/threat-detection-report/.
[251] The DFIR Report - 2022 Year in Review - https://thedfirreport.com/2023/03/06/2022-year-in-review/.
[252] Recorded Future - 2022 Annual Report - https://www.osintme.com/wp-content/uploads/2023/03/Recorded_Future_Annual_Report.pdf.
[253] Trellix - Qakbot Evolves to OneNote Malware Distribution - https://www.trellix.com/en-us/about/newsroom/stories/research/qakbot-evolves-to-onenote-malware-distribution.html.
[254] Bleeping Computer - Microsoft OneNote to get enhanced security after recent malware abuse - https://www.bleepingcomputer.com/news/microsoft/microsoft-onenote-to-get-enhanced-security-after-recent-malware-abuse/.
[255] Proofpoint - Crime Finds a Way: The Evolution and Experimentation of the Cybercrime Ecosystem - https://www.proofpoint.com/sites/default/files/misc/pfpt-us-threat-research-2023-05-12-cybercrime-experimentation.pdf.
[256] PWC - Cyber Threats 2022: A Year in Retrospect - https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/pdf/2022-year-in-retrospect-report.pdf.
[257] Group IB – Hi-Tech Crime Trends 2022/2023 – https://go.group-ib.com/hubfs/report/protected/group-ib-hi-tech-crime-trends-2022-2023-en.pdf.
[258] Crowdstrike - Global Threat Report - https://www.crowdstrike.com/global-threat-report/.

commodified, their look and feel has also changed[259]. Instead of clumsy interfaces, these forums now foresee having space for advertisements with animated banners directed at the forum's users. The operators pay more attention to graphic design and layout, moving to eye-catching imagery designed to give products an **air of professionalism** and **legitimacy**. One of the reasons for its success is the fact that the cybercrime industry is relatively easy to enter even for inexperienced threat actors. Operators offering their tools and expertise as subscription services making[260] it so that almost anyone can conduct attacks.

One of the trends we expect to witness in the future is different **interconnected Crime-as-a-Service** or CaaS markets providing blueprints for attacks. One service does the intelligence gathering and profiling, whereas others get an initial foothold in the organisation and associates then launch the final objective of the attack.

2.3.3 Spyware industries and global surveillance continue booming

The spyware industry has boomed[261] [262] [263] further and this type of borderline-illegal software remains a threat to all of us. In ways to legitimise their products this industry often claims[264] that their services are intended to focus on criminals and terrorists, whereas in fact they regularly target **journalists, politicians** and **political opposition** as well as **human rights activists**. And while surveillance technologies can serve a purpose, there are rising **concerns**[265] about privacy, human rights, transparency, accountability and ethical considerations. There is a trend from public and private entities to **take action**[266] [267] [268] [269] [270] [271] and address these concerns.

In March 2023 multiple opensource reports documented the "Vulkan files". These files included emails and other documents, implicating the Russian company NTC Vulkan in providing equipment's and technology to Russian governmental military including the GRU. We can assess that these technologies supported Russian cyber malicious activities, with some of them conducted by the GRU-linked group Sandworm. Based on Mandiant's report, Vulkan also provided technologies capable of targeting OT systems, including a training platform to simulate OT attacks. The leaks showed[272] [273] that cybersecurity companies contribute to bolster Russia's cyber offensive capabilities.

2.3.4 Geopolitical motivations

Hackers-for-hire are not immune from being influenced by geopolitical events. We had a first taste during the previous reporting period with the split of the Conti group and this only **expanded further**[274] [275] [276]. Also, it is interesting that **state-nexus groups** adopted attack patterns typically seen in criminal campaigns.

[259] Sophos 2023 – Threat Report – https://www.sophos.com/en-us/content/security-threat-report.
[260] Seqrite - 2023 Cybersecurity Trend Forecast - https://www.seqrite.com/seqrite-prediction-report-2023.
[261] Cisco Talos - Threat Source newsletter (Feb. 16, 2023) — Recapping what we may have missed so far this year - https://blog.talosintelligence.com/threat-source-newsletter-feb-16-2023/.
[262] Google TAG - Spyware vendors use 0-days and n-days against popular platforms https://blog.google/threat-analysis-group/spyware-vendors-use-0-days-and-n-days-against-popular-platforms/.
[263] Amnesty International - uncovers new hacking campaign linked to mercenary spyware company - https://www.amnesty.org/en/latest/news/2023/03/new-android-hacking-campaign-linked-to-mercenary-spyware-company/.
[264] Meta – Threat Report on the Surveillance-for-Hire Industry – https://about.fb.com/wp-content/uploads/2022/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf.
[265] SOCRadar - Beyond the Veil of Surveillance: Private Sector Offensive Actors (PSOAs) - https://socradar.io/beyond-the-veil-of-surveillance-private-sector-offensive-actors-psoas/.
[266] European Parliament - Spyware: MEPs sound alarm on threat to democracy and demand reforms - https://www.europarl.europa.eu/news/en/press-room/20230505IPR84901/spyware-meps-sound-alarm-on-threat-to-democracy-and-demand-reforms.
[267] https://www.europarl.europa.eu/committees/en/pega/home/highlights.
[268] Greek City Times – Greece to ban spyware as wiretap scandal continues – https://greekcitytimes.com/2022/12/09/greece-to-ban-spyware-as-wiretap-scandal-continues/.
[269] The White House - EO on Prohibition on Use by the United States Government of Commercial Spyware that Poses Risks to National Security - https://www.whitehouse.gov/briefing-room/presidential-actions/2023/03/27/executive-order-on-prohibition-on-use-by-the-united-states-government-of-commercial-spyware-that-poses-risks-to-national-security/.
[270] Cybersecurity Tech Accord - Cyber mercenaries: An old business model, a modern threat Cybersecurity Tech Accord principles limiting offensive operations in cyberspace - https://cybertechaccord.org/uploads/prod/2023/03/Cyber-mercenary-principles_Tech-Accord_032723_FINAL.pdf.
[271] Microsoft - https://blogs.microsoft.com/on-the-issues/2023/04/11/cyber-mercenaries-cybersecurity-tech-accord/.
[272] The Guardian - 'Vulkan files' leak reveals Putin's global and domestic cyberwarfare tactics - https://www.theguardian.com/technology/2023/mar/30/vulkan-files-leak-reveals-putins-global-and-domestic-cyberwarfare-tactics.
[273] Mandiant - Contracts Identify Cyber Operations Projects from Russian Company NTC Vulkan - https://www.mandiant.com/resources/blog/cyber-operations-russian-vulkan.
[274] Sophos - 2023 Threat Report – https://www.sophos.com/en-us/content/security-threat-report.
[275] Dragos - Industrial Ransomware Analysis: Q3 2022 - https://www.dragos.com/blog/industry-news/dragos-industrial-ransomware-analysis-q3-2022/.
[276] CrowdStrike - 2023 Global Threat Report - https://www.crowdstrike.com/global-threat-report/.

The Cuba ransomware group, for example, conducted an information stealing operation[277] against government agencies in Montenegro, allegedly in retaliation after Montenegro joined EU sanctions against Russia and expelled several Russian diplomats. The group[278] [279] [280] primarily targets[281] [282] government and military officials in Ukraine, not only for ransomware purposes but also for intelligence collection. The group behind Cuba ransomware uses a variety of techniques that include targeted **malvertising**[283] where the RomCom lure[284] sites point to trojanised versions of legitimate applications.

2.4 HACKTIVISTS' TRENDS

2.4.1 Hacktivists capitalising on geopolitical events

There is an intensification of activities by groups that emerged after the invasion of **Ukraine**. Several new groups have emerged and those that were well-established continued doing at what they were good. In most cases this concerns **DDoS** attacks, despite promises of changes in their TTPs. And while in general the longstanding effects of attacks are limited, the disruption of services can have an undesirable impact. Although it includes the largest part of reported incidents, hacktivist activities were not limited to the war in Ukraine. There was also a strong uptick[285] of attacks in Taiwan following the visit from US officials.

One of the most active groups is NoName057, a pro-Russian hacktivist group first observed in March 2022. The group launched a **crowdsourced** project 'DDOSIA' where volunteers are encouraged to download and install a bot on their computers to launch denial-of-service attacks. The group went even as far as offering[286] financial rewards to its volunteers. Another notorious DDoS group is Killnet. Their campaigns are focussed on the disruption of services and drawing public attention to their cause. They do not seek financial gain and the victimology is similar to NoName057. What sets Killnet apart is that they collaborate with other groups to execute their operations. These alliances, and the decentralised structure, do not come without a risk. The doxing[287] of the leader of Anonymous Russia by the supposed leader of Killnet is an example of the 'fight' for leadership between these groups. It also shows their desire to preserve a degree of **operational independence** from affiliated groups.

Hacktivists' activities related to the Ukrainian war are not limited to DDoS campaigns. There is a trend for hacktivists to conduct **espionage campaigns**, in line with the global objectives of the Belarusian and Russian governments. These activities[288] can sometimes put them in the category of state-sponsored groups but their lack of resources and scrappiness makes them stand out and warrants that they be categorised as hacktivists. In response to Russia's invasion, pro-Ukraine hacktivists remained active and launched cyberattacks against Russia such as hack-and-leaks and DDoS attacks and claimed they had disrupted critical infrastructure. There is limited visibility of the impact these claimed attacks had on Russian targets.

It is very likely that hacktivism will continue to support a variety of political ideals, particularly in countries experiencing civil unrest or war. Some of these groups will remain active for a longer period of time, where others will dissolve and their members will continue operations under the umbrella of other groups.

[277] Reuters - Montenegro blames criminal gang for cyberattacks on government - https://www.reuters.com/world/europe/montenegro-blames-criminal-gang-cyber-attacks-government-2022-08-31/.
[278] Google TAG - Ukraine remains Russia's biggest cyber focus in 2023 - https://blog.google/threat-analysis-group/ukraine-remains-russias-biggest-cyber-focus-in-2023/.
[279] CERT-UA - https://cert.gov.ua/article/2394117.
[280] Blackberry - Unattributed RomCom Threat Actor Spoofing Popular Apps Now Hits Ukrainian Militaries - https://blogs.blackberry.com/en/2022/10/unattributed-romcom-threat-actor-spoofing-popular-apps-now-hits-ukrainian-militaries.
[281] Trend Micro - Void Rabisu's Use of RomCom Backdoor Shows a Growing Shift in Threat Actors' Goals - https://www.trendmicro.com/en_us/research/23/e/void-rabisu-s-use-of-romcom-backdoor-shows-a-growing-shift-in-th.html.
[282] BlackBerry - RomCom Threat Actor Abuses KeePass and SolarWinds to Target Ukraine and Potentially the United Kingdom - https://blogs.blackberry.com/en/2022/11/romcom-spoofing-solarwinds-keepass.
[283] Trend Micro - IcedID Botnet Distributors Abuse Google PPC to Distribute Malware - https://www.trendmicro.com/en_us/research/22/l/icedid-botnet-distributors-abuse-google-ppc-to-distribute-malware.html.
[284] Trend Micro - Void Rabisu's Use of RomCom Backdoor Shows a Growing Shift in Threat Actors' Goals - https://www.trendmicro.com/en_us/research/23/e/void-rabisu-s-use-of-romcom-backdoor-shows-a-growing-shift-in-th.html.
[285] Reuters - Attacks on Taiwan websites likely work of Chinese 'hacktivists' - researchers - https://www.reuters.com/world/attacks-taiwan-websites-likely-work-chinese-hacktivists-researchers-2022-08-02/.
[286] TechMonitor - Pro-Russian hacktivist group offers citizens financial rewards to join DDoS attacks - https://techmonitor.ai/technology/cybersecurity/noname057-russia-ukraine-hacktivist.
[287] Flashpoint - Killnet Ostracises Leader of Anonymous Russia, Adding New Chapter to Pro-Kremlin Hacktivist Drama – https://flashpoint.io/blog/killnet-anonymous-russia-pro-kremlin-hacktivism/.
[288] Avertium – APT Winter Vivern Resurfaces in 2023 – https://explore.avertium.com/resource/apt-winter-vivern-resurfaces.

2.4.2 Regime opposing groups

During the reporting period there were hacktivists activities linked to **civil unrest** on what is happening in Iran. Since October, several anti-regime groups conducted[289] DDoS and hack-and-leak operations against Iran to foment nationwide protests. Some of these groups were established previously and shifted their focus, whereas other groups have cropped up.

2.4.3 Targeting OT

Hacktivists are increasingly claiming[290] that they target OT environments but public reporting indicate they often[291] **overestimate** or **do not substantiate** their claims. The operations are done against insecure, internet accessible devices or public-facing applications with default credentials or insecure configurations.

In some cases, hacktivists also conduct a **form of information manipulation** campaigns. This includes sharing videos and photos of physical incidents and claiming these are the result of their activities without substantial proof to support their claims. An example is the Iraqi group Altahrea who took responsibility for a power plant fire in Israel without any evidence linking the incident to the groups' activity. Regardless of the existence of proof, the objective of the hacktivist groups, i.e. to obtain attention and, in some cases, to cause fear, was achieved. We expect that hacktivists will continue claiming to have successfully targeted OT (or industrial) environments. This is not to say that they cannot achieve success, though when they are successful it will most likely be because of a misconfiguration or the unintended exposure of a system; however, it is unlikely they will be successful in the immediate future. It is more likely that physical hacktivists actions will be more successful.

2.4.4 Hacktivism or false flags?

There is **state-sponsored activity** that tries to **hide under the flag of hacktivism**. The most notable case has been that of **Anonymous Sudan** targeting several Swedish entities with DDoS attacks. Investigations[292] [293] revealed that Anonymous Sudan is likely a sub-group of the pro-Russian group Killnet. The campaigns[294] [295] were most likely created as part of a Russian operation to create fear and uncertainty in Sweden to complicate its application to join NATO.

As long as the war in Ukraine continues, it is very likely that groups such as Anonymous Sudan will continue to exist. These groups, seemingly hacktivists but most likely state-sponsored or affiliated, will continue to participate in hacktivists activities, causing various provocations and manipulations. It is highly likely that the activities of these groups will strongly underline the operations carried out through information manipulation and interference campaigns.

[289] Microsoft - Microsoft Threat Intelligence Iran turning to cyber-enabled influence operations for greater effect – https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/05/Iran-turning-to-cyber-enabled-influence-operations-for-greater-effect-05022023.pdf.
[290] Mandiant - We (Did!) Start the Fire: Hacktivists Increasingly Claim Targeting of OT Systems - https://www.mandiant.com/resources/blog/hacktivists-targeting-ot-systems.
[291] Claroty - Hacktivist Group Claims Ability to Encrypt an RTU Device - https://claroty.com/team82/blog/hacktivist-group-claims-ability-to-encrypt-an-rtu-device.
[292] Trustwave - Anonymous Sudan: Religious Hacktivists or Russian Front Group? – https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/anonymous-sudan-religious-hacktivists-or-russian-front-group/.
[293] Japan Times - Posing as Islamists, Russian hackers take aim at Sweden - https://www.japantimes.co.jp/news/2023/05/14/world/russia-hackers/.
[294] TrueSec - Hacktivists Target Denmark in Simultaneous Attacks - https://www.truesec.com/hub/blog/hacktivists-target-denmark-in-simultaneous-attacks.
[295] The Record - Hacker group Anonymous Sudan demands $3 million from Scandinavian Airlines - https://therecord.media/hacker-group-anonymous-sudan-demands-three-million-from-sas.


CVE

3. ANALYSIS OF THE VULNERABILITIES LANDSCAPE 2022-2023

The analysis of the vulnerabilities landscape provides insights into the evolving landscape of software vulnerabilities and allows the reader to identify trends, patterns and emerging threats, thus aiding the enhancement of cybersecurity strategies. By understanding the frequency, severity and types of vulnerabilities discovered, organisations can prioritise patching and mitigation efforts, allocate resources effectively and proactively address potential risks to their systems and data This proactive approach helps to minimize the potential for security breaches, data breaches, and other cyberattacks, ultimately contributing to a more resilient and secure digital environment[296].

Moreover, this work is meant to complement the annual ETL by giving a glimpse into the vulnerabilities that are often leveraged in cyberattacks. The ETL is based on public sources and ENISA has tried to cross-correlate the analysis of the vulnerability landscape with that of the publicly disclosed incidents, to identify trends in the vulnerabilities exploited etc. However, unfortunately it is not common practice to disclose such information to the public and hence this much need and useful analysis was not feasible. With the Network and Information Security Directive 2 (NISD 2), enhancements in both incident reporting and vulnerability management and disclosure are expected in the EU, which will hopefully enable us to conduct more in depth and correlated analysis. In our exploration of the CVE Landscape, we considered the following definitions of key terms associated with Vulnerability foreclosure:

CVE[297] (Common Vulnerabilities and Exposures) is a standardized system designed for identifying and naming security vulnerabilities in various software and hardware products. It assigns a unique identifier to each vulnerability, making it simpler to track and reference vulnerabilities across different systems and databases.

CVSS[298] [299] (Common Vulnerability Scoring System) is a framework used to evaluate the severity of security vulnerabilities. It offers a numerical score that quantifies a vulnerability's impact and exploitability, helping organizations prioritize which vulnerabilities to address first.

Table 1: NVD Vulnerability Severity Ratings: CVSS v2.0 Ratings CVSS v3.0 Ratings

Severity	Base Score Range
Low	0.0-3.9
Medium	4.0-6.9
High	7.0-10.0

Severity	Base Score Range
None	0.0
Low	0.1-3.9
Medium	4.0-6.9
High	7.0-8.9
Critical	9.0-10.0

[296] It should be noted that the CVE, CWE, OWASP, and CVSS frameworks have altered the trajectory of vulnerability reporting and data in the past: https://www.first.org/events/colloquia/cardiff2023/program#pTime-and-Magnitude-Epoch-Fail-Forecasting-Vulnerabilities-Amid-Temporal-Discontinuity
[297] https://cve.mitre.org/
[298] https://www.first.org/cvss/
[299] https://nvd.nist.gov/vuln-metrics/cvss/v3-calculator

CNA[300] (CVE Numbering Authority) is an organization or entity responsible for assigning CVE identifiers to vulnerabilities and ensuring their accuracy and consistency.

CWE[301] (Common Weakness Enumeration) is a catalog of common software and hardware weaknesses, security issues, and coding errors. It serves as a reference for known software security vulnerabilities and is instrumental in improving the understanding and mitigation of these security weaknesses during the software development process.

3.1 SUMMARY

During the timeframe under examination in this report, spanning from July 1, 2022, to June 30, 2023, a total of **24,690** vulnerabilities were recorded after excluding those that were rejected, disputed, or reserved. This represents a significant increase compared to the **21,920** vulnerabilities reported in the previous ETL document for the period between July 1, 2021, and June 30, 2022.

Additionally, it's noteworthy that within this specific time frame, **100** out of the **24,690** published vulnerabilities are cross-referenced in the 'CISA Known Exploited Vulnerabilities catalogue'[302] (KEV).

It's important to highlight that for a vulnerability to be included in the 'CISA Known Exploited Vulnerabilities Catalog,' it must satisfy specific criteria. To qualify for inclusion in the catalog, a vulnerability must meet three key criteria: it should have a Common Vulnerabilities and Exposures (CVE) ID, there must be credible evidence of active exploitation, and a clear remediation action, such as a vendor-provided update, should be available.

3.2 ANALYSIS OF THE CVE NUMBERING AUTHORITIES (CNA[303])

In the section below, an examination of the allocation of CVEs by CVE numbering authorities (CNAs) has been carried out. The aim of this analysis is to identify any discernible trends or patterns related to specific vendors, which can assist the reader in making informed decisions about prioritizing patching activities. Within the EU and EFTA countries, there are a total of 49 partner CNAs.

The following illustration presents the distribution of CVE numbers assigned by each CVE numbering organization (CNA) for the specified period from July 2022 till June 2023:

[300] https://cve.mitre.org/cve/cna.html
[301] https://cwe.mitre.org/
[302] Known Exploited Vulnerabilities Catalogue | CISA.
[303] CNAs are vendor, researcher, open source, CERT, hosted service, and bug bounty provider organizations authorized by the CVE Program to assign **CVE IDs** to vulnerabilities and publish **CVE Records** within their own specific scopes of coverage. https://www.cve.org/ProgramOrganization/CNAs

Figure 12: Percentage of CVEs by CVE Numbering Authority (CNA) (Percentage of the total)

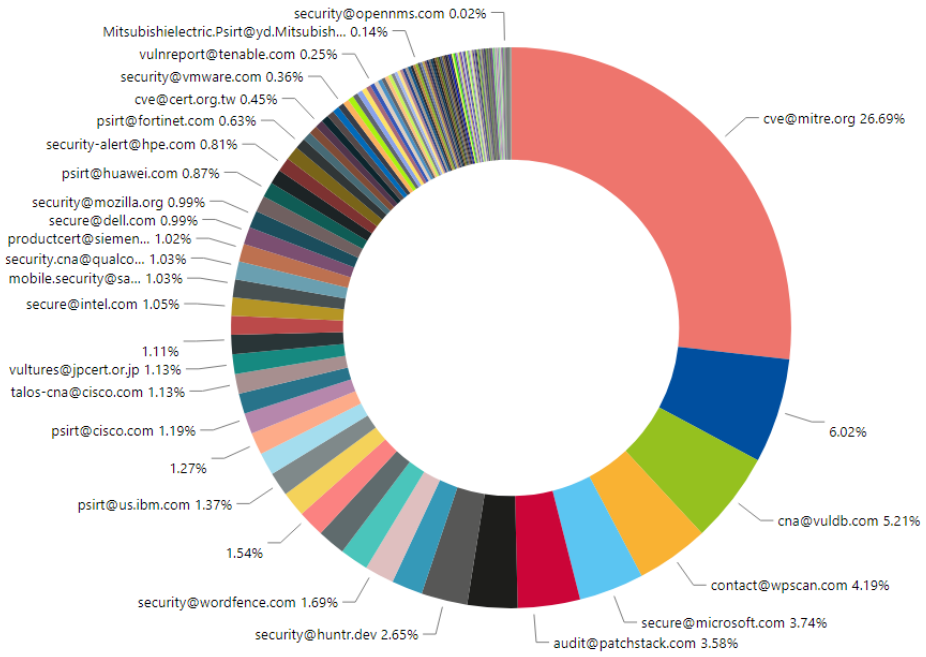
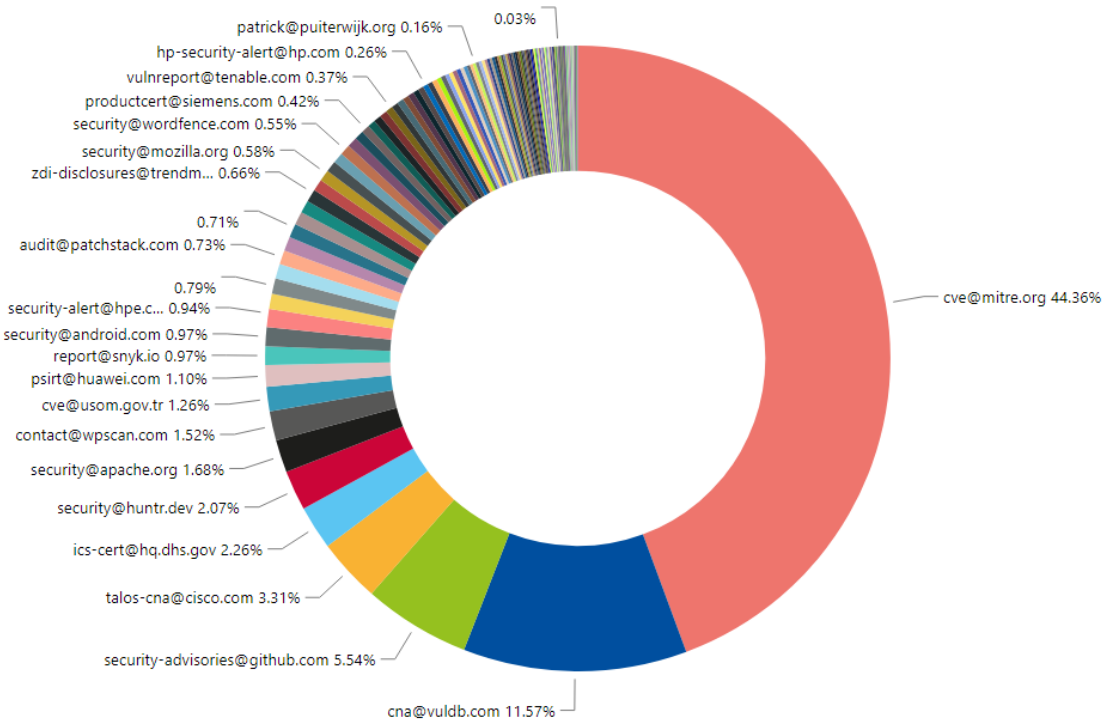


Figure 13: Percentage of CVEs with CVSS greater than 9 by CNA (Percentage of the total)



By comparing both figures (figure 12, 13) it becomes evident that the proportion of critical vulnerabilities, those with a CVSS score exceeding 9, differs among various CNAs. For example, MITRE, one of the two Top-Level Root CNAs, is

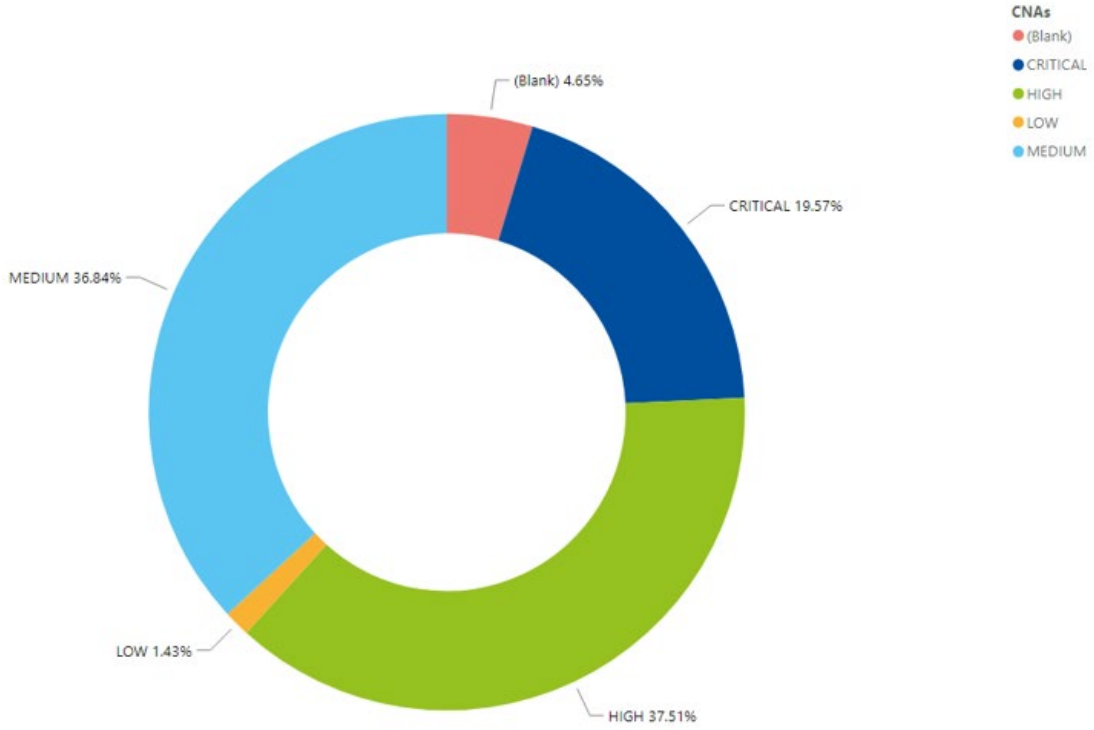
accountable for nearly half of the critical vulnerabilities in the overall count, despite being responsible for assigning a smaller proportion of the total CVEs, approximately around one-third.

3.3 ANALYSIS OF THE CVE LANDSCAPE

In the duration covered by this year's ETL report, a substantial number of vulnerabilities, specifically 13,650 in total, were identified. These vulnerabilities were categorized based on their severity, with 19.57% falling into the "critical" category and 37.51% categorized as "high" according to NVD baseSeverity assessments.

Among these vulnerabilities, it's noteworthy that approximately 100 of them were subsequently included in the CISA Known Exploited Vulnerabilities (KEV) list. This selection indicates that these particular vulnerabilities were actively targeted and exploited by malicious actors, making them of significant concern to the security community[304].

Figure 14: Percentage of CVEs by Severity (Percentage of the total)

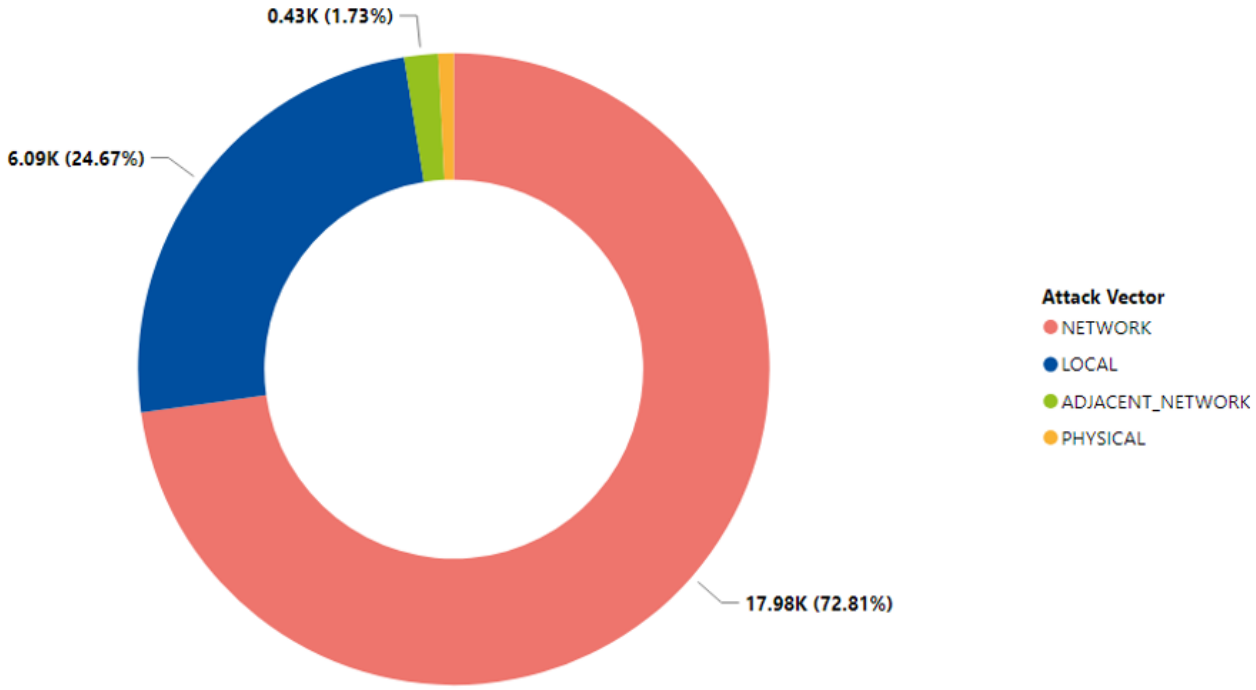


The donut chart, as depicted in Figure 14, offers a comprehensive view of the distribution of vulnerabilities. It doesn't solely display the percentages of vulnerabilities that fall into the predefined categories of "baseSeverity LOW, MEDIUM, HIGH, or CRITICAL," but it also accounts for another significant aspect. This includes vulnerabilities for which no specific severity level has been assigned at the present moment.

This additional category acknowledges that there are vulnerabilities for which the assessment of their severity is either pending, not yet determined, or for some reason hasn't been assigned. In essence, this section of the chart highlights the existing uncertainties or gaps in categorizing these vulnerabilities based on their severity.

[304] https://www.cisa.gov/known-exploited-vulnerabilities

Figure 15: Number and percentage of CVEs by attack vector



It is crucial to underscore the importance of patching internet-facing applications that contain vulnerabilities rated as "high" or "critical." This practice is essential to safeguard your organization from potential attacks. In numerous instances, vulnerabilities falling into these categories may present a more accessible entry point for malicious actors seeking to breach your systems and access your data. Such breaches could result in financial losses, harm to your organization's reputation, or even lead to regulatory penalties. However, it's imperative not to disregard vulnerabilities with lower severity ratings, as they often serve as footholds in later stages of cyberattacks. It's worth noting that approximately 20% of vulnerabilities from the CISA KEV list fall into the "medium" severity category.

These findings align to a significant extent with the list of the top 25 vulnerabilities in 2023[305] published by Mitre, as well as with the previous year's ETL report. The recurring appearance of fundamentally similar software development flaws in the data, with a few exceptions, sheds light on the enduring challenges in secure software development. It underscores the limited progress made in addressing these vulnerabilities over time. While there are certainly outliers in the comparison and no absolute congruence, a broader view reveals striking resemblances in the types of vulnerabilities.

In Table 2 and Figure 16, the most prevalent vulnerabilities published during the period from July 1, 2022, to July 1, 2023, are captured by assessing the average CVSSv3 baseScore and the overall count of CISA KEV vulnerabilities

[305] https://cwe.mitre.org/top25/index.html

Figure 16: Number of CWEs from July2022 till June 2023

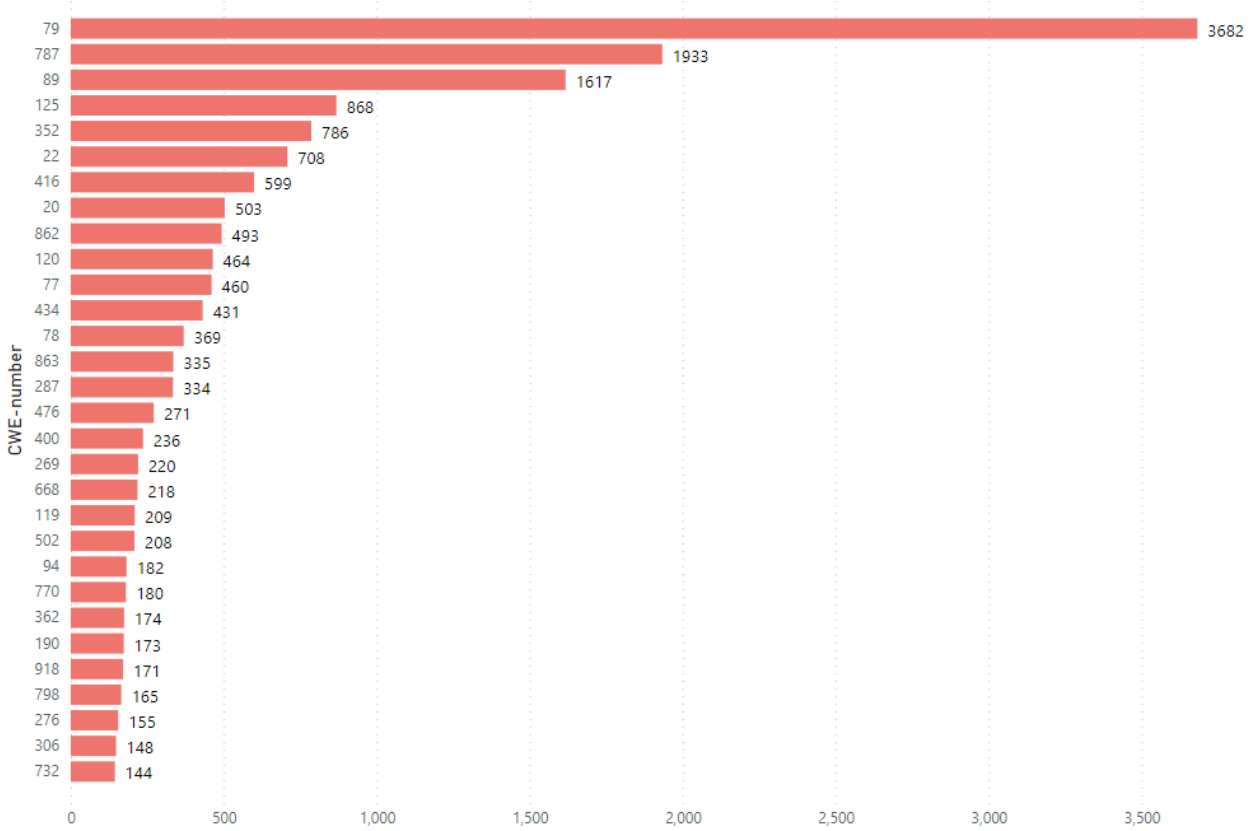


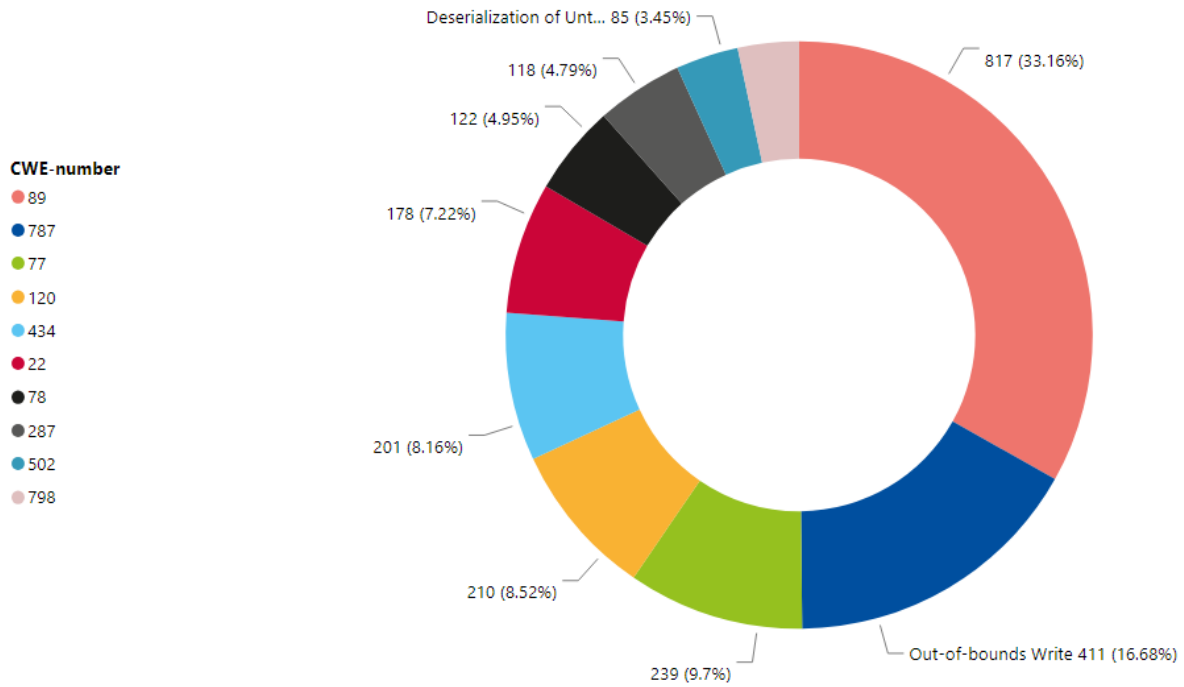
Table 2: Description of top 25 CWEs, their average CVSSv3 baseScore and Number of CISA KEV

Rank	CWE-number	No of occurrences CWE-number	CWE-description	Average of cvssV3 baseScore	KEV
1	79	3682	Improper Neutralisation of Input During Web Page Generation ('Cross-site Scripting')	5,618,007	2
2	787	1,933	Out-of-bounds Write	7,812,157	2
3	89	1,617	Improper Neutralisation of Special Elements used in an SQL Command ('SQL Injection')	871,713	2
4	125	868	Out-of-bounds Read	6,451,959	2
5	352	786	Cross-Site Request Forgery (CSRF)	7,039,822	1
6	22	708	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	7,493,079	2
7	416	599	Use After Free	7,813,356	2
8	20	503	Improper Input Validation	6,970,378	2
9	862	493	Missing Authorisation	6,055,172	1
10	120	464	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	8,419,828	2
11	77	460	Improper Neutralisation of Special Elements used in a Command ('Command Injection')	8,941,087	2

12	434	431	Unrestricted Upload of File with Dangerous Type	8,687,239	2
13	78	369	Improper Neutralisation of Special Elements used in an OS Command ('OS Command Injection')	8,563,686	2
14	863	335	Incorrect Authorisation	6,970,746	2
15	287	334	Improper Authentication	7,941617	2
16	476	271	NULL Pointer Dereference	6,414,391	1
17	400	236	Uncontrolled Resource Consumption	6,685,169	1
18	269	220	Improper Privilege Management	7,791,818	2
19	668	218	Exposure of Resource to Wrong Sphere	5,920,642	1
20	119	209	Improper Restriction of Operations within the Bounds of a Memory Buffer	7,137,321	1
21	502	208	Deserialisation of Untrusted Data	8,727,053	2
22	94	182	Improper Control of Generation of Code (‘Code Injection’)	8,558,242	2
23	770	180	Allocation of Resources Without Limits or Throttling	6,800,556	1
24	362	174	Concurrent Execution using Shared Resource with Improper Synchronisation ('Race Condition')	6,475,287	1
25	190	173	Integer Overflow or Wraparound	7,697,688	2

The figure below (figure 17) shows the top 10 weaknesses (CWEs) that are responsible for a large chunk of critical severity vulnerabilities. In this instance, the data was appropriately filtered to focus on the "critical" severity parameter.

Figure 17: Number and percentage of top 10 CWEs by critical severity CVEs (% percentage of total)



According to the National Vulnerability Database (NVD), vulnerabilities that carry the "CRITICAL" base severity tag are those with a Common Vulnerability Scoring System version 3 (CVSSv3) score falling in the range of 9.0 to 10.0. These are the most severe vulnerabilities, indicating that they possess a high potential for exploitation and pose significant risks to systems and data.

It is noticeable that many of these weaknesses are particular to web related vulnerabilities. These types of vulnerabilities tend to be prime targets for attackers, who often exploit them to gain unauthorized access etc. Web-related vulnerabilities include flaws that affect web applications, websites, and the infrastructure that underpins the internet.

To mitigate the risks posed by these critical vulnerabilities, organizations should strongly consider investing in secure software development practices and adopting relevant strategies. Secure by design and default principles play a pivotal role in this context. These principles emphasize building software with security in mind from the very beginning and configuring systems in a secure manner by default. By incorporating secure development practices, organizations can proactively reduce the likelihood of critical vulnerabilities surfacing in their software or systems.

Recent efforts have been made by a consortium of international organizations to advocate for and propose good practices in secure software development.[306].

Table 3: Descriptions of the 20 weaknesses responsible for most of the CRITICAL severity vulnerabilities

CWE-number	CWE-description	Count of CWE-number
89	Improper Neutralisation of Special Elements used in an SQL Command ('SQL Injection')	817
787	Out-of-bounds Write	411
77	Improper Neutralisation of Special Elements used in a Command ('Command Injection')	239
120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	210
434	Unrestricted Upload of File with Dangerous Type	201
22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	178
78	Improper Neutralisation of Special Elements used in an OS Command ('OS Command Injection')	122
287	Improper Authentication	118
502	Deserialisation of Untrusted Data	85
798	Use of Hard-coded Credentials	83
306	Missing Authentication for Critical Function	70
79	Improper Neutralisation of Input During Web Page Generation ('Cross-site Scripting')	56
94	Improper Control of Generation of Code ('Code Injection')	56
125	Out-of-bounds Read	49
863	Incorrect Authorisation	49
918	Server-Side Request Forgery (SSRF)	43
190	Integer Overflow or Wraparound	36
20	Improper Input Validation	34
611	Improper Restriction of XML External Entity Reference	33

3.4 ANALYSIS OF KNOWN EXPLOITED VULNERABILITIES (KEV).

The CISA KEV catalogue[307] is a dynamic catalogue of known exploited vulnerabilities that is updated with new vulnerabilities on a regular basis (the attackers never stop hence the list is constantly increasing). It is recommended that the catalogue of KEVs be used as a basis for any organisation's vulnerability management plans because those vulnerabilities have been observed in the wild by CISA to have been exploited or are under active exploitation.

[306] https://www.cisa.gov/resources-tools/resources/secure-by-design-and-default
[307] Known Exploited Vulnerabilities Catalog | CISA.

In the time-frame of this year's ETL there were 76 vulnerabilities that were published in the KEV list, however currently the entire CISA KEV contains a total of 992 vulnerabilities.

The table below highlights the CWEs which account for the 76 vulnerabilities from the KEV list, with rather similar findings as in the previous tables.

Table 4: CWEs responsible for KEVs

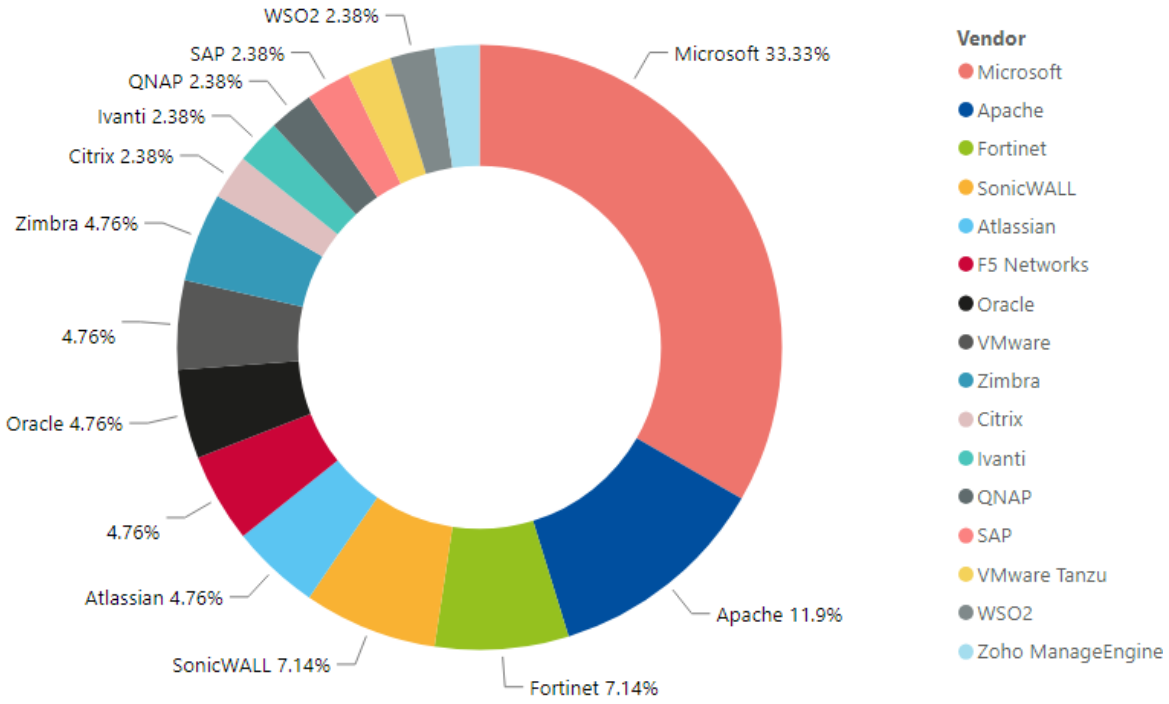
CWE-number	CWE-desc	Count of CWE-number
787	Out-of-bounds Write	10
843	Access of Resource Using Incompatible Type ('Type Confusion')	9
416	Use After Free	7
77	Improper Neutralisation of Special Elements used in a Command ('Command Injection')	5
78	Improper Neutralisation of Special Elements used in an OS Command ('OS Command Injection')	5
20	Improper Input Validation	4
502	Deserialisation of Untrusted Data	3
863	Incorrect Authorisation	3
94	Improper Control of Generation of Code ('Code Injection')	3
120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	2
190	Integer Overflow or Wraparound	2
22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	2
269	Improper Privilege Management	2
284	Improper Access Control	2
287	Improper Authentication	2
74	Improper Neutralisation of Special Elements in Output Used by a Downstream Component ('Injection')	2
79	Improper Neutralisation of Input During Web Page Generation ('Cross-site Scripting')	2
125	Out-of-bounds Read	1
200	Exposure of Sensitive Information to an Unauthorised Actor	1
294	Authentication Bypass by Capture-replay	1
295	Improper Certificate Validation	1
306	Missing Authentication for Critical Function	1
401	Missing Release of Memory after Effective Lifetime	1
434	Unrestricted Upload of File with Dangerous Type	1
532	Insertion of Sensitive Information into Log File	1
610	Externally Controlled Reference to a Resource in Another Sphere	1
798	Use of Hard-coded Credentials	1
89	Improper Neutralisation of Special Elements used in an SQL Command ('SQL Injection')	1

Approximately one-quarter of the entries in the CISA Catalogue pertain to incidents and threat actors associated with ransomware, while an additional quarter is linked to APT (Advanced Persistent Threat) actors. [308]

[308] Source: CISA Launches Known Exploited Vulnerabilities (KEV) Catalog - Securin

Another notable deliverable for the current year is the informative report titled "2022 Top Routinely Exploited Vulnerabilities, "[309] jointly published by CISA in collaboration with the 5 Eyes partners, which include the United Kingdom, Australia, Canada, New Zealand, and the United States.

Figure 18: 2022 Top routinely exploited vulnerabilities by Vendors

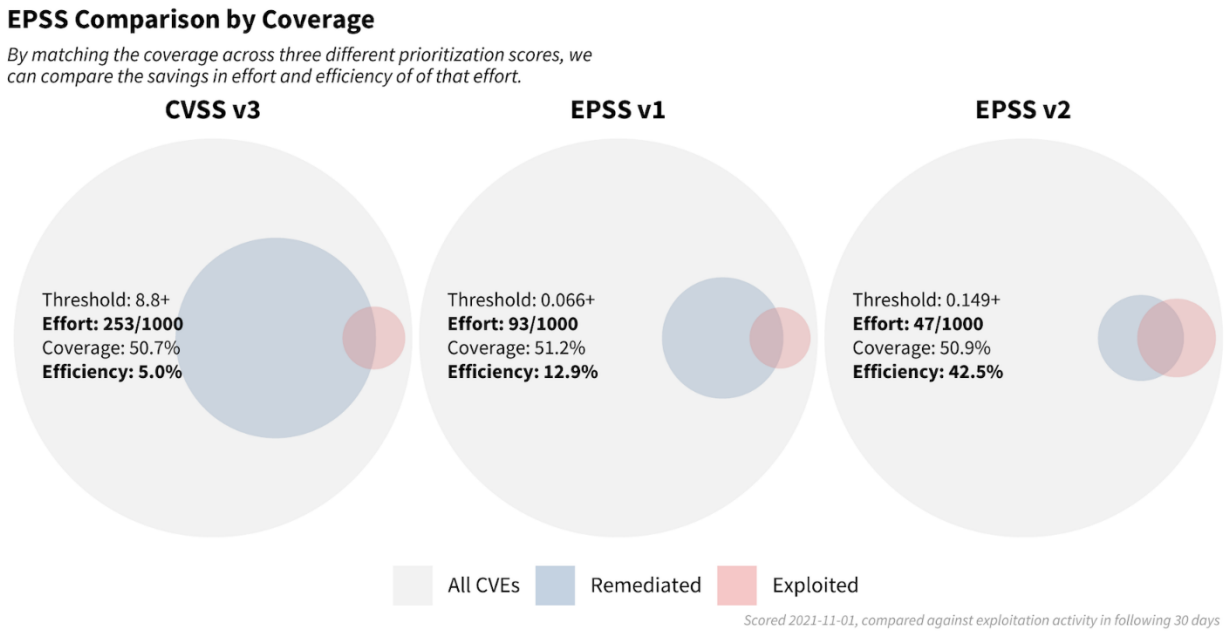


In the ETL report from the previous year, we introduced the Exploit Prediction Scoring System (EPSS), which underwent a significant update at the beginning of 2023. The EPSS score is designed to enhance organizations' ability to prioritize system patching effectively. It quantifies the likelihood of a vulnerability being exploited within the

[309] 2022 Top Routinely Exploited Vulnerabilities | CISA

next 30 days. It's important to note that the EPSS score is a momentary snapshot and can evolve over time as vulnerabilities progress.

Figure 19 : Epss Comparison by coverage[310]



As part of our analysis, we also considered the correlations between monthly EPSS values for the reported KEV vulnerabilities. As expected, due to the update of the underlying algorithm[311] there is a big upward movement in scores for many of the KEVs.

3.5 BACKGROUND

In conducting the analysis of the CVE (Common Vulnerabilities and Exposures) landscape, several crucial data sources were used into to ensure a comprehensive and well-informed analysis. These data sources played a pivotal role in shedding light on the state of vulnerabilities and security threats. Here are the primary sources used:

1. NIST NVD (National Vulnerability Database):
The NVD, maintained by the National Institute of Standards and Technology (NIST), stands as one of the foremost repositories for information regarding known vulnerabilities. It provides a comprehensive listing of vulnerabilities across a wide spectrum of software and hardware products. The database is continually updated to reflect the latest discoveries and assessments of vulnerabilities. You can explore the full listing here: NVD Full Listing.

2. CISA Known Exploited Vulnerability Catalogue (KEV):
The CISA (Cybersecurity and Infrastructure Security Agency) Known Exploited Vulnerability Catalogue is a valuable resource that catalogues vulnerabilities that are actively exploited by malicious actors. The catalog provides insights into vulnerabilities that are currently targeted and exploited in the cybersecurity landscape. A snapshot of this catalogue, as of August 12, 2022, was used to identify vulnerabilities that are actively leveraged in attacks. Further details on the KEV catalogue can be accessed here: CISA KEV Catalog.

3. FIRST Exploit Prediction Scoring System (EPSS):
The FIRST (Forum of Incident Response and Security Teams) Exploit Prediction Scoring System, also known as EPSS, is an important tool for predicting the likelihood of a vulnerability being exploited. It offers a scoring system that assesses the potential risk associated with vulnerabilities. EPSS provides valuable data and statistics related to

[310] https://www.first.org/epss/model
[311] https://arxiv.org/abs/2302.14172.

vulnerability predictions and exploits. To delve deeper into the details of EPSS, you can refer to these resources: EPSS Details and EPSS Data and Stats.

By drawing insights from these sources, the analysis of the CVE landscape benefited from a well-rounded perspective on vulnerabilities, their severity, and their potential exploitation. This multifaceted approach allows for a more comprehensive understanding of the evolving cybersecurity threats and vulnerabilities that impact the digital landscape.

4. RANSOMWARE

In ENISA's most recent report on the Threat Landscape for Ransomware Attacks[312], **ransomware** was defined as: *a type of attack where threat actors take control of a target's assets and demand a ransom in exchange for the return of the assets' availability.* This work covers the three key elements present in every ransomware attack:

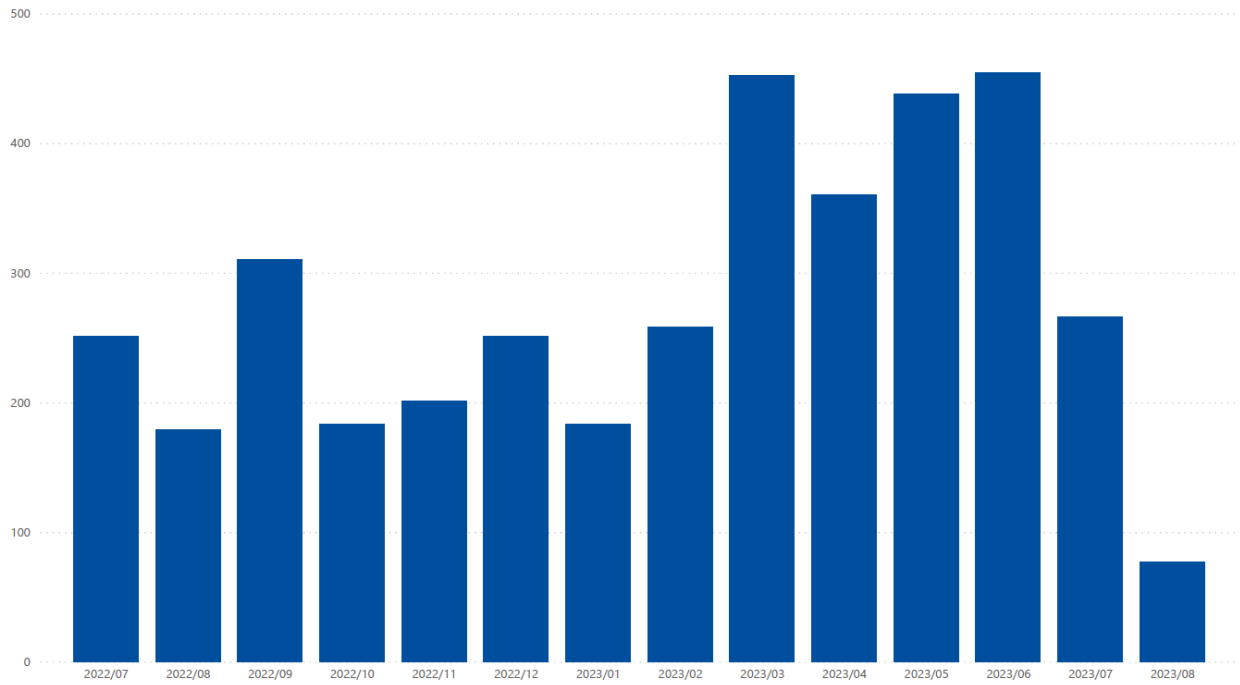
- assets
- actions
- blackmail.

This action-agnostic definition was needed to cover the changing ransomware threat landscape, the prevalence of multiple extortion techniques and the various goals other than solely financial gains. This report also covers the four high-level actions (lock, encrypt, delete and steal) used by ransomware to impact the availability, confidentiality and integrity of the assets. It can serve as a reference to better understand this threat.

By contrast, the definition of ransomware in NIST describes ransomware as: *a type of malicious attack where attackers encrypt an organisation's data and demand payment to restore access. In some instances, attackers may also steal an organisation's information and demand additional payment in return for not disclosing the information to authorities, competitors or the public*[313].

Once again, throughout the reporting period a substantial increase in ransomware-related incidents was witnessed, thus reaffirming the ongoing growth of the ransomware threat. Notably, the number of ransomware incidents has seen a noticeable surge, particularly since March 2023 (figure 20). It is worth mentioning that the incidents under analysis predominantly centred on European Union (EU) countries.

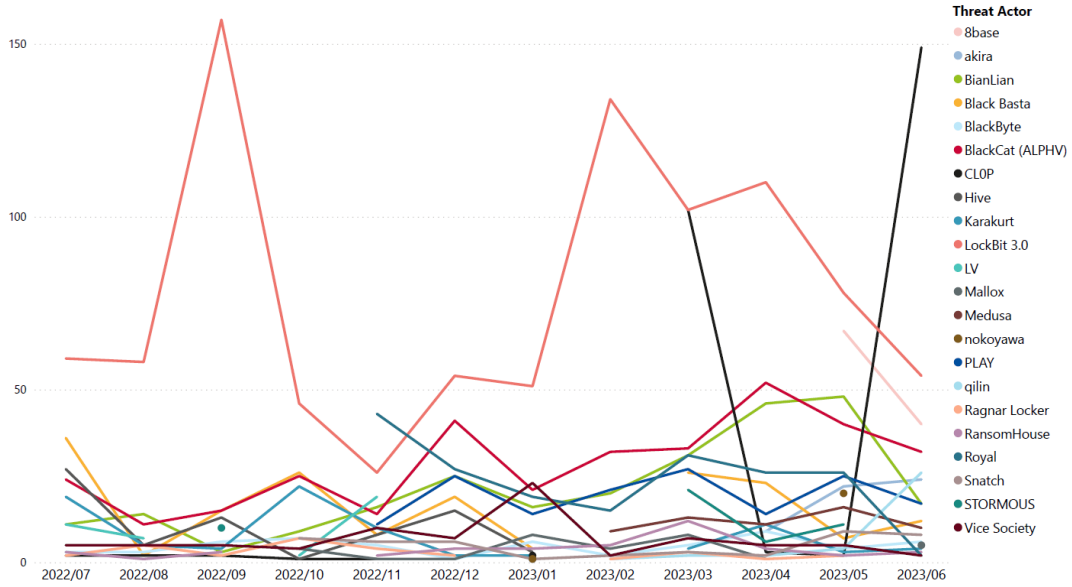
Figure 20: Time series of major incidents observed by ENISA (July 2022-June 2023)



[312] https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks.
[313] https://csrc.nist.gov/CSRC/media/Publications/nistir/draft/documents/NIST.IR.8374-preliminary-draft.pdf.

In Figure 21, the timeline illustrates the activity of the most active ransomware groups as seen through their leak sites and the victims posted there. Notably, Lockbit maintained consistent activity throughout the entire period. However, the Cl0p group's increased activity, particularly during the latter half of the period, specifically in H1 2023, will be discussed in greater detail below

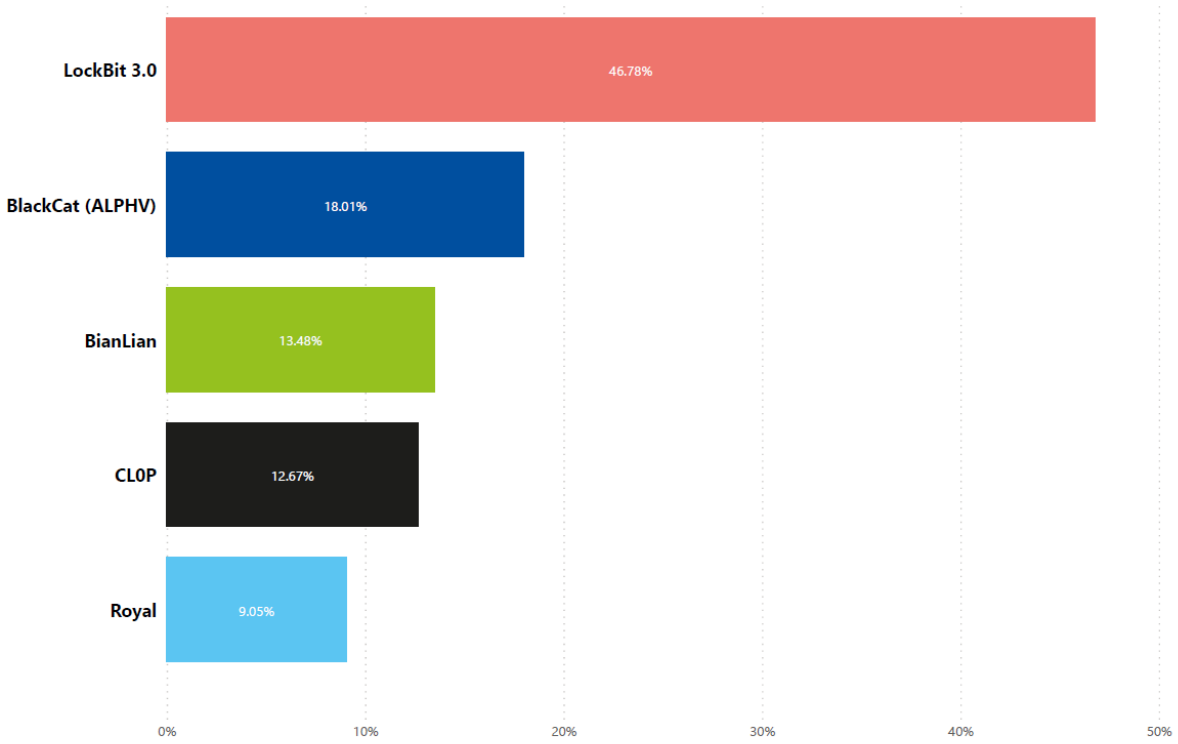
Figure 21: Timeline of the 20 most active Ransomware groups during the reporting period



4.1 LOCKBIT, ALPHV, AND BIAN LIAN STAND OUT AS THE TOP PERFORMERS, WHILE IN THE EU, PLAY GROUP JOINS THE RANKS OF LEADING THREAT ACTORS

LockBit, ALPHV (BlackCat) and Bian Lian were some of the top ransomware strains used in RaaS (Ransomware as a Service) and extortion attacks in terms of victim organisations, dominating the Global landscape during the reporting period (figure 22). Lockbit accounted for nearly half the number of incidents that were collected.

Figure 22: Five Most active Ransomware groups on the Global Landscape



The sectors that are most frequently targeted by the top three ransomware groups encompass a wide range of industries, with particular emphasis on the Industrial and Manufacturing sector, which appears to have been the most frequently victimised during this reporting period. The reason the industrial and manufacturing sector stands out as the primary target for these top-tier ransomware groups could be because of its particular appeal to cybercriminals due to its heavy reliance on automation, supply chain operations and critical infrastructure. Disrupting manufacturing processes or seizing control of industrial systems can result in significant financial losses and operational downtime, making it an attractive target.

In the global landscape of ransomware incidents, it is evident that the United States emerges as the primary hotspot for cyberattacks, hosting a sizeable portion of the victims targeted by Lockbit. During the reporting period, nearly half of all recorded ransomware incidents worldwide were concentrated in the United States The country's diverse range of industries, critical infrastructure and large corporations make it an attractive destination for cybercriminals seeking substantial ransoms.

Figures 23, 24 and 25 present a breakdown of three ransomware groups. It is evident that, on a global scale and in terms of targeted sectors, Lockbit and BlackCat primarily focus on similar sectors in the majority of incidents. On the other hand, Bian Lian also exhibits a significant concentration of attacks on healthcare organisations. When

considering the regional aspect, the majority of victims in all cases originate from the USA, followed by various other European countries.

Figure 23: Lockbit break down by sectors and countries

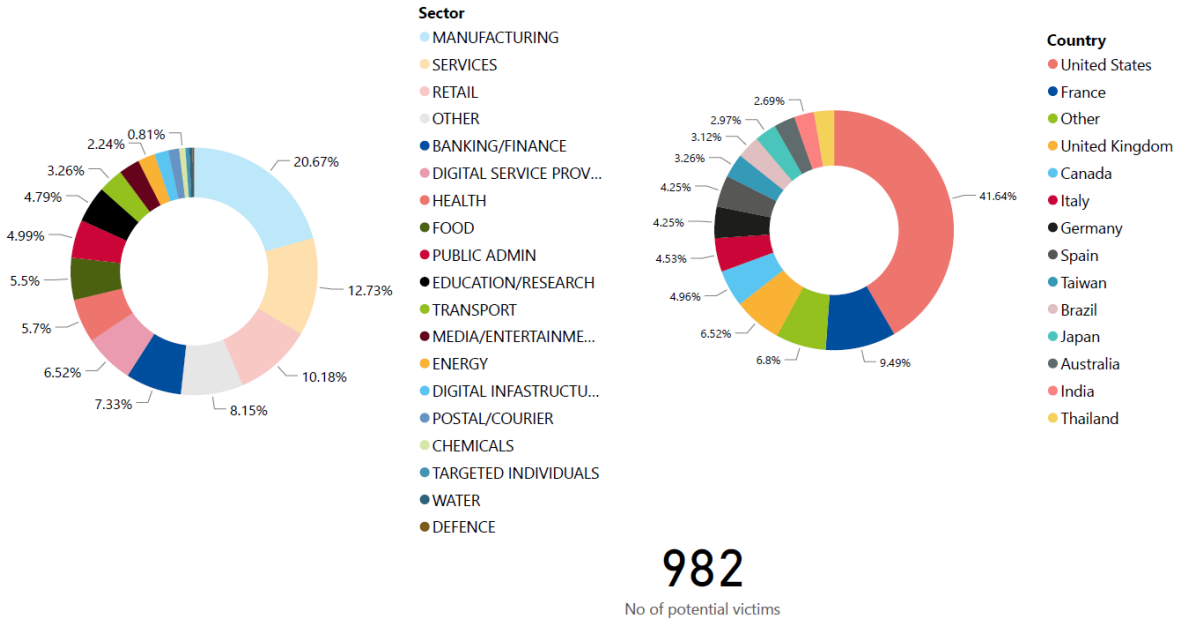


Figure 24: Blackcat /ALPHV break down on sectors and countries

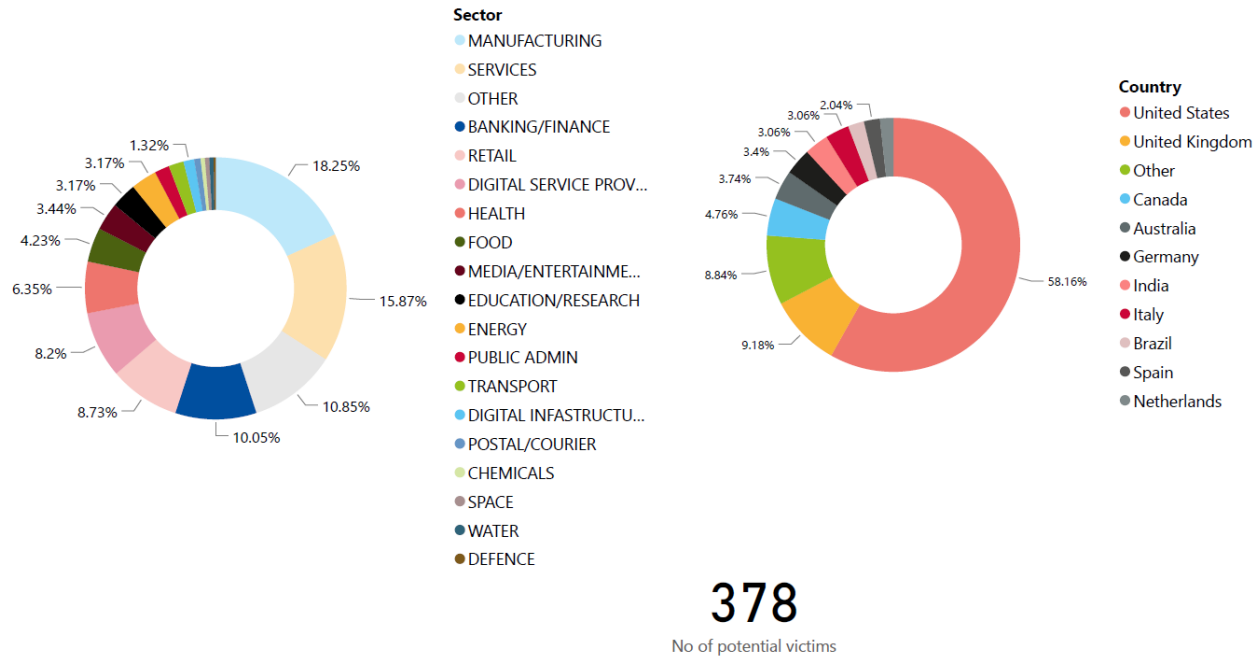
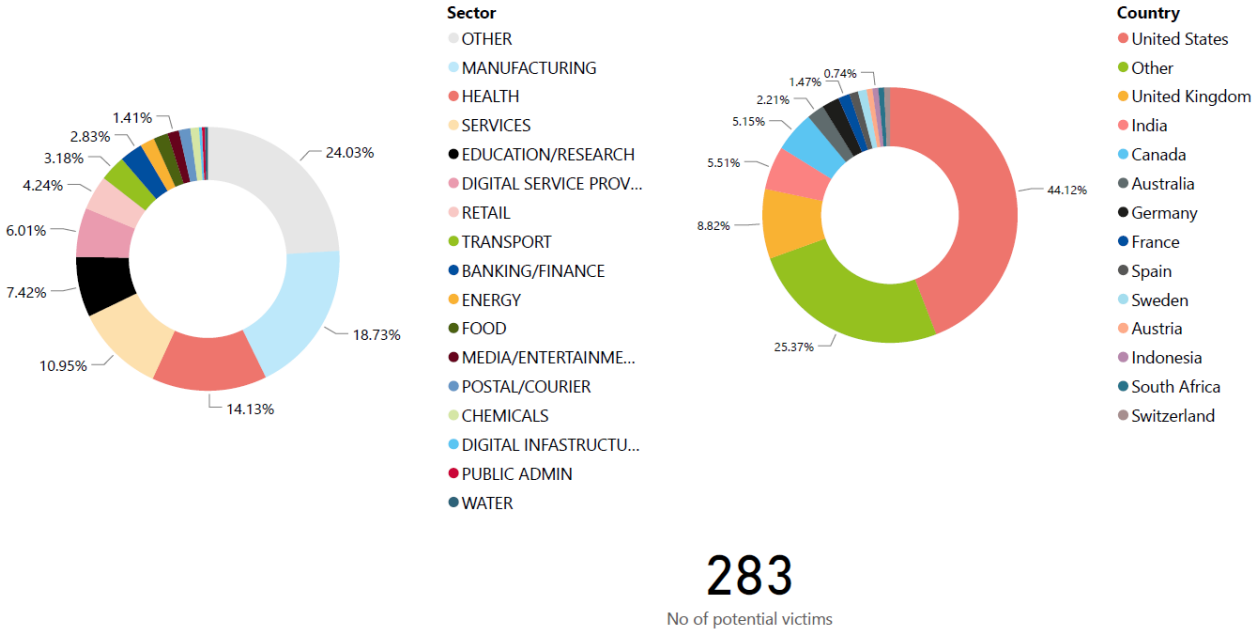
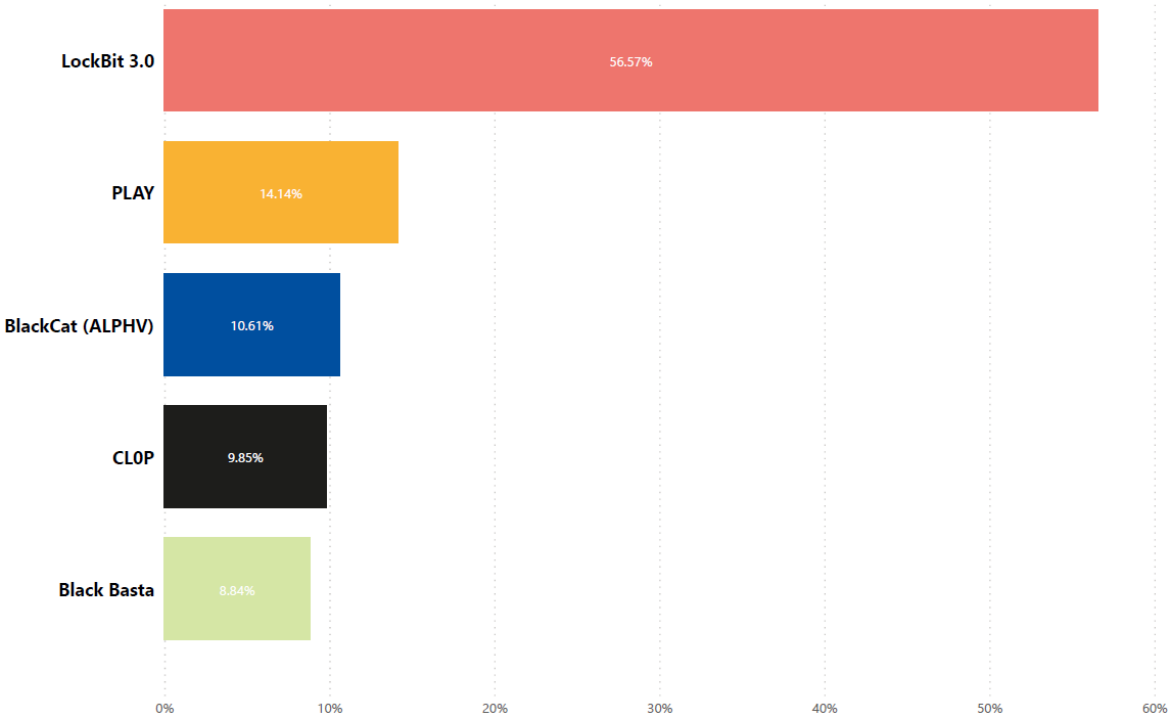


Figure 25: Bian Lian break down on sectors and countries



In the context of the European landscape, it is notable that the Lockbit ransomware has also emerged as a prominent ransomware as a service group, being responsible for more than half of the recorded ransomware incidents during the reporting period (figure 26). This can be caused also due to the leakage of the builder code which can lead to new actors using Lockbit. Furthermore, two other ransomware groups, PLAY and BlackCat, have also played significant roles in this cybersecurity landscape, contributing to the complexity and diversity of ransomware attacks across Europe.

Figure 26: Five Most active Ransomware groups on the European Landscape



In Figures 27, 28 and 29, we can observe a detailed analysis of three distinct ransomware groups. Notably, the most targeted sector varies across all three groups, indicating a diverse range of targets within each group's operations. However, this contrasts with the global perspective, where Lockbit and Blackcat have displayed a heightened focus on the manufacturing sector, while the PLAY group has directed its attention towards digital service providers.

Figure 27: Lockbit break down on countries and sectors EU

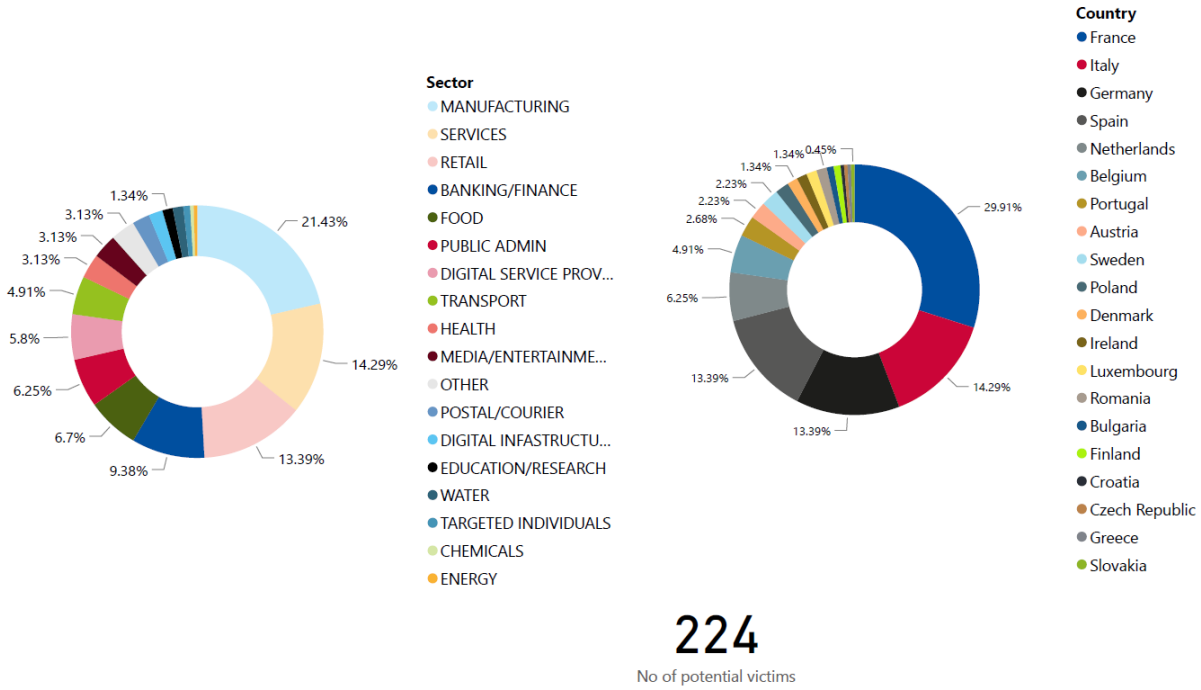


Figure 28: PLAY group break down on sectors and countries EU

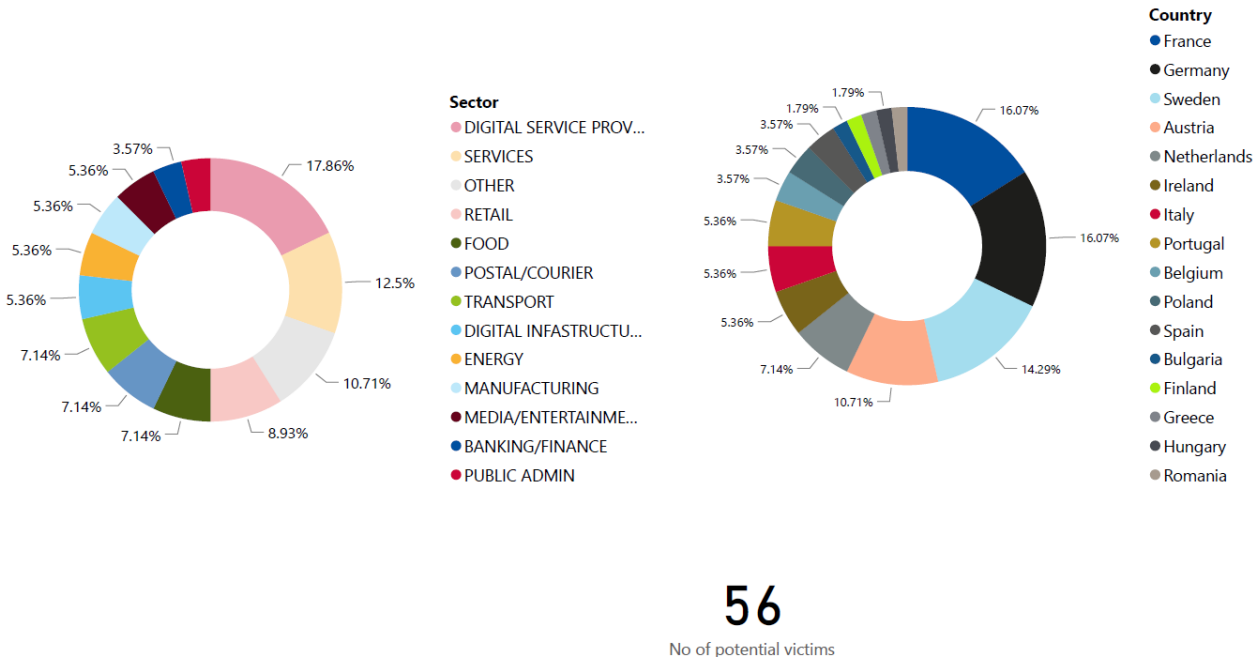
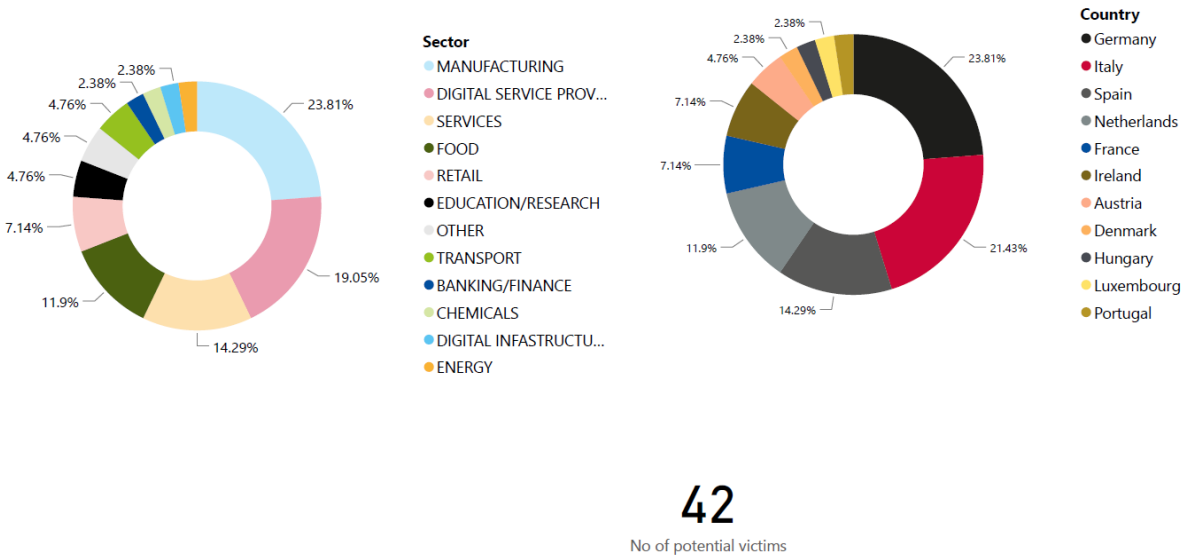


Figure 29: Blackcat /ALPHV break down on sectors and countries EU



The information presented here has been derived by merging data collected from the leak sites associated with various extortion groups and supplementing it with Open-Source Intelligence (OSINT). This comprehensive approach allows for a more thorough understanding of the matter, as it draws upon both the insights gleaned from these leak sites and publicly available information from diverse sources. This fusion of data sources provides a more holistic and accurate perspective on the ransomware threat, enriching the overall analysis and conclusions drawn from it.

Different statistics from different Vendors also confirm LockBit and BlackCat as the two most active ransomware gangs in 2023[314] with Cl0p accounting for more than half of all ransomware incidents in first half of 2023 though[315].

4.2 RISE OF CL0P USE OF TWO 0-DAYS

In March 2023 (as seen in figure 22) Cl0p ransomware emerged as the dominant threat in the cybercriminal landscape, effectively dethroning the previous leader, LockBit. This seismic shift in the world of ransomware was primarily attributed to Cl0p's phenomenally successful GoAnywhere campaign. According to public reports, the group behind Cl0p managed to infiltrate and compromise a staggering 104 organisations during this period, and their ascent was fuelled by the exploitation of a critical zero-day vulnerability within the widely-used managed file transfer software, GoAnywhere MFT[316].

However, their audacious tactics did not stop there. On May 27th (as seen in figure 22), a significant shift occurred in Cl0p's modus operandi when they began exploiting another vulnerability, identified as CVE-2023-34362, within the file transfer service MOVEit Transfer. This timing was strategically chosen during the extended US Memorial Day holiday[317] [318], a period when many organisations have reduced staff and heightened vulnerabilities. It is worth noting that conducting cyberattacks around holidays has become a signature tactic for the Cl0p ransomware operation, as they have previously executed large-scale exploitation attacks during similar periods of reduced security staffing.

The bulk of these MOVEit Transfer breaches appear to have taken place between May 30 and May 31. As a result of this Memorial Day attack on vulnerable internet-facing MOVEit Transfer installations, the number of alleged victims affected by Cl0p's ransomware campaign had exceeded an alarming count of 420[319] by the conclusion of the reporting period.

[314] https://www.guidepointsecurity.com/wp-content/uploads/2023/04/GRIT_Ransomware_Report_Q1_2023.pdf.
[315] https://www.reliaquest.com/blog/ransomware-q2-2023-victim-count-hits-new-heights/ .
[316] https://www.malwarebytes.com/blog/threat-intelligence/2023/04/ransomware-review-april-2023.
[317] https://www.malwarebytes.com/blog/news/2023/06/cl0p-ransomware-gang-claims-first-victims-of-the-moveit-vulnerability.
[318] https://www.bleepingcomputer.com/news/security/clop-ransomware-claims-responsibility-for-moveit-extortion-attacks/.
[319] https://cybersecuritynews.com/moveit-hack-mass-hack/.

It is worth noting that in both cases these campaigns did not involve any ransomware attacks, no ransomware was deployed, even though Cl0p is considered a ransomware group. This was a case of data exfiltration and extortion rather a trend, as seen below, is increasing.

This series of high-impact attacks showcased Cl0p's evolving and advanced capabilities, underscoring the urgent need for organisations to bolster their cybersecurity measures and stay vigilant against emerging threats in the ever-changing landscape of cybercrime. The increased exploitation of two highly effective zero-day vulnerabilities has underscored the importance of responsible disclosure of vulnerabilities even further.

4.3 MONETISATION TOP MOTIVATION - RAAS GROUPS APOLOGING FOR INCIDENTS

On December 18th, the Hospital for Sick Children (SickKids) experienced a ransomware attack that had far-reaching consequences. This attack impacted various aspects of the hospital, including its internal and corporate systems, phone lines and website. In a surprising turn of events, LockBit, the ransomware group responsible for the attack, took a step by releasing a free decryption tool specifically for the Hospital for Sick Children. LockBit acknowledged that one of its members had violated their own rules by targeting this healthcare institution. Notably, LockBit's ransomware operation permits its affiliates to encrypt data from pharmaceutical companies, dentists and plastic surgeons. However, it explicitly prohibits attacks on 'medical institutions' due to the potential life-threatening consequences such actions could have[320].

Similarly, on 26 February 2023, the Olympia Community Unit School District 16, discovered that it had fallen victim to a ransomware attack. This attack was carried out by an affiliate associated with the notorious LockBit ransomware group. Subsequently, LockBit's dark web leak site initiated a countdown, announcing that on April 12, they would release all the data they had exfiltrated unless a ransom was paid. Once again, LockBit issued an apology and offered a free decryption tool for the affected school district. The ransomware operation's policy explicitly states that it forbids encrypting institutions where data loss could potentially lead to fatalities. This includes cardiology centres, neurosurgical departments, maternity hospitals and any facility where critical surgical procedures involving high-tech equipment and computers are performed[321].

These instances underscore the fact that, although financial gain remains the primary motive for attacks in most Ransomware-as-a-Service (RaaS) groups (as depicted in Figure 1), there are still certain constraints and regulations governing their choice of targets.

4.4 MARCH 2023 BROKE RANSOMWARE ATTACK RECORDS - RANSOMWARE CONTINUES TO BE ON THE RISE

In March 2023, the cybersecurity landscape experienced an unprecedented surge in ransomware attacks, establishing it as the most active month in recent years. A total of 459 ransomware attacks were documented during this period, demonstrating a remarkable 91% surge compared to the preceding month and a substantial 62% increase compared to March 2022.[322]

A report compiled by NCC Group[323] shed light on the primary reason behind this surge in ransomware attacks. It pointed to the exploitation of a specific vulnerability, identified as CVE-2023–0669, found within Fortra's GoAnywhere Managed File Transfer (MFT) software. This vulnerability had become a focal point for cybercriminals, providing them with an entry point to orchestrate their attacks, ultimately leading to the significant uptick in ransomware incidents during this particular month.

4.5 INCREASED OPERATIONS BY LAW ENFORCEMENT

In January 2023, the actions taken by the US Justice Department through their meticulously planned and executed months-long disruption campaign culminated in the seizure of the Hive ransomware group's IT infrastructure.

[320] https://www.bitdefender.com/blog/hotforsecurity/ashamed-lockbit-ransomware-gang-apologises-to-hacked-school-offers-free-decryption-tool/.
[321] Ransomware gang apologises, gives SickKids hospital free decryptor (bleepingcomputer.com).
[322] https://www.nccgroup.com/media/l2anvmij/ncc-group-monthly-threat-pulse-march-2023-v20.pdf.
[323] https://www.nccgroup.com/media/l2anvmij/ncc-group-monthly-threat-pulse-march-2023-v20.pdf.

Hive, while a prominent target, was not the sole entity to feel the heat of law enforcement's relentless pursuit[324]. The year 2022 had already witnessed high-profile operations aimed at crippling ransomware groups. In February of 2023, the United States and the United Kingdom took a decisive step by imposing sanctions on Trickbot operatives, disrupting one of the most pernicious and far-reaching cybercriminal networks.

During March, the law enforcement community scored another win with the apprehension of two members of the prolific DoppelPaymer ransomware group. During April, the hacker marketplace Genesis Market was subjected to a disruption operation, effectively curbing illicit cyber activities. In May, the Federal Bureau of Investigation (FBI) delivered a resounding blow to the ransomware ecosystem by seizing control of nine cryptocurrency exchanges known to be conduits for laundering ransom payments. This audacious move not only deprived cybercriminals of a critical means to cash in on their ill-gotten gains but also demonstrated the government's unwavering commitment to upholding the rule of law in the digital realm[325].

4.6 NEW TECHIQUES EMERGING

4.6.1 Franken Ransomware - code being repurposed

A noteworthy shift in the ransomware landscape has been observed from RaaS (Ransomware as a Service) towards independent actors. This intriguing development has given rise to a new phenomenon that has been coined as 'Franken-ransomware'. This term aptly describes a trend wherein malicious actors are piecing together new ransomware variants using fragments of stolen or leaked code from various sources[326]. The ESXiArgs malware being used to target VMware systems starting in February was one such example, borrowing a 'ransom note from one ransomware, the encryption scheme from another ransomware' (potential Babuk).

Other emerging actors who have adopted this strategy include Rapture, which seems to have incorporated the leaked source code of the Paradise crypto-locker from 2021. GazProm, named after the Russian gas giant and known for its ransom notes featuring ASCII art of Russia's president, has used the leaked Conti source code. Additionally, newcomers such as the RA Group, Rorschach and RTM Locker have all integrated source code from the Babuk ransomware, which became available in September 2021[327].

4.6.2 URL delivered Ransomware dominates attack vectors

Threat actors have adopted increasingly dynamic tactics for disseminating ransomware. Alongside the conventional use of polymorphic ransomware variants, they frequently alter hostnames, paths, filenames or a combination of these elements to broadly propagate ransomware. Historically, email attachments, such as those using SMTP and POP3 protocols, were the predominant means for distributing ransomware. However, recent findings from Palo Alto's Unit 42, who analysed ransomware samples throughout the whole of 2022, indicate a notable shift in the primary entry point for ransomware infections. URL links and web browsing have emerged as the dominant methods for delivering ransomware, accounting for more than 77% of cases[328].

4.7 FEWER VICTIMS PAID IN 2022 BUT NOT THE CASE FOR 2023 - SHIFTING FROM ENCRYPTION TO DATA EXTORTION

In the latter part of 2022 (Q3 and Q4), it was evident that generating profits through crypto-locking attacks had become increasingly difficult as the global community strengthened its defences against ransomware[329]. According to findings from blockchain intelligence firm Chainalysis, available data showed a significant decline in ransomware earnings. Throughout 2022, the total revenue generated from ransomware dropped substantially, reaching a minimum of $456.8 million. This marked a substantial decrease of 40.3% compared to the $765.6 million reported in 2021. This decline was primarily attributed to victims' growing reluctance to pay ransomware perpetrators, rather than a reduction in the number of ransomware incidents[330].

[324] https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant.
[325] https://www.sonicwall.com/medialibrary/en/white-paper/mid-year-2023-cyber-threat-report.pdf.
[326] https://www.recordedfuture.com/ransomware-changing-why-threat-intelligence-essential.
[327] https://www.bankinfosecurity.com/blogs/new-entrants-to-ransomware-unleash-frankenstein-malware-p-3459.
[328] https://unit42.paloaltonetworks.com/url-delivered-ransomware/.
[329] https://www.bankinfosecurity.com/blogs/ransomware-profits-dip-as-fewer-victims-pay-extortion-p-3358.
[330] https://www.chainalysis.com/blog/crypto-ransomware-revenue-down-as-victims-refuse-to-pay/.

Nonetheless, the scenario shifted during the initial two quarters of 2023 (Q1 and Q2). Information from this time-frame indicates that ransomware operations are poised to exceed previous benchmarks, witnessing a rise in both substantial and minor ransom payments. Remarkably, ransomware perpetrators are heading for their second-most profitable year in history, having coerced a minimum of $449.1 million by the end of June[331] as Chainanalysis reports.

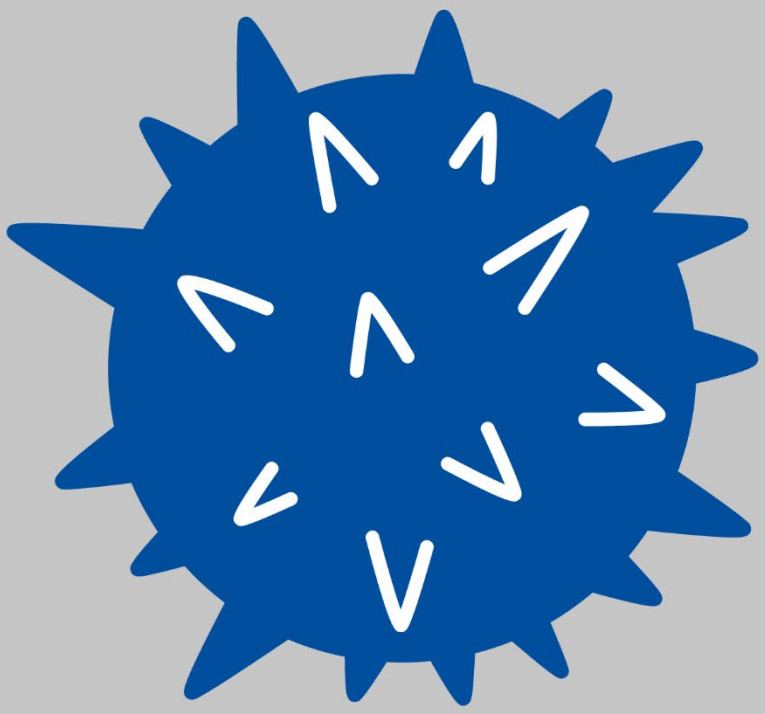
Alongside the surge in ransomware incidents throughout 2023, the escalation in cases of data theft extortion when compared to previous quarters aligns with publicly reported trends indicating a growing number of ransomware groups are pilfering data and coercing victims without encrypting their files or resorting to the deployment of traditional ransomware. Although data theft extortion is not a new phenomenon, the number of incidents this quarter suggests that financially motivated threat actors are increasingly seeing this as a viable means of receiving a good payout[332][333].

Data extortion presents multiple advantages for ransomware groups when compared to encryption-based attacks. These advantages possibly include a lower risk of detection and the ability to generate profits without employing encryption. Additionally, data extortion enables cybercriminals to more efficiently target organisations with sensitive information. Critical infrastructure entities like hospitals and schools are more likely to pay ransoms to avoid data breaches, given the sensitivity and potential harm associated with their data. This targeted approach further encourages the adoption of data extortion as a primary method for ransomware attacks[334].

Examples of this shift can be seen in the activities of groups such as RansomHouse and Karakurt extortion groups. Some ransomware groups, including Bian Lian and Clop, have reportedly moved away from using encryption and are now favouring data theft extortion in their recent attacks, according to public reports[335].

.

[331] https://www.bleepingcomputer.com/news/security/ransomware-payments-on-record-breaking-trajectory-for-2023/.
[332] https://blog.talosintelligence.com/talos-ir-q2-2023-quarterly-recap/.
[333] Palo Alto Unit42 ransomware extortion report https://start.paloaltonetworks.com/2023-unit42-ransomware-extortion-report
[334] https://www.conquer-your-risk.com/2023/04/20/the-evolution-of-ransomware-from-encryption-to-data-extortion/.
[335] https://blog.talosintelligence.com/talos-ir-q2-2023-quarterly-recap/.



5. MALWARE

Malware, also referred to as malicious code and malicious logic, is an overarching term used to describe any software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity or availability of a system[336]. Examples of malicious code include viruses, worms, trojan horses or other code-based entities that infect a host[337]. Malicious actors develop malware or acquire it through **Malware-as-a-Service** to carry out digital attack campaigns and support their operations, gaining and retaining control over assets, evading defences and conducting post-compromise actions[338].

Depending on the goal of the threat actor, malware functionality can range from getting control over **systems** and **networks** (e.g.botnets), over **data** (e.g. information stealing), to making them **unavailable altogether** (DoS). Information stealers, including AgentTesla, FormBook and RedLine, were found to be a top malware threat in this year's report.

While classic mobile malware (e.g banking trojan) has witnessed a decline, adware remains a prevalent threat to mobile devices. However, the use of commercial spyware has been increasing, driven by advanced zero-click exploits that enable surveillance without user interaction. Notable incidents include the Pegasus Project, which exposed the widespread abuse of spyware by the NSO Group.

Pre-installed systems on Chinese Android smartphones have raised concerns due to dangerous privileges granted to vendor and third-party applications. Data leakage and tracking risks pose a threat to users' privacy and security, even beyond China's borders. Criminal enterprises have also infected millions of devices worldwide, turning them into mobile proxies for fraudulent activities and generating illicit revenue[339].

The use of disruptive wipers, particularly by Russian APT groups such as Sandworm, has intensified, impacting critical infrastructure. Distinguishing between nation-state APT activities and hacktivist groups has become increasingly challenging.

Finally, law enforcement agencies have conducted successful operations against ransomware gangs, spyware networks and criminal enterprises involved in cybercrime. Covert operations and international collaborations have resulted in the takedown of ransomware infrastructure, sanctions against cybercriminals and the dismantling of marketplaces selling stolen credentials. These actions highlight the importance of collaborative efforts to combat malware threats.

In this reporting period, we have noted a significant uptick in incidents related to malware, as depicted in Figure 30. We can also discern a more detailed breakdown of these threats based on sectors and regions. It is notable that, despite a decrease in 2022, as previously highlighted in the ETL 2022 report, the beginning of 2023 has witnessed a resurgence in incidents involving this particular type of threat type.

[336] https://csrc.nist.gov/glossary/term/malware.
[337] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.
[338] https://attack.mitre.org/techniques/T1587/001/.
[339] https://arstechnica.com/information-technology/2021/09/security-audit-raises-severe-warnings-on-chinese-smartphone-models/

Figure 30: Time series of major incidents observed by ENISA (July 2022-June 2023)

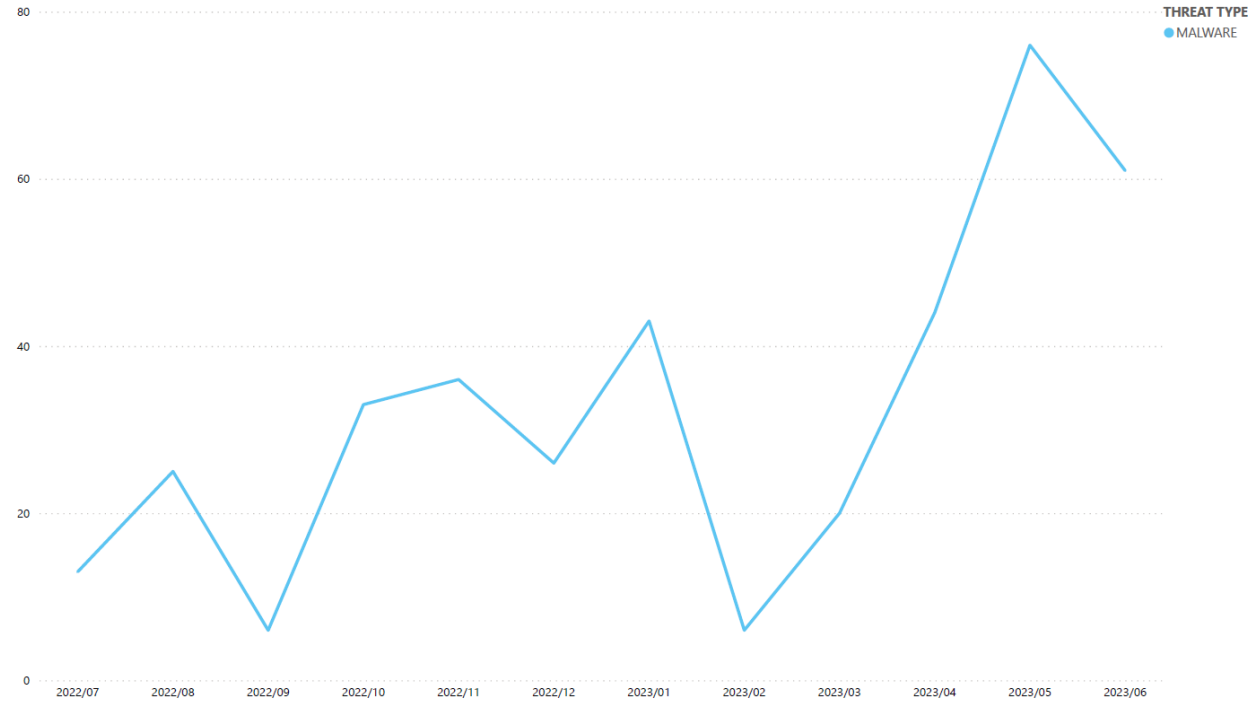
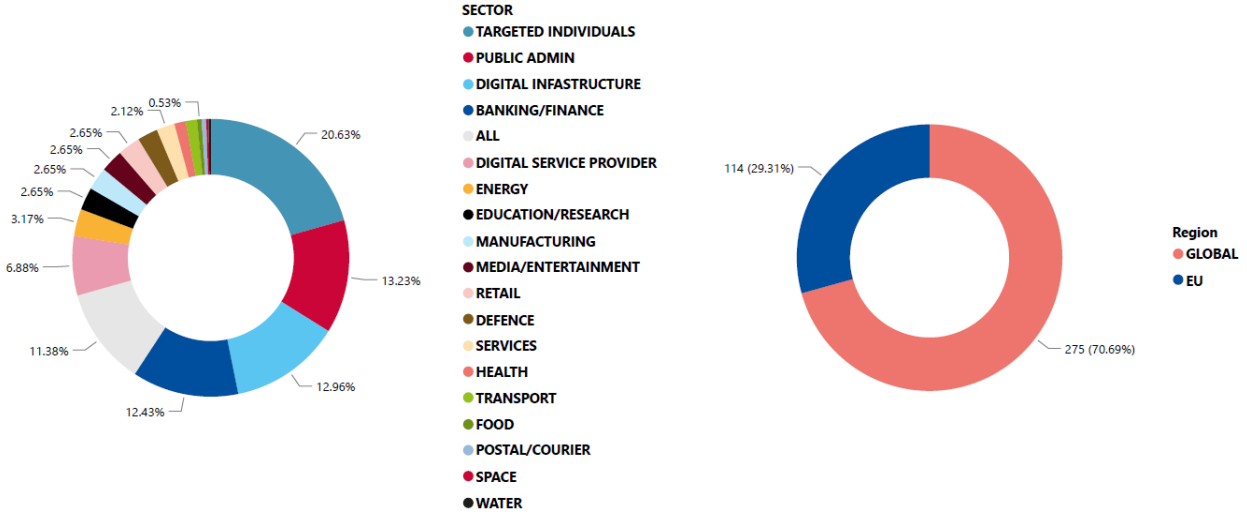


Figure 31: Breakdown of Sectors by threat type and region



5.1 INFORMATION STEALERS REMAIN ONE OF THE TOP MALWARE THREATS

One of the biggest malware threats is still information stealers. According to information from multiple sources, the most common information stealers[340] [341] throughout 2022 and 2023 were:

[340] Avast Q1/2023 Threat Report, https://decoded.avast.io/threatresearch/avast-q1-2023-threat-report/.
[341] Sophos-2023 threat report, https://www.sophos.com/en-us/content/security-threat-report.

- AgentTesla
- FormBook
- RedLine

Overall, we see many similarities between the most common malware strains.

5.1.1 Agent Tesla

Agent Tesla is a Remote Access Trojan (RAT) written in .NET that has been around since 2014[342]. Initial access brokers (IAB) often use it to exploit corporate networks. This access is then resold to affiliated threat actors, as part of a Malware-as-a-Service (MaaS) business model. Agent Tesla is a first-stage malware and is leveraged to push more specific and specialised second-stage malware. The malware is predominantly distributed as e-mail attachments during phishing attacks.

5.1.2 RedLine Stealer

RedLine Stealer is a Remote Access Trojan (RAT); more specifically it is an information stealer malware written in .NET and distributed in a Malware-as-a-Service (MaaS) model. It is available for around $100 to $150 and on a subscription basis ($100 a month). The malware has been around since 2020[343]. This low cost seems to be one of the drivers for the popularity of this malware strain.

Typical features are information extraction from browsers (cached/saved credentials, autocomplete data and credit card information). At the beginning of 2023, the malware was found to be distributed through Microsoft OneNote[344].

5.1.3 RedLine Stealer FormBook

FormBook malware (also known as xLoader) has characteristics that are very similar to the previous two malware strains but is known for its form-grabbing techniques to extract data directly from website HTML forms, steal data from keystrokes, browser autofill features and copy-and-paste clipboards. It is also very cheap which drives its adoption.

It is important to remember that these lists are constantly changing as cybercriminals come up with new malware strains and product releases, and that there are many other types of information stealers beyond those mentioned here. However, the Malware-as-a-Service (MaaS) model seems to be shifting to a subscription-based business.

[342] https://attack.mitre.org/software/S0331/.
[343] https://malpedia.caad.fkie.fraunhofer.de/details/win.redline_stealer.
[344] https://www.rapid7.com/blog/post/2023/01/31/rapid7-observes-use-of-microsoft-onenote-to-spread-redline-infostealer-malware/.

5.2 EVOLUTION OF MALWARE DELIVERY MECHANISMS

Last year, we reported how Microsoft announced it would begin blocking XL4 and VBA macros by default for Microsoft Office users in October 2021 and February 2022, respectively[345]. Microsoft macros had long been an easy way for threat actors to distribute malware globally. This change has forced even the most skilled actors to shift their tactics and brought forth a monumental shift in activity and threat behaviour over the last year.

Research from May 2023 details how threat actors are continuously testing various tactics to determine the most effective methods for gaining initial access via email. Based on the available telemetry, no consistent and reliable technique has been adopted by the entire threat landscape. Furthermore, many threat actors tend to copy each other's tactics. If one threat actor or a group uses a new technique, other threat actors may start using the same technique in the following weeks or months. Certain actors have enough time and resources to create, refine and experiment with various methods for delivering malware that are more advanced[346].

Take, for example, QBot malware, which is leveraged by numerous threat actors and is popular among Ransomware-as-a-Service (RaaS) operators; we have seen the distribution model change over time. In May 2023, it was distributed through ZIP files containing an executable DLL file to abuse a DLL hijacking flaw in Windows 10 WordPad. Other examples of distribution methods include PDFs and Windows Script Files (WSF) to infect Windows hosts[347].

Threat actors are also increasingly using container files such as ISO and RAR, and Windows Shortcut (LNK) files in campaigns to distribute malware. These filetypes can have the capability to circumvent Microsoft's macro blocking protections (e.g. Mark Of The Web or MOTW) and can be used to distribute malicious executables that can lead to follow-on malware, data reconnaissance and theft, and ransomware[348].

5.3 LOLBIN AND COBALT STRIKE

A LOLBin (Living Off the Land Binary) attack is a technique used to exploit legitimate, built-in binaries or tools to execute malicious activities while evading detection. It allows attackers to blend in with normal system processes, making it challenging for traditional security solutions to identify and block their activities.

The most notable LOLBIN attack tools detected include Mimikatz, Apteryx (Mimikatz version), Powersploit suite, SrpSuite. Although not a LOLBin in the sense of the word, Cobalt Strike is frequently used during attacks and is therefore a common presence in such instances. Cobalt Strike is a widely used commercial penetration testing and red teaming tool. It gained popularity among malicious actors due to its feature set, including advanced social engineering, post-exploitation and command-and-control capabilities.

According to a Sophos report, Cobalt Strike was involved in almost half of the customer incidents handled in the first three quarters of 2022[349]. Most of the incidents involved ransomware or activities that could lead to a ransomware attack, such as the use of tools and methods typically associated with it.

Fortra, the creator of Cobalt Strike, has teamed up with Microsoft to fight against servers that host pirated versions of Cobalt Strike. In March 2023, the Eastern District of New York's US District Court issued a court order allowing both the seizure of the domain names and the take down of the IP addresses of servers that host this software[350] [351].

5.4 MOBILE SPYWARE

The use of commercial spyware is increasing, as more individuals and groups are using advanced zero-click exploit tools to conduct surveillance on a wider range of targets without any interaction being required. Numerous incidents were discovered worldwide including in Europe.

[345] https://learn.microsoft.com/en-us/deployoffice/security/internet-macros-blocked.
[346] https://www.proofpoint.com/sites/default/files/misc/pfpt-us-threat-research-2023-05-12-cybercrime-experimentation.pdf.
[347] https://twitter.com/Cryptolaemus1/status/1643277974823661573.
[348] https://www.proofpoint.com/us/blog/threat-insight/how-threat-actors-are-adapting-post-macro-world.
[349] Sophos-2023 threat report, https://www.sophos.com/en-us/content/security-threat-report.
[350] https://noticeofpleadings.com/crackedcobaltstrike/files/ComplaintAndSummons/1%20-Microsoft%20Cobalt%20Strike%20-%20Complaint(907040021.9).pdf.
[351] https://noticeofpleadings.com/crackedcobaltstrike/files/CourtOrders/2023-04-03%20Order_23-cv-2447_Microsoft%20Corporation%20et%20al%20v.%20John%20Does%201-2%20et%20al(907079167.1).pdf.

Back in 2021, the European Parliament launched an investigation after the Pegasus Project, a collective of journalists, NGOs and researchers, revealed a list of 50,000 persons that had been targeted with the spyware from the NSO group. This report was published in November 2022[352].

In May of 2022, five Android zero-day vulnerabilities were discovered. According to Google research, these vulnerabilities were chained and exploited by Predator spyware[353]. A recent Talos analysis in May 2023 on the Alien loader revealed that it not only functions as a loader but also establishes low-level capabilities for Predator to monitor its victims[354].

In March of 2023, the US government issued an Executive Order prohibiting the use of commercial spyware that may pose a threat to national security or that has been used by foreign actors to facilitate human rights violations[355].

The Israeli company QuaDream reportedly targeted journalists, opposition figures and advocacy organisations in at least 10 countries[356]. In April 2023, it was shut down due to the Israeli regulator's decision to decrease the number of countries to which it was permitted to export[357]. This came after two Israeli companies, Candiro and the NSO Group were added to a blacklist by the US Chamber of Commerce for their involvement in malicious cyber activities[358].

5.5 THE HIDDEN THREAT OF PRE-INSTALLED MALWARE

Research dating to February 2023 detailed how preinstalled systems, with vendor- and third-party applications, on Chinese Android smartphones are granted dangerous privileges. Data such as geolocation, profile data and social relationships are transmitted without consent or even notification. This poses deanonymisation and tracking risks that extend outside China when the user leaves the country[359].

In May 2023, a BlackHat presentation was given on the operations of a criminal enterprise (Lemon Group) that have infected millions of Android devices, mainly mobile phones but also smart watches, smart TVs and more. When infected, these devices become mobile proxies that can be used for SMS fraud and generating revenue through advertisements and click fraud. The research telemetry data confirms millions of infected devices globally (the group claimed a reach of 8.9 million devices) with the main clusters in South-East Asia and Eastern Europe[360]. Further analysis by TrendMicro on the malware, named Guerilla, identified over 50 different images from a variety of vendors carrying initial malware loaders. The malware spread and it is estimated that the threat actor spread this malware over the last five years[361].

A lot of these devices are widely available through the European supply chain and to properly address these issues is very challenging[362].

5.6 THE ESCALATION OF DESTRUCTIVE MALWARE

The use of disruptive wipers by Russian APT groups, especially Sandworm, against Ukrainian organisations is not new. In 2022, there was, according to ESET, a significant increase in the use of wipers, which have undergone advances in both their deployment and impact[363].

[352] https://www.europarl.europa.eu/doceo/document/PEGA-AM-740916_EN.pdf.
[353] https://blog.google/threat-analysis-group/protecting-android-users-from-0-day-attacks/.
[354] https://blog.talosintelligence.com/mercenary-intellexa-predator/.
[355] https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security/.
[356] https://citizenlab.ca/2023/04/spyware-vendor-quadream-exploits-victims-customers/.
[357] https://www.jpost.com/breaking-news/article-739390.
[358] https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list.
[359] https://arxiv.org/abs/2302.01890.
[360] https://www.blackhat.com/asia-23/briefings/schedule/index.html#behind-the-scenes-how-criminal-enterprises-pre-infect-millions-of-mobile-devices-31235.
[361] https://www.trendmicro.com/en_us/research/23/e/lemon-group-cybercriminal-businesses-built-on-preinfected-devices.html.
[362] https://www.eff.org/deeplinks/2023/05/android-tv-boxes-sold-amazon-come-pre-loaded-malware.
[363] ESET Threat Report T3 2022, https://www.eset.com/int/about/newsroom/press-releases/research/eset-threat-report-t3-2022-when-war-meets-cyberspace-the-impact-of-russias-invasion-on-digital-threa/.

Some actors in this area are willing to engage in actions that could potentially have a global political impact. As a result, distinguishing between nation-state APT activity and hacktivist groups has become increasingly more difficult[364].

Adversaries such as FANCY BEAR, EMBER BEAR, VOODOO BEAR, PRIMITIVE BEAR and GOSSAMER BEAR were particularly active against Ukraine in 2022[365] according to Crowdstrike.

In June 2023, Microsoft linked a previously identified wiper named Cadet Blizzard (Microsoft has shifted to a taxonomy for naming threat actors aligned around the theme of weather) to the Russian GRU. Starting in February 2023, a series of attacks were launched against government agencies and IT service providers in Ukraine. In addition, the report identifies Cadet Blizzard as the source of the destructive WhisperGate wiper attacks against Ukraine that occurred in January 2022, before Russia's invasion[366].

5.7 EVOLUTION OF MALWARE THREATS IN OT

In 2022, following the invasion of Ukraine, Industroyer2 was discovered targeting energy substations. This is a variant of Industroyer malware that was used by the Sandworm APT group to cut power in Ukraine in 2016[367]. Another malware strain detected was INCONTROLLER (aka PIPEDREAM) that was built to manipulate and disrupt industrial processes[368].

In June 2022, a report published information on more than 56 vulnerabilities affecting operational technology (OT) equipment used in various critical infrastructure environments[369].

In May 2023, novel malware targeting OT and ICS was discovered and tracked as COSMICENERGY. The purpose of this malware was to disrupt electric power through interactions with devices, such as remote terminal units (RTUs), used in electric transmission and distribution operations in Europe[370].

Further code analysis of the malware and its components showed it lacks maturity, contains errors and is far from having a full-fledged attack capability like Industroyer2 or CRASHOVERRIDE. It was concluded that COSMICENERGY is not an immediate threat and that is likely part of a training exercise or for use in detection development[371]. However, these incidents show that industrial protocols are susceptible to attacks and served as a wake-up call for the critical infrastructure sector, emphasising the need for continuous vigilance and proactive measures to safeguard operational technology and industrial control systems.

5.8 IMPACT OF LAW ENFORCEMENT ACTIONS

In July 2022, the FBI, along with Europol and 13 other law enforcement agencies, conducted a covert operation to infiltrate the infrastructure of the Hive ransomware gang. Finally, in January 2023, after intensive activity monitoring, the payment and leak sites were taken down[372] [373].

In February 2023, seven Russian cybercriminals linked to the ransomware group behind Trickbot malware, as well as Conti and RYUK, were sanctioned. This operation was led by the UK NCA and the US Department of the Treasury's Office of Foreign Assets Control[374].

Also, around February 2023, Spanish Police and the European Cybercrime Centre (EC3) at Europol, through operation Ransom, dismantled a cybercrime network dedicated to spreading police ransomware, which blocks

[364] Checkpoint 2023 Cyber Security Report, https://pages.checkpoint.com/cyber-security-report-2023.html.
[365] CrowdStrike2023 Global Threat Report, https://www.crowdstrike.com/global-threat-report/.
[366] https://blogs.microsoft.com/on-the-issues/2023/06/14/russian-cyberattacks-ukraine-cadet-blizzard/.
[367] https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/.
[368] https://www.mandiant.com/resources/blog/incontroller-state-sponsored-ics-tool.
[369] https://www.forescout.com/resources/ot-icefall-report/.
[370] https://www.mandiant.com/resources/blog/cosmicenergy-ot-malware-russian-response.
[371] https://hub.dragos.com/hubfs/116-Whitepapers/Dragos_SB_COSMICENERGY_June23_FINAL_WEB.pdf.
[372] https://www.europol.europa.eu/media-press/newsroom/news/cybercriminals-stung-hive-infrastructure-shut-down.
[373] https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant.
[374] https://www.nationalcrimeagency.gov.uk/news/ransomware-criminals-sanctioned-in-joint-uk-us-crackdown-on-international-cyber-crime.

computers, accusing the victims of having visited illegal websites containing child abuse material or file sharing and demanding payment of a fine[375].

In March of 2023, Europol reported that they had apprehended two individuals who were considered core members of the ransomware group known as DoppelPaymer. During an operation coordinated by Europol, the German and Ukrainian police conducted raids and confiscated devices, receiving assistance from law enforcement in Denmark and the US[376].

In April 2023, the FBI and Dutch National Police led an international law enforcement operation involving 17 countries. This resulted in the takedown of Genesis Market, a well-known marketplace that sold stolen account credentials. The service was closed and its infrastructure taken over. Additionally, a total of 119 people were arrested[377].

In May 2023, the US Department of Justice announced how, through Operation MEDUSA and in coordination with multiple international governments, a global peer-to-peer network used by Russian malware was dismantled. The FBI developed a tool called Perseus, designed to issue commands that would make the Snake malware overwrite its own key components. This malware referred to as Snake or Turla had been used for almost two decades by the Russian government to conduct cyber-espionage on the US, NATO and its allies[378].

The battle against malware threat actors has had varying degrees of success, but effective collaboration on an international level has resulted in successful high-profile operations. This underscores the significance of cooperation among law enforcement in order to have a substantial impact.

[375] https://www.europol.europa.eu/media-press/newsroom/news/police-dismantle-prolific-ransomware-cybercriminal-network.
[376] https://www.europol.europa.eu/media-press/newsroom/news/germany-and-ukraine-hit-two-high-value-ransomware-targets
[377] https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-notorious-hacker-marketplace-selling-your-identity-to-criminals.
[378] https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-snake-malware-network-controlled.

6. SOCIAL ENGINEERING

Social engineering encompasses a broad range of activities that attempt to exploit a human error or human behaviour with the objective of gaining access to information or services[379]. It uses various forms of manipulation to trick victims into making mistakes or to hand over sensitive or secret information. Users may be lured to open documents, files or e-mails, to visit websites or to grant access to systems or services. Although the lures and tricks used may abuse technology, they rely on a human element to be successful. This threat canvas consists mainly of the following attack vectors: phishing, spear-phishing, whaling, smishing, vishing, watering hole attack, baiting, pretexting, quid pro quo, honeytraps and scareware. While social engineering techniques are often used to gain initial access, they may be used at later stages of an incident or breach. The examples are business e-mail compromise (BEC), fraud, impersonation, counterfeit and lately extortion.

Phishing aims at stealing important information such as credit card numbers and passwords through e-mails involving social engineering and deception. **Spear-phishing** is a more sophisticated version of phishing that targets specific organisations or individuals. **Whaling** is a spear-phishing attack aimed at users in high positions (executives, politicians etc.). **Smishing**, a term derived as a combination of 'SMS' and 'phishing', occurs when the attacker gathers sensitive information or convinces the victims to click on the malicious links that are shared with the use of SMS messages. Another related threat is **vishing**, a combination of phishing and voice that occurs when information is given via phone, where malicious actors are using social engineering techniques to extract sensitive information from users. A **watering hole attack** occurs when hackers infect a site that they know the target victims regularly visit.

There are different approaches to convincing a victim of a social engineering attack to provide sensitive information or perform a specific action demanded by an attacker[380]. **Baiting** is a type of social engineering attack in which scammers lure victims into providing sensitive information by promising them something valuable in return (e.g. free games, music or movie downloads). **Pretexting** occurs when someone creates a fake persona or misuses their actual role; this happens most often with data breaches from the inside. **Quid Pro Quo** attacks occur when scammers pretend to be from an IT department or other technical service provider. **Honeytraps** are a type of social engineering in which scammers create fake online dating and social media profiles using attractive stolen photos. **Scareware** frightens victims into believing they are under imminent threat, e.g. you could receive a message saying that your device has been infected with a virus.

Business e-mail compromise (BEC) is a sophisticated scam targeting businesses and organisations, whereby criminals employ social engineering techniques. The attacker can deceive an employee or executive to initiate bank transfers under fraudulent conditions. The other BEC is to gain access to an employee's or executive's e-mail account to send emails containing malicious code company-wide (to clients, vendors etc.)[381].

Fraud[382] is the intentional misrepresentation or concealment of an important fact upon which the victim is meant to rely. **Impersonation** is when one entity illegitimately assumes the identity of another entity in order to benefit from it. **Counterfeit** is the fraudulent imitation of something.

In this chapter we include **extortion attacks**, where threat actors target networks with the specific purpose of exfiltrating sensitive data to hold for ransom or sell on the dark web without deploying any encryption malware, which is what originally gave ransomware its name.

During this reporting period, a noteworthy increase in social engineering incidents was observed towards the conclusion of H1 2023, as illustrated in Figure 32. Moreover, a more granular analysis of these threats taking into

[379] https://www.imperva.com/learn/application-security/social-engineering-attack/.
[380] https://www.aura.com/learn/types-of-social-engineering-attacks.
[381] https://www.fbi.gov/how-we-can-help-you/safety-resources/scams-and-safety/common-scams-and-crimes/business-email-compromise.
[382] https://www.britannica.com/dictionary/fraud.

account sectors and regions is available. One crucial takeaway is that social engineering campaigns, in various forms, persist as a substantial threat to users as evidenced in Figure 33.

Figure 32: Time series of major incidents observed by ENISA (July 2022-June 2023)

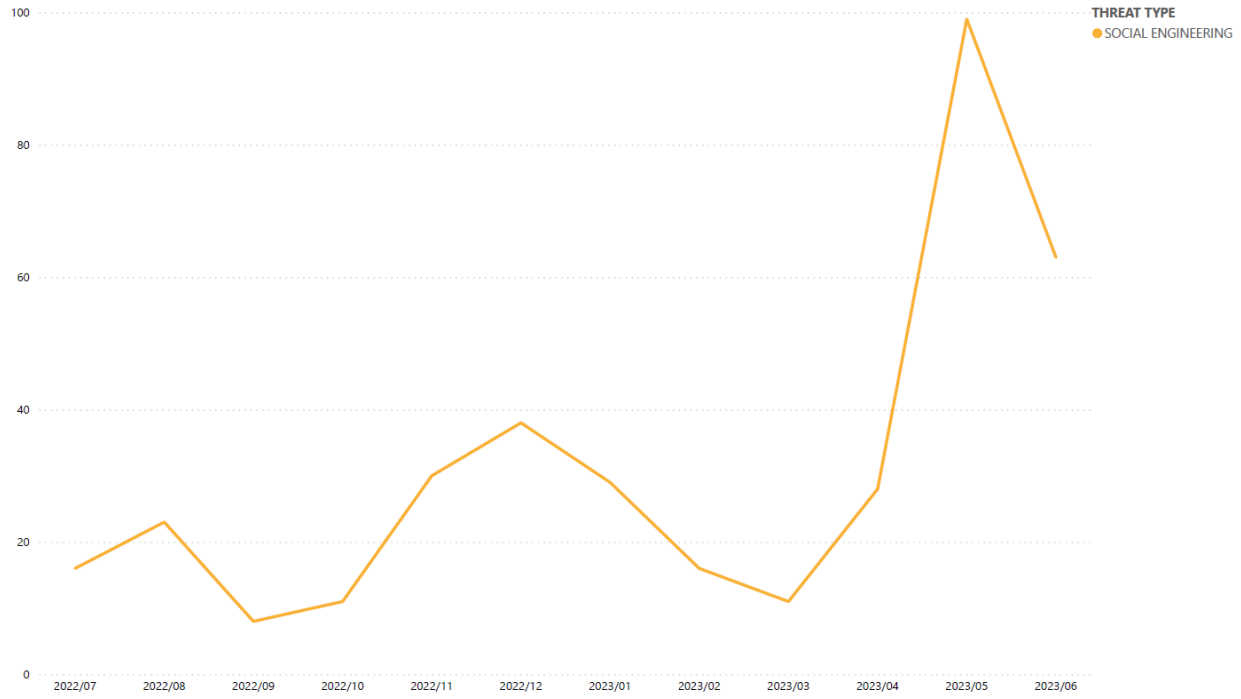
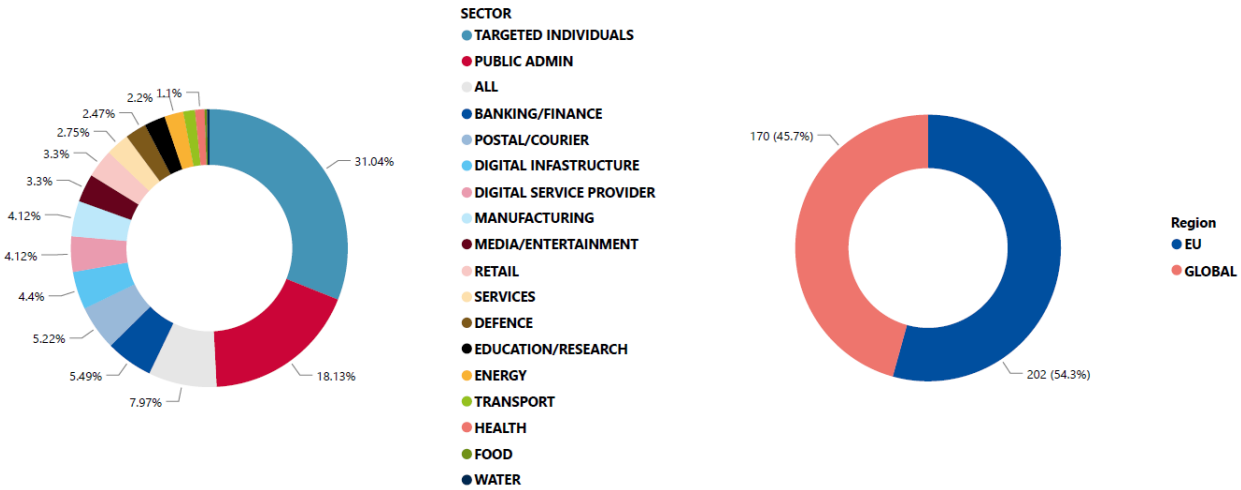


Figure 33: Break down of Sectors with threat type and region



Social engineering remains a preferred attack vector for threat actors due to its simplicity, low cost, ease of execution, and profitability according to reports by IBM and Verizon[383] [384]. Phishing in particular continues to be the most prevalent initial infection vector in the EMEA based on a Mandiant report[385]. Moreover, the emergence of Phishing-as-a-Service (PhaaS) has further amplified the reach of social engineering attacks. Trend Micro has observed[386] PhaaS

[383] https://www.ibm.com/reports/threat-intelligence.
[384] https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf.
[385] https://www.mandiant.com/m-trends.
[386] https://www.trendmicro.com/en_us/ciso/23/c/phishing-as-a-service-phaas.html.

offerings with prices as low as $15 per day, providing individuals with even minimal knowledge of cybersecurity the means to execute a complex phishing attack. The availability and affordability of such services contributes to the proliferation of social engineering attacks.

Phishing is the top digital crime type identified by the FBI[387] by far, followed by personal data breach, non-payment / non-delivery, extortion and tech support categories. Most of those cases directly use a form of social engineering. According to the same report, BEC complaints increased by 10% with adjusted losses of over $2.7 billion. Last year we observed increasing attacks targeting the web3 ecosystem, the expansion from targeting crypto exchanges and cryptocurrency owners. Today's attacks, as reported by Mandiant, spread to the whole web3 ecosystem, including non-fungible tokens (NFTs), cross-blockchain connection mechanisms and even online games.[388]

One of the main themes used for phishing was the war against Ukraine. We observed multiple global reaching campaigns. The campaigns had different topics, ranging from humanitarian assistance and various types of fundraising[389,390] up to gathering intelligence related to western military support to Ukraine[391]. One of the spear-phishing campaigns targeted EU diplomatic entities in early March 2023[392] [393]. European countries which were directly targeted by threat actors included Poland[394] and Lithuania[395].

Innovations in social engineering are mainly driven by artificial intelligence, especially considering the release of ChatGPT during this reporting period. We observed three novel areas: the use of AI for crafting more convincing phishing emails and messages that closely mimic legitimate sources, deepfakes used mainly for voice cloning and AI-driven data mining.

Changes in the modus operandi of threat actors were observed during the reporting period. Threat actors were employing novel approaches in order to overcome the increased use of multi-factor authentication: MFA fatigue attack[396], adversary in the middle (AitM)[397] and SIM swapping[398]. In response to the blocking of VBA macros for office files obtained from Internet in July 2022[399], threat actors turned to LNK, OneNote and ISO/ZIP files to infect victims[400]. We also observed the re-emergence of the distribution of infected USB keys[401], call-back phishing[402] and the use of QR codes (quishing)[403] [404], whereas combinations of the above and persistence was also observed.

Lastly, social engineering techniques were used to extort victims and included even more personal and intimidating approaches[405]. The attacker's inclination to specifically target individuals with personal threats and involve even their family members presents a progression in the scope of these attacks.

6.1 PHISHING AS THE INITIAL INFECTION VECTOR AND ON THE RISE

Phishing dominated most of the relevant threat reports published by cybersecurity organisations and communities. IBM X-Force identified phishing as an initial access vector in 41% of incidents[406], followed by exploitation of public-facing applications. Verizon DBIR reported 82% of breaches involved the human element[407], whether it is the use of stolen credentials, phishing, misuse or simply an error. ESET reported phishing as the only category to grow in the last four months in 2022[408] as the remaining cyber threats went down. The number of phishing websites blocked was

387 https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.
388 https://www.mandiant.com/m-trends.
389 https://blog.talosintelligence.com/talos-year-in-review-2022/.
390 https://www.sophos.com/en-us/content/security-threat-report.
391 https://www.crowdstrike.com/global-threat-report.
392 https://blogs.blackberry.com/en/2023/03/nobelium-targets-eu-governments-assisting-ukraine.
393 https://therecord.media/nobelium-apt29-cozy-bear-phishing-eu-ukraine.
394 https://cert.gov.ua/article/3761023.
395 https://www.tvnet.lv/7696931/ukrainu-begli-lietuva-sanem-viltus-e-pasta-vestules-uzbrukums-saistits-ar-krieviju.
396 https://blog.isc2.org/isc2_blog/2023/02/the-top-5-new-social-engineering-attacks-in-2023-.html.
397 https://attack.mitre.org/techniques/T1557/.
398 https://sennovate.com/the-future-of-social-engineering-emerging-trends-and-threats/.
399 https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/ba-p/3071805.
400 https://www.ibm.com/reports/threat-intelligence.
401 https://www.mandiant.com/m-trends.
402 https://socradar.io/a-new-rising-social-engineering-trend-callback-phishing/.
403 https://www.thelocal.com/20220902/french-postal-service-warns-of-new-qr-code-scam/.
404 https://sfstandard.com/criminal-justice/san-francisco-fake-parking-tickets-scam-what-you-need-to-know/.
405 https://www.crowdstrike.com/global-threat-report/.
406 https://www.ibm.com/reports/threat-intelligence.
407 https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf.
408 https://www.welivesecurity.com/wp-content/uploads/2023/02/eset_threat_report_t32022.pdf.

up by 80%. APWG observed 1 270 883 phishing attacks in Q3 2022[409] and 1 350 037 in Q4 2022[410], both being new record highs for a quarter for phishing observed by APWG.

We can also see that the distribution around the globe is not uniform. For example, phishing ended up in the second place as the initial access vector globally (even with 67% increase compared to previous period) according to Mandiant[411]. Mandiant determined exploits as the most leveraged initial infection vector (32%), followed by phishing (22%), stolen credentials (14%) and prior compromise (12%). The threat actors favoured exploits for initial compromise in the Americas but phishing completely dominated in the EMEA region with 40%. Verizon DBIR identified the same non-uniformity[412], where social engineering increased in the EMEA to almost 60% of breaches from the previous year's 20%.

We expect e-mail to remain as one of the top initial infection vectors as long as this approach delivers results. As confirmed by the reported data, it still does, and it will probably continue to do so over the long term, as it is cheap, easy to conduct and profitable. The main lures used to spread threats via email also stay very steady[413], with the majority posing as generic purchase orders, shipment notifications and bank payments. These are regularly supplemented by popular subjects getting broad attention in the current time, such as the COVID-19 pandemic, the war in Ukraine or the World Cup in 2022 in Qatar.

Finance, followed by social media and shipping, remained at the top of the most impersonated list[414] [415]. Social media-related phishing websites were dominated by Facebook look-alikes.

Apart from initial access vectors, phishing also dominates the ranks of cybercriminals. Phishing is the top digital crime type identified by the FBI[416] by far, followed by personal data breach, non-payment / non-delivery, extortion and the tech support categories.

6.2 WAR AGAINST UKRAINE USED AS THE LURE

A significant spike in spear-phishing activity targeting NATO countries was observed by the Google threat analysis group[417]. We observed multiple campaigns with global reach. Threat actors send email lures with themes related to the conflict, including humanitarian assistance and various types of fundraising[418] [419]. These emails are primarily used for scam activity but have also delivered a variety of threats. This pattern is consistent with what we typically see following global events or crises, such as the COVID-19 pandemic, when opportunistic cybercriminals attempt to exploit high public interest for their own gain. CrowdStrike reported on credential phishing operations targeting government research labs, military suppliers, coordination companies and non-governmental organisations (NGOs) from August 2022 onward[420]. This focused targeting likely indicates this adversary's ambitions to gather intelligence related to western military support to Ukraine, although the targeting of NGOs could also represent the preparation of information operations against organisations that may be involved in impending Russian war crime investigations. The campaign was attributed to Gossamer Bear, also known as Coldriver[421].

The CyberPeace Institute observed 20 phishing and spear-phishing campaigns during the reporting period[422]. Most of them were targeted on Ukraine but some were targeting European countries including Germany, Poland and Lithuania. Campaigns directly targeting Ukraine focused on both government entities and citizens. In June 2023, the threat actor targeted Ukrainian civilians with phishing SMS with the objective of gaining access to their Telegram accounts[423]. A second campaign targeted users of Ukrainian email services with the goal of obtaining credentials[424].

[409] https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf.
[410] https://docs.apwg.org/reports/apwg_trends_report_q4_2022.pdf.
[411] https://www.mandiant.com/m-trends.
[412] https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf.
[413] https://www.welivesecurity.com/wp-content/uploads/2023/02/eset_threat_report_t32022.pdf.
[414] https://www.welivesecurity.com/wp-content/uploads/2023/02/eset_threat_report_t32022.pdf.
[415] https://docs.apwg.org/reports/apwg_trends_report_q3_2022.pdf.
[416] https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.
[417] https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/.
[418] https://blog.talosintelligence.com/talos-year-in-review-2022/.
[419] https://www.sophos.com/en-us/content/security-threat-report.
[420] https://www.crowdstrike.com/global-threat-report.
[421] https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1243&context=scholcom.
[422] https://cyberconflicts.cyberpeaceinstitute.org/threats/attack-details.
[423] https://cert.gov.ua/article/4789582.
[424] https://cert.gov.ua/article/4928679.

During April 2023, CERT-UA recorded cases in which e-mails with the subject line 'Windows Update' were distributed among government bodies in Ukraine, apparently sent on behalf of system administrators of departments[425] [426]. Another case was a phishing campaign containing SmokeLoader malware[427]. In February 2023, there was a mass distribution of e-mails allegedly on behalf of the Pechersk District Court of the city of Kyiv[428] and on behalf of National Security and Defence Council[429], both with malicious attachments. At the end of 2022, the phishing campaigns were mimicking CERT-UA itself[430], targeting victims with the subject line 'Attention! Harmful software (CERT-UA)', again with a malicious executable. Several other phishing campaigns were conducted in July 2022; for additional information we refer the reader to the following references below: 431, 432, 433, 434 and 435.

We observed a spear-phishing campaign against EU diplomatic entities in early March 2023[436] [437]. The campaign targeted EU countries aiding Ukraine. The threat actor sent emails with information concerning the Polish Ambassador's visit to the USA and abused the legitimate electronic system for official document exchange in the EU called LegisWrite. These emails contained malware allowing the threat actor to drop files on the victim's machine and move throughout the victim's network. The campaign was attributed to APT29, also known as Cozy Bear, Nobelium or The Dukes.

CERT-UA in cooperation with Polish colleagues detected web pages mimicking the webpages of Ukrainian and Polish government entities[438]. The web pages offered a download of malware file for the 'detection of infected computers'. If the file was downloaded, it searched for interesting document types that were later exfiltrated. The attack was attributed to threat actor UAC-0114, also known as Winter Vivern.

6.3 THE POTENTIAL USE OF AI FOR SOCIAL ENGINEERING

Artificial intelligence generated massive public attention with the introduction of ChatGPT[439]. Due to its ability to mimic human interaction, it presents a completely new ground for novel social engineering techniques. Gartner predicts that AI-enabled fraud will fundamentally change the enterprise attack surface in following years[440]. We observed at least three areas highly influenced by AI: crafting more convincing phishing emails and messages that closely mimic legitimate sources, deepfakes focusing mainly on voice cloning and AI-driven data mining.

Checkpoint illustrated that ChatGPT is more than capable of writing a wide range of phishing e-mails[441], from simple basic phishing up to targeted spear-phishing mails using malicious files with macros. The main benefit for the attacker is the ability to target a wide range of organisations by easily letting the AI to generate spear-phishing e-mails on the fly. Darktrace researchers observed a 135% increase in novel social engineering attacks from January to February 2023, corresponding with the widespread adoption of ChatGPT[442]. The attacks used sophisticated linguistic techniques, including increased text volume, punctuation and sentence length. The trend suggests that generative AI is providing an avenue for threat actors to craft sophisticated and targeted attacks at speed and scale. Europol issued a warning about the potential use by cybercriminals of ChatGPT in March 2023[443].

We anticipate more targeted social engineering attacks using AI-based technology in the future. One of the prominent uses would be vishing attacks employing AI-based voice cloning. Voice cloning is the process of creating a synthetic voice using the audio recordings of a real person. Attackers can create the clones by capturing a sample of a person's voice, which could be accomplished by pulling a video from YouTube, TikTok or any other social network[444]. Even a

[425] https://cert.gov.ua/article/4492467.
[426] https://thehackernews.com/2023/05/apt28-targets-ukrainian-government.html.
[427] https://cert.gov.ua/article/4555802.
[428] https://cert.gov.ua/article/3931296.
[429] https://cert.gov.ua/article/3863542.
[430] https://cert.gov.ua/article/2698320.
[431] https://cert.gov.ua/article/971405.
[432] https://cert.gov.ua/article/861292.
[433] https://cert.gov.ua/article/955924.
[434] https://cert.gov.ua/article/703548.
[435] https://cert.gov.ua/article/619229.
[436] https://blogs.blackberry.com/en/2023/03/nobelium-targets-eu-governments-assisting-ukraine.
[437] https://therecord.media/nobelium-apt29-cozy-bear-phishing-eu-ukraine.
[438] https://cert.gov.ua/article/3761023.
[439] https://openai.com/blog/chatgpt.
[440] https://www.bitsight.com/resources/gartner-predicts-2023-cybersecurity-industry-focuses-human-deal.
[441] https://research.checkpoint.com/2022/opwnai-ai-that-can-save-the-day-or-hack-it-away/.
[442] https://ir.darktrace.com/press-releases/2023/4/3/8b2d6ba25d9d54a1895956a985fe4a7d08d9f42607a112fb17964e4b57fad7d6.
[443] https://www.europol.europa.eu/media-press/newsroom/news/criminal-use-of-chatgpt-cautionary-tale-about-large-language-models.
[444] https://www.thestreet.com/technology/fraudsters-new-trick-uses-ai-voice-cloning-to-scam-people.

few seconds could be enough to create a reasonable fake voice. Cybercriminals are using AI to make clones of people's voices to pretend to be a friend or family member and scam the victim for money. The US Federal Trade Commission issued a warning about calls where attackers pretend to be a family member who is in trouble and is asking for money, e.g. due to a broken car or getting into jail and needing to pay a lawyer[445] [446]. In another case, the attacker pretended that the victim's daughter called crying and saying that she was kidnapped; this was followed up with the attacker asking for the money as a ransom[447].

AI-based vishing attacks not only target the general public but also businesses. The first targeted attack on a business was in 2019 when cybercriminals used voice cloning to impersonate a CEO on the phone and convinced the CEO of a UK company to transfer $243 000 to an attacker's account[448]. This was a very rare case at that time but we expect to see a spike in similar attacks in the future. The FBI also observed[449] cases where threat actors used a real-time deepfake video in an attempt to get fraudulently hired by companies so as to get access to personal and financial information. Those attacks were mostly unsuccessful[450] due to the fact that the state-of-the-art of real-time deepfake tools is not quite good enough yet but we expect it will be soon.

With respect to AI-driven data mining, the attackers are using AI to identify potential targets and to determine the most effective approach for a social engineering attack, thus increasing the likelihood of success[451]. Automating data collection and creating persuasive messages can significantly enhance the potential impact of such attacks[452].

6.4 ABUSING MULTI-FACTOR AUTHENTICATION

Multi-factor authentication (MFA) is continuously being adopted more widely. The most representable sample from the business environment could be Microsoft products. According to Microsoft, the adoption of MFA rose to 28%[453] from the 22% we saw a year before[454]. Similar numbers were observed by Prove[455]. This is still a very low number but is high enough to force threat actors to develop new techniques to abuse multi-factor authentication[456]. We observed several novel approaches on how to overcome multi-factor authentication: MFA fatigue attack[457], adversary in the middle (AitM), and SIM swapping. On top of those tactics, the attackers use standard methods of phishing and vishing to steal MFA tokens[458] [459].

MFA fatigue attack[460], also known as MFA Bombing or MFA Spamming, abuses the push notification via smartphone. After using stolen credentials, the threat actor bombards users with repeated push notifications hoping the user will agree to approve a push notification to stop the flooding or mistakenly approve at least one notification. Moreover, the threat actors may improve the success of the attack by contacting the target through email, messaging platforms or over the phone, pretending to be IT support to convince the user to accept the MFA prompt. Several well-known companies have been successfully targeted this way. Acronis observed that this technique has proven to be very successful for the Lapsus$ and Yanluowang threat actors[461].

The Uber breach in September 2022 by Lapsus$ was one such case[462] [463]. The attacker probably bought the user password on the dark web initially; the attacker then repeatedly tried to log in to the Uber account. Each time, the user received a two-factor login approval request which initially blocked access. Eventually, the user accepted one and the attacker successfully obtained access to the Uber corporate infrastructure.

[445] https://consumer.ftc.gov/articles/scammers-use-fake-emergencies-steal-your-money.
[446] https://consumer.ftc.gov/consumer-alerts/2023/03/scammers-use-ai-enhance-their-family-emergency-schemes?utm_source=govdelivery.
[447] https://www.insideedition.com/artificial-abduction-daughter-calls-mom-to-say-shes-been-kidnapped-and-needs-ransom-but-its-an-ai.
[448] https://www.wsj.com/articles/fraudsters-use-ai-to-mimic-ceos-voice-in-unusual-cybercrime-case-11567157402.
[449] https://www.ic3.gov/Media/Y2022/PSA220628.
[450] https://securityintelligence.com/articles/synthetic-media-new-social-engineering-threats/.
[451] https://cyberconiq.com/blog/how-hackers-are-using-ai-for-social-engineering/.
[452] https://thecyberexpress.com/social-engineering-2023-what-has-changed/.
[453] https://www.microsoft.com/en-us/security/blog/2023/01/26/2023-identity-security-trends-and-solutions-from-microsoft/.
[454] https://news.microsoft.com/wp-content/uploads/prod/sites/626/2022/02/Cyber-Signals-E-1-218.pdf.
[455] https://assets-global.website-files.com/602ec799ae322d88eafe1d05/64467cf75122a13b20bf46d6_2023%20Prove%20Identity%20State%20of%20MFA%20Report.pdf.
[456] https://www.mandiant.com/m-trends.
[457] https://blog.isc2.org/isc2_blog/2023/02/the-top-5-new-social-engineering-attacks-in-2023-.html.
[458] https://www.social-engineer.com/the-2023-security-landscape-a-social-engineers-take/.
[459] https://www.crowdstrike.com/global-threat-report/.
[460] https://www.beyondtrust.com/resources/glossary/mfa-fatigue-attack.
[461] https://www.acronis.com/en-us/lp/cyberthreats-report-2022-end-year/.
[462] https://www.uber.com/newsroom/security-update.
[463] https://www.darkreading.com/attacks-breaches/uber-breach-external-contractor-mfa-bombing-attack.

Another example could be Cisco being hacked by the Yanluowang group[464]. As in the Uber case, the threat actors gained access to Cisco's network using an employee's stolen credentials and then convinced the Cisco employee to accept MFA push notifications through MFA fatigue and a series of sophisticated vishing attacks that impersonated a trusted support organisation.

Adversary in the middle[465] is the technique where the attacker positions himself between the victim and the legitimate service capable of circumventing MFA through reverse-proxy functionality. During the attack, the threat actor intercepts both user password and MFA token, allowing him to get initial access. Zscaler spotted a large-scale phishing campaign[466] [467] targeting the credentials of the Microsoft 365 email services of organisations in the US, UK, New Zealand and Australia. The campaign was unique as the threat actors were using a custom proxy-based phishing kit allowing the AitM technique to bypass multi-factor authentication. The kit was able to modify legitimate login pages pulled directly from victim logins. Microsoft identified DEV-1101 (also known as Storm-1101) as the threat actor developing, supporting and advertising several AitM phishing kits, which other cybercriminals can buy or rent[468].

SIM swapping[469] [470], also known as SIM splitting or SIM jacking is an attack type where the phone number of the victim is transferred to the fraudster's SIM card. The attacker first gathers information about the victim in order to be able to impersonate him or her to the mobile network operator. Criminals usually claim that the previous SIM card was lost, stolen or damaged. The attack allows the threat actor to intercept the one-time password sent by SMS or the verification voice calls. Mandiant reported the use of this technique by UNC3661 and UNC3944 threat actors[471]; CrowdStrike reported its use by Scattered Spider[472]. One of the latest high-profile cases involved the breach of the Google Fi telecommunications service[473] in January 2023, where the customer's information was leaked and later used for a SIM swapping attack.

6.5 SOCIAL ENGINEERING IN THE PHYSICAL WORLD

In its forecast, Mandiant reported that a new model of social engineering is emerging (or re-emerging), an approach that consists of deceiving victims in the physical world[474] as opposed to the virtual world. The most prevalent techniques used by threat actors are QR codes, sometimes called quishing, and USB keys. When the victim scans the malicious QR code with their smartphone or other devices, it redirects them to a malicious website or file. Alternatively, QR codes may be configured to automatically download malware onto the victim's device, allowing the attacker to steal sensitive information or take control of the device[475]. Spreading USB sticks around different physical locations is quite an old technique yet we observed a rise in its use during the reporting period.

We reported on incidents involving the use of QR codes in the 2022 ETL report. We have also detected multiple campaigns this year but those focused mainly on the Americas and China. Attackers were using multiple themes to lure the victims, including fake parking tickets, fake delivery notice slips and fake advertisements. One case in Europe included fake delivery notice slips from the French postal service distributed directly to victims' physical mailboxes[476]. The document provides information about the failed delivery attempt and invited the victim to scan a QR code and to enter their personal information and bank details. In another example, attackers were targeting citizens in San Francisco with fake parking tickets that direct victims to a payment website[477]. In another case, a 19-year-old man was arrested after he designed fake parking tickets and put them on cars near a beach in Northern California[478]. A victim lost $20 000 when she scanned a survey QR code in the bubble tea shop in Singapore[479]. Fortinet and HP Wolf

[464] https://www.bleepingcomputer.com/news/security/cisco-hacked-by-yanluowang-ransomware-gang-28gb-allegedly-stolen/.
[465] https://attack.mitre.org/techniques/T1557/.
[466] https://www.zscaler.com/blogs/security-research/large-scale-aitm-attack-targeting-enterprise-users-microsoft-email-services.
[467] https://www.acronis.com/en-us/lp/cyberthreats-report-2022-end-year/.
[468] https://www.microsoft.com/en-us/security/blog/2023/03/13/dev-1101-enables-high-volume-aitm-campaigns-with-open-source-phishing-kit/.
[469] https://www.incognia.com/the-authentication-reference/what-is-sim-swap-attack-and-why-fast-detection-is-important.
[470] https://sennovate.com/the-future-of-social-engineering-emerging-trends-and-threats/.
[471] https://www.mandiant.com/m-trends.
[472] https://www.crowdstrike.com/blog/analysis-of-intrusion-campaign-targeting-telecom-and-bpo-companies/.
[473] https://www.securityweek.com/google-fi-data-breach-reportedly-led-to-sim-swapping/.
[474] https://www.mandiant.com/resources/reports/mandiant-cyber-security-forecast-2023.
[475] https://heimdalsecurity.com/blog/quishing/.
[476] https://www.thelocal.com/20220902/french-postal-service-warns-of-new-qr-code-scam/.
[477] https://sfstandard.com/criminal-justice/san-francisco-fake-parking-tickets-scam-what-you-need-to-know/.
[478] https://www.cbsnews.com/news/fake-parking-ticket-scam-santa-cruz-california/.
[479] https://www.straitstimes.com/singapore/woman-who-scanned-qr-code-with-malware-lost-20k-to-bubble-tea-survey-scam-while-she-was-sleeping.

Security observed a large-scale Chinese-language phishing campaign abusing QR codes to steal credit card details and other sensitive information[480] [481].

When it comes to compromised removable devices, Mandiant observed several campaigns involving the use of infected USB drives and other external drives to spread malicious payloads[482] which were mostly financially motivated and espionage activities. The UNC3840 threat actor distributed BIRDBAIT LNK downloader to deploy multiple malware families. Mandiant determined the campaign used the malware as a pay-per-install service which provided an intrusion for other threat actors. Another two campaigns identified by Mandiant were executed by China-based groups UNC4191 and UNC53. UNC4191 was targeting a range of public and private sector entities based primarily in Southeast Asia but also in the US, Europe, and Oceania[483]. The activity began in April 2022, continued throughout the year, and leveraged infected USB devices as the initial intrusion vector for the campaign. UNC53 targeted a variety of industries across the globe. The group gained initial access to victims' environments through infected USB drives, leveraging legitimate binaries to side-load malicious DLLs and encrypted payloads.

IBM X-Force observed infection attempts by Raspberry Robin malware impacting organisations in mid-May 2022; the worm began spreading quickly within victims' networks from users sharing USB devices[484]. The infections spiked in early June and by early August Raspberry Robin peaked at 17% of infection attempts that X-Force observed. This peak was identified in the oil and gas, manufacturing and transportation industries. A Honeywell identified similar trend who reported a 52% increase in malware designed to propagate over USBs or to specifically exploit USBs for infection; targeting mainly industrial environments[485]. Talos observed several malware families delivered through removable media as an initial infection vector, including Sality and PlugX[486].

6.6 FROM MICROSOFT MACROS TO ISO, ONENOTE AND LNK FILES

Microsoft disabled outdated Excel 4.0 macros by default in January 2022[487]. Moreover, the VBA macros obtained from the Internet are blocked by default on Windows devices running its Access, Excel, PowerPoint, Visio and Word apps from July 2022[488]. As files with macros was the prevalent technique used in phishing and spear-phishing e-mails[489], threat actors were forced to change their tactics and techniques. Infection attempts were reported at the start of that shift in last year's report and this year we observed a continuation of the shift towards the use of LNK, OneNote and ISO/ZIP files in response to Microsoft's macro changes[490].

As LNK files can execute any file on the system with arguments (path, arguments, etc.), threat actors usually invoke legitimate applications such as PowerShell, CMD and MSHTA to download malicious files. We observed two tactics for the distribution of LNK files. The payload could be delivered directly within the LNK file or the malicious LNK file could be inserted into a Microsoft Office document. The second approach is to keep using the MS office document with macros that are being delivered in container-like ISO or ZIP file. The macros are blocked based on a Mark of the Web (MOTW) attribute which flags files that were downloaded from the web. However, delivering files inside ISO or ZIP only places a MOTW marking on the attachment itself, not on the files inside, allowing the delivery of macros-enabled documents undetected. Both tactics were heavily used by threat actors during the reporting period. McAfee[491] and Talos[492] reported multiple malware campaigns where the shift in tactic was observed, including Emotet, IcedID, and Qakbot.

6.7 PHISHING KITS AND PHISHING-AS-A-SERVICE (PHAAS)

Phishing as a service[493] is one category of the crime-as-a-service (CaaS) phenomenon. We recognise expert crime groups that include ransomware-as-a-service (RaaS), access-as-- service (AaaS), and most recently PhaaS. PhaaS

[480] https://www.fortinet.com/blog/threat-research/qr-code-phishing-attempts-to-steal-credentials-from-chinese-language-users.
[481] https://threatresearch.ext.hp.com/wp-content/uploads/2023/03/HP-Wolf-Security-Threat-Insights-Report-Q4-2022.pdf.
[482] https://www.mandiant.com/m-trends.
[483] https://www.mandiant.com/resources/blog/china-nexus-espionage-southeast-asia.
[484] https://www.ibm.com/reports/threat-intelligence.
[485] https://www.honeywellforge.ai/us/en/campaigns/industrial-cybersecurity-threat-report-2022.
[486] https://blog.talosintelligence.com/talos-year-in-review-2022/.
[487] https://techcommunity.microsoft.com/t5/excel-blog/excel-4-0-xlm-macros-now-restricted-by-default-for-customer/ba-p/3057905.
[488] https://techcommunity.microsoft.com/t5/microsoft-365-blog/helping-users-stay-safe-blocking-internet-macros-by-default-in/ba-p/3071805.
[489] https://documents.trendmicro.com/assets/rpt/rpt-rethinking-tactics-annual-cybersecurity-roundup-2022.pdf.
[490] https://www.ibm.com/reports/threat-intelligence.
[491] https://www.mcafee.com/blogs/other-blogs/mcafee-labs/rise-of-lnk-shortcut-files-malware/#:~:text=During%20the%20second,the%20LNK%20attacks.
[492] https://blog.talosintelligence.com/talos-year-in-review-2022/.
[493] https://www.sophos.com/en-us/content/security-threat-report.

allows anyone with even an entry-level knowledge of cybersecurity to benefit from a phishing attack. Threat actors are positioned as a service provider. Trend Micro observed[494] offers for the service with prices as low as $15 a day and a portion of any ransom pay out, or flat $40 fee for a phishing kit. The service and kits usually include the capabilities and tools required to launch a phishing attack, including email templates, spoof website templates, contact lists of potential targets, detailed instructions on how to execute an attack, capabilities to bypass spam filters, capabilities to bypass multi-factor authentication, panels for monitoring results as well as access to customer support[495].

IBM X-Force conducted a large analysis of phishing kits covering thousands of phishing kits from around the world. IBM X-Force discovered that kit deployments are operational longer, reach more users and target personal data over credit card data[496]. Analysis of almost every reported phishing kit revealed a strong emphasis on gathering personal information, with names being the primary target at a rate of 98%. Following closely were email addresses at 73%, home addresses at 66% and passwords at 58%. Interestingly, the focus on credit card information experienced a significant drop, declining from a 61% target rate in the previous year to just 29%. The lifespan of phishing kits that were observed has shown notable growth, more than doubling year over year. Despite this increase, the median deployment duration remained relatively short at 3.7 days. In terms of impact, approximately half of all reported kits affected 93 users. The maximum number of victims recorded for a single phishing attack surpassed 4 000.

In September 2022, Resecurity identified a Phishing-as-a-Service (PhaaS) with MFA bypass called EvilProxy advertised in the Dark Web[497]. It functions as a reverse proxy that's set up between the target and a legitimate login page to intercept credentials, two-factor authentication (2FA) codes, and session cookies to hijack accounts of interest. Since early March 2023, Proofpoint researchers have been monitoring an ongoing hybrid campaign using EvilProxy to target thousands of Microsoft 365 user accounts. This campaign's reach is approximately 120,000 phishing emails sent to hundreds of targeted organizations across the globe between March and June 2023[498].

Cisco Talos identified a Phishing-as-a-Service platform named Greatness that has been leveraged by cybercriminals to target business users of the Microsoft 365 cloud service since at least mid-2022[499] [500]. Greatness focused only on Microsoft 365 phishing pages, providing its affiliates with an attachment and link builder that creates highly convincing decoy and login pages. It contained features such as having the victim's email address pre-filled and displaying their company logo and background image extracted from the target organisation's real Microsoft 365 login page.

Akamai Security Research observed a highly sophisticated phishing kit that was mimicking several large retail brands ahead of the holiday season[501]. The kit used a mixture of social engineering, multiple evasion detection techniques, and access control to bypass security measures. Mandiant reported a PhaaS platform called Caffeine[502], a platform which is unique in the sense that it features an entirely open registration process allowing anyone with an email to register for their services.

More advanced phishing kits provide services to overcome multi-factor authentication, e.g. the technique adversary in the middle (AitM) described in a previous section. Microsoft identified DEV-1101 (also known as Storm-1101) as the threat actor developing, supporting and advertising several AitM phishing kits[503].

6.8 BUSINESS AND VENDOR EMAIL COMPROMISE (BEC, VEC)

Business e-mail compromise (BEC) remains one of attackers' favourite means for extracting financial gain from their victims. The threat actors employ more and more sophisticated techniques, from the standard spear-phishing e-mail to a compromised company e-mail, to persuade a victim to initiate malicious money transactions. The techniques includes spear-phishing e-mails from clients or vendor e-mail addresses (vendor email compromise), pretexting or

[494] https://www.trendmicro.com/en_us/ciso/23/c/phishing-as-a-service-phaas.html.
[495] https://heimdalsecurity.com/blog/what-is-phishing-as-a-service-phaas/.
[496] https://www.ibm.com/reports/threat-intelligence.
[497] https://www.resecurity.com/blog/article/evilproxy-phishing-as-a-service-with-mfa-bypass-emerged-in-dark-web. https://securityaffairs.com/135318/cyber-crime/evilproxy-phishing-as-a-service.html.
[498] https://www.proofpoint.com/us/blog/email-and-cloud-threats/cloud-account-takeover-campaign-leveraging-evilproxy-targets-top-level.
[499] https://thehackernews.com/2023/05/new-phishing-as-service-platform-lets.html.
[500] https://blog.talosintelligence.com/new-phishing-as-a-service-tool-greatness-already-seen-in-the-wild/.
[501] https://www.akamai.com/blog/security-research/sophisticated-phishing-scam-abusing-holiday-sentiment.
[502] https://www.mandiant.com/resources/blog/caffeine-phishing-service-platform.
[503] https://www.microsoft.com/en-us/security/blog/2023/03/13/dev-1101-enables-high-volume-aitm-campaigns-with-open-source-phishing-kit/.

thread hijacking and external thread hijacking. Another technique is call-back phishing that we describe in an individual section of this report.

The FBI reported a 10% increase in BEC complaints with adjusted losses of over $2.7 billion[504]. IBM X-Force observed BEC as one of the top three specific actions threat actors took on victim networks[505]. Trellix detected BEC accelerating at the end of 2022, with a 64% increase on a quarterly basis. Trellix observed most of CEO fraud emails were sent using free email services and 78% of all BEC attacks were using common CEO phrases[506]. APWG reported that the average payment requested increased by 41%[507]; this suggests that treat actors focused on larger targets. Abnormal Security analysis showed that VEC has a three times higher success rate than the traditional BEC approach, as employees are trained to look for emails impersonating an internal executive, not a vendor[508].

Verizon discovered that pretexting constitutes 27% of social engineering breaches, almost all of which are BECs[509]. One of the major events in 2023 was the collapse of Silicon Valley Bank and Signature bank. Threat actors used a pretext of the events to impersonate known vendors (who had their accounts in one of those banks) to the targeted victims and requested the victims to update payment information related to that vendor[510].

Cisco Talos observed many threat actors employing thread hijacking and external thread hijacking techniques[511]. Threat actors are using compromised email threads between target organisations and third parties, masquerading email replies from the third party. The researchers observed that the compromised thread could even come from completely different and older security breaches and still provide good success rates.

6.9 INCREASING ATTACKS TO THE WEB3 ECOSYSTEM

Cryptocurrencies are still the most prominent means whereby cyber criminals obtain payment from their victims. Last year, we reported that attacks directly targeting crypto exchanges and owners of cryptocurrencies are increasing. In this reporting period we noted that this trend is continuing and spreading to the whole web3 ecosystem, including crypto exchanges, owners of cryptocurrencies, non-fungible tokens (NFTs), cross-blockchain connection mechanisms and even online games[512]. The FBI observed an unprecedented increase of 183% in the number of victims and losses in cryptocurrency-related fraud[513]. Sonicwall reported on a steady and sustained rate of crypto-related phishing, even at a time when cryptocurrencies, including Bitcoin, were falling in value[514].

The NFT airdrop scam[515] usually involves minting a new malicious token, sending it to user accounts and relying on users investigating this mysterious token. Threat actors create phishing pages and social media accounts to socially engineer victims into connecting their wallets and steal the cryptocurrencies and other NFTs. Mandiant observed[516] a broad, months-long cryptocurrency phishing campaign, where thousands of smart contacts were used to deliver malicious NFTs to over a million unsuspecting users. When the victims connected their wallets, the attacker was able to collect and transfer assets, including NFTs. Assets were quickly sold, and the funds moved through various blockchains to launder the funds and obscure their trail.

Airdrop scams are not limited to NFTs only but include crypto tokens in general. In February 2023, attackers were promoting fake airdrop links to claim BLUR tokens on malicious websites and managed to steal over $300,000 from their victims[517]. In July 2022, a threat actor used the lure of free UNI tokens airdrops to trick victims into granting the hacker full access to victims' wallets, resulting in $8 million being stolen[518].

[504] https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.
[505] https://www.ibm.com/reports/threat-intelligence.
[506] https://www.trellix.com/en-us/advanced-research-center/threat-reports/feb-2023.html.
[507] https://docs.apwg.org/reports/apwg_trends_report_q4_2022.pdf.
[508] https://www.techrepublic.com/article/cybersecurity-bec-attack-mimics-vendors/.
[509] https://www.verizon.com/business/en-gb/resources/2022-data-breach-investigations-report-dbir.pdf
[510] https://ironscales.com/blog/emerging-bec-variant-to-exploit-collapse-of-silicon-valley-bank.
[511] https://blog.talosintelligence.com/talos-year-in-review-2022/.
[512] https://www.mandiant.com/m-trends.
[513] https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf.
[514] https://www.sonicwall.com/2023-cyber-threat-report/.
[515] https://medium.com/metamask/phisher-watch-airdrop-scams-82eea95d9b2a.
[516] https://www.mandiant.com/m-trends.
[517] https://blockchain.news/news/scammers-target-nft-users-in-blur-token-airdrop-scam.
[518] https://www.bleepingcomputer.com/news/security/8-million-stolen-in-large-scale-uniswap-airdrop-phishing-attack/.

Cryptocurrency giveaway scams are rapidly gaining in popularity[519] [520]. The giveaway scam typically promises a large prize in exchange for a small processing fee or your personal information. Multiple cases included the names of Elon Musk and Tesla[521]. Trend Micro reported a case in which victims were persuaded to deposit small amounts of crypto into a threat actor's wallet on a false promise that they may receive up to 5,000 Bitcoin in return[522]. PC Risk reported on the Andrew Tate giveaway scam[523] and FIFA crypto giveaway scam[524], where victims were instructed to send a certain amount of cryptocurrency to a specific address in exchange for a double return on their initial investment.

Pig butchering, a cryptocurrency investment scam, is a novel scheme that involves the threat actor gaining the victim's trust and then enticing them into making deposits into crypto-investment accounts, providing fictitious returns to encourage additional investments. The FBI issued a public service announcement on 3 October 2022, warning against this threat[525]. Victims can usually track their investments on fake websites and apps that display dizzying growth. The operators of the scheme later proceed to the butchering part. When the victims attempt to cash out the investments, they are told they need to pay income taxes or additional fees, causing them to lose additional funds. Last, the attacker is cutting contact with the victim and disappearing with their cryptocurrency[526]. One of the biggest cases happened in San Francisco[527]. An investor lost US$1.2 million after the attacker gained his trust pretending to be an old colleague from a previous job.

The FBI issued a public service announcement alerting the public to new schemes targeting users who play play-to-earn Web3 games[528]. According to the FBI, fake gaming applications that advertise lucrative financial incentives lure victims into depositing funds into specific wallets. The play-to-earn game provides fake rewards in exchange for some activity such as growing crops on an animated farm. Victims play the game and see fake rewards accumulating in the app. When victims stop depositing funds into the wallet, criminals drain victim wallets using a malicious program that victims unknowingly activated upon joining the game.

6.10 EXTORTION WITHOUT THE USE OF RANSOMWARE IS RISING

Extortion was once mostly connected with ransomware and ransomware groups. But extortions without the use of ransomware are now rising continuously. CrowdStrike observed a 20% increase in the number of adversaries conducting data theft and extortion campaigns without deploying ransomware[529]. Tenable reported that extortion-only attacks are rising in prominence[530]. The extortion without ransomware usually includes threatened DDoS attacks, publishing data or reporting the breach to customers or regulators. Last year, we reported on double and triple extortion threats that combine several previously seen elements with data encryption. During this period we observed employment of different social engineering techniques during the victim extortion phase that included even more personal and intimidating approaches[531].

Cybercriminals expressed quite a high degree of professionalism during ransomware attacks and while coordinating decryption. The criminals adopted the services normally provided by IT service organisations, including 24/7 support and helpdesk (e.g. helping customers to pay ransom in cryptocurrencies). Threat groups hardly communicated with their victims apart from phishing or spear-phishing during the initial access phase. Mandiant observed a shift in that area, cybercriminals using different approaches and employing social engineering techniques in different stages of cyberattacks, actively threatening individuals and attempting to bribe individuals to obtain system access[532].

Mandiant observed two groups, Lapsus$ and UNC3944, that went to extreme lengths to harass and, in some cases, intimidate members of the organisations they compromised[533]. The groups targeted individual employees of an organisation by changing their titles in the Global Address List and, in another, spammed obscene messages to

[519] https://www.welivesecurity.com/wp-content/uploads/2023/02/eset_threat_report_t32022.pdf.
[520] https://www.group-ib.com/media-center/press-releases/massive-crypto-attack/.
[521] https://www.forbes.com/sites/mattnovak/2023/01/31/25-elon-musk-impersonator-scams-on-social-media-people-actually-fell-for/?sh=1a100d1357f8.
[522] https://news.trendmicro.com/2022/12/09/elon-musk-freedom-giveaway-crypto-scam-twitter/.
[523] https://www.pcrisk.com/removal-guides/26430-andrew-tate-crypto-giveaway-scam.
[524] https://www.pcrisk.com/removal-guides/25342-fifa-crypto-giveaway-scam.
[525] https://www.ic3.gov/Media/Y2022/PSA221003.
[526] https://www.welivesecurity.com/wp-content/uploads/2023/02/eset_threat_report_t32022.pdf.
[527] https://www.forbes.com/sites/cyrusfarivar/2022/09/09/pig-butchering-crypto-super-scam/.
[528] https://www.ic3.gov/Media/Y2023/PSA230309.
[529] https://www.crowdstrike.com/global-threat-report/.
[530] https://www.tenable.com/cyber-exposure/tenable-2022-threat-landscape-report.
[531] https://www.crowdstrike.com/global-threat-report/.
[532] https://www.mandiant.com/m-trends.
[533] https://www.mandiant.com/m-trends.

employees using a variety of internal tools. UNC3661 went as far as joining teleconference calls held by employees of the compromised organisations to push for capitulation to the demands for extortion. Dragos disclosed an attempt at extortion where the attackers reached out to family members to push the negotiations for extortion forward[534].

The attackers' inclination to specifically target individuals with personal threats and involve even their family members presents a progression in the scope of these attacks. Malicious actors now view individual people and their families as acceptable targets in their pursuit of profits from their intrusions. Organisations should consider this change in attack surface during the planning phase for the defence.

6.11 RE-EMERGENCE OF CALL-BACK PHISHING

Call-back phishing is a hybrid technique which combines standard phishing or spear-phishing with vishing. It is used to overcome technical restrictions to sending a malicious link or file or to improve the success rate of a spear-phishing campaign by increasing the perceived trustworthiness. For example, the attackers include a phone number into a phishing e-mail, which makes the victim less likely to consider it spam and, thus, the victim is lured into calling. SOC Radar observed an increased number of such attacks[535].

In July 2022, CrowdStrike observed a call-back phishing campaign impersonating CrowdStrike and other cybersecurity companies[536]. The phishing email informed the victim of a security breach and tried to persuade him or her to call the phone number provided. In November 2022, Palo Alto identified the Luna Moth call-back phishing campaign and attributed it to the Silent Ransom threat actor[537]. The campaign targeted small and medium-sized organisations in the legal industry and large organisations in the retail sector. The phishing email claimed that the victim is responsible for charges detailed in an attached invoice. If the victim did not recognise the invoice, it had the phone number to call and clarify. During the call, attackers requested remote connection to the victim computer and installed malware.

[534] https://www.techtarget.com/searchsecurity/news/366537202/Dragos-discloses-blocked-ransomware-attack-extortion-attempt.
[535] https://socradar.io/a-new-rising-social-engineering-trend-callback-phishing/.
[536] https://www.crowdstrike.com/blog/callback-malware-campaigns-impersonate-crowdstrike-and-other-cybersecurity-companies/.
[537] https://unit42.paloaltonetworks.com/luna-moth-callback-phishing/.

7. THREATS AGAINST DATA

In 2006, the British mathematician Clive Humby coined the phrase *data is the new oil*, magnifying the importance data were assuming in IT and production domains, and more generally in society overall. This concept was renewed in 2017 in an article that appeared in the Economist claiming that *the world's most valuable resource is no longer oil, but data*[538]. The phrase *data is the new oil* anticipated the data-driven revolution that we observed in the following years. Today, in fact, we live in an interconnected society where cloud, edge and IoT technologies and applications produce huge amounts of data every second[539]. These data are fundamental for all enterprises that want to compete in the global market and must be properly managed and analysed. Better management and analysis, in fact, leads to faster processes, better customer management and lower overhead costs.

On top of this, in the last few years, Machine Learning (ML) and Artificial Intelligence (AI) are being increasingly adopted and are boosting the migration from traditional software systems based on deterministic algorithms to systems where ML/AI models use data to calculate a solution to individual instances of a problem. AI can profoundly change the current norm by revolutionising our society and the way it operates[540]. Looking back to data, *if AI is the new electricity, high quality training data is the new oil*[541]. The difficulty in finding high-quality data can harm current AI tools and their decision-making, introducing new security, privacy and safety risks.

The central role assumed by data as the enabler of modern systems built on AI/ML makes data in the cloud-edge continuum a major target for cybercriminals. Threats against data aim to block access to data as well as to manipulate (e.g. poison) data to interfere with system behaviour. For instance, ransomware, RDoS and DDoS aim to deny access to data and possibly collect a payment to restore this access. In addition, information manipulation is built on the manipulation of data and phishing in its novel form based on deepfakes, is also built on the manipulation of data.

A data breach is defined in the GDPR as *any breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorised disclosure of or access to personal data transmitted, stored or otherwise processed* (article 4.12 GDPR). Technically speaking, threats against data can be mainly classified as data breach or data leak. Though often used as interchangeable concepts, they entail fundamentally different concepts that mostly lie in how they happen[542] [543].

Data breach is an intentional cyberattack executed by a cybercriminal with the goal of gaining unauthorised access to release sensitive confidential or protected data. In other words, a data breach is a deliberate and forceful attack against a system or organisation with the intention to steal data.

Data leak is an event (e.g. due to misconfigurations, vulnerabilities or human errors) that can cause the unintentional loss or exposure of sensitive, confidential or protected data. It does not consider intentional attacks and is sometimes referred to as data exposure.

In addition to data leak and data breach, the increasing adoption of ML/AI models at the core of novel distributed systems and decision-making put data manipulation under the spotlight. Data manipulation attacks modern systems affecting the accuracy of their results by manipulating datapoints either during training (i.e. data poisoning) or inference (i.e. adversarial attacks) time, undermining trust in IT/production systems and society overall, as follows.

Data manipulation is a category of attacks that aims to manipulate trustworthy data into untrustworthy, bugged data, targeting the accuracy and performance of ML/AI, as well as the perception of reality by people[544]. It includes **data**

[538] https://www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data.
[539] https://www.domo.com/learn/infographic/data-never-sleeps-10.
[540] https://www.linkedin.com/pulse/data-new-oil-ai-electricity-arshad-hisham/.
[541] https://becominghuman.ai/training-data-is-the-new-oil-where-should-i-drill-284229f0dae9.
[542] https://blog.f-secure.com/data-breach-and-data-leak-whats-the-difference/.
[543] https://www.upguard.com/blog/data-breach-vs-data-leak#:~:text=Simply%20put%2C%20a%20data%20leak,Apps%20data%20leak%20in%202021.
[544] https://securityintelligence.com/articles/data-poisoning-ai-and-machine-learning/.

poisoning, attacks during training time that manipulates the training set to reduce the accuracy of the trained model or cause the misclassification of specific data points at inference time[545], **adversarial attacks,** inference-time attacks that consist of specially-crafted data points that are routed to the ML model to cause a faulty or wrong inference (mis-classification), and **information manipulation**, an intentional attack that consists of the creation or sharing of false or misleading information, targeting people's perception of a specific event. Given its significance and prominence during the reporting period, information manipulation is in detailed analysed in a forthcoming dedicated chapter.

Threats against data consistently rank high among the leading threats in the ETL and this trend continued during the reporting period of the ETL 2023 report. Adversaries explored a series of new techniques and exploited the increasing online presence and use of online services by the general public, as well as the increasing migration to cloud computing and the pervasiveness of ML/AI solutions and models. As already observed in ETL2022, identity theft is one of the major data breach attacks (in terms of impact and value), where malicious actors use personal data to impersonate a user and cause huge damage to a target system. Moreover, given the significance of data and, in particular, of private and sensitive data, adversaries are combining more sophisticated threats to target data, such as ransomware or supply chain attacks, as well as distributed denial of services and the manipulation of information, all of which are described in other parts of this report. Ransomware accounted for a large part of data breaches, 24% according to Verizon[546] and 35% according to Tenable Research[547]. The number of data breaches originating from supply chain attacks outperformed the ones caused by malware by about 40%[548] according to ITC report. Finally, given the massive role assumed by ML/AI models in the operations of modern systems, adversaries are focusing on decreasing the accuracy and performance of ML/AI models by launching new and more powerful adversarial and poisoning attacks.

During this reporting period, a substantial increase in malware-related incidents, particularly evident in the latter part of H1, has been observed, a trend largely attributed to the surge in ransomware incidents discussed in Chapter 4. Additionally, a more comprehensive analysis of these threats, taking sectors and regions into account, reveals that public administration, individuals and healthcare sectors continue to be the primary targets for data leaks and breaches.

The Cost of a Data Breach Report 2022 released by IBM in July 2022 proposed an overview of the costs of data breaches that occurred between March 2021 and March 2022. In particular, USD 4.35 million is the average total cost of a data breach but this rises to USD 4.82 million when critical infrastructure is targeted. The average cost decreases to USD 3.05 million when security AI and automation are used. The average cost savings when an incident response (IR) team is constituted and IR plan is regularly tested is USD 2.66 million[549].

Following up from the overall cybersecurity landscape overview of Chapter 1, the following Figures (figure 34 and figure 35) provide a deeper insight into the timeline of observed incidents related to data threats during the reporting period, as well as their break down by sectors and by geographical spread.

[545] https://arxiv.org/abs/2209.14013.
[546] https://www.verizon.com/business/resources/T14a/reports/2023-data-breach-investigations-report-dbir.pdf.
[547] Tenable Research, TENABLE 2022 THREAT LANDSCAPE REPORT A guide for security professionals to navigate the modern attack surface.
[548] ITRC 2022 Data Breach Report.
[549] IBM, The Cost of a Data Breach Report 2022.

Figure 34: Time series of major incidents observed by ENISA (July 2022 - June 2023)

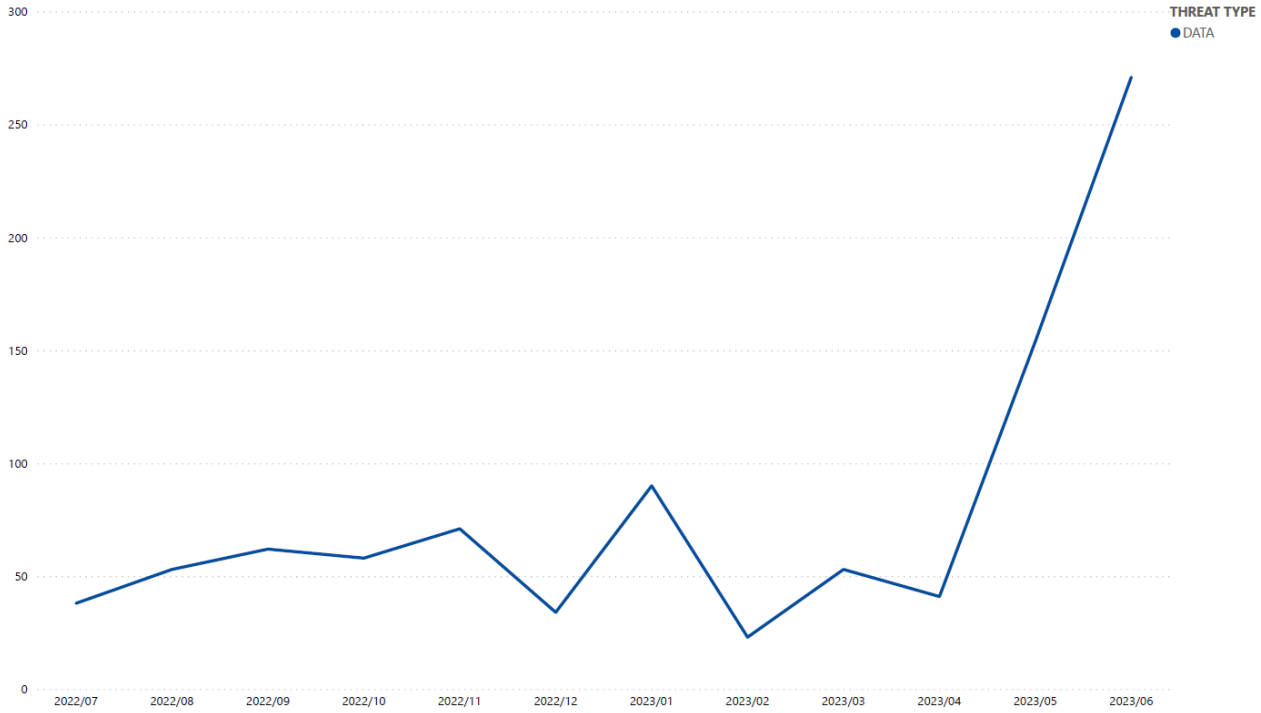
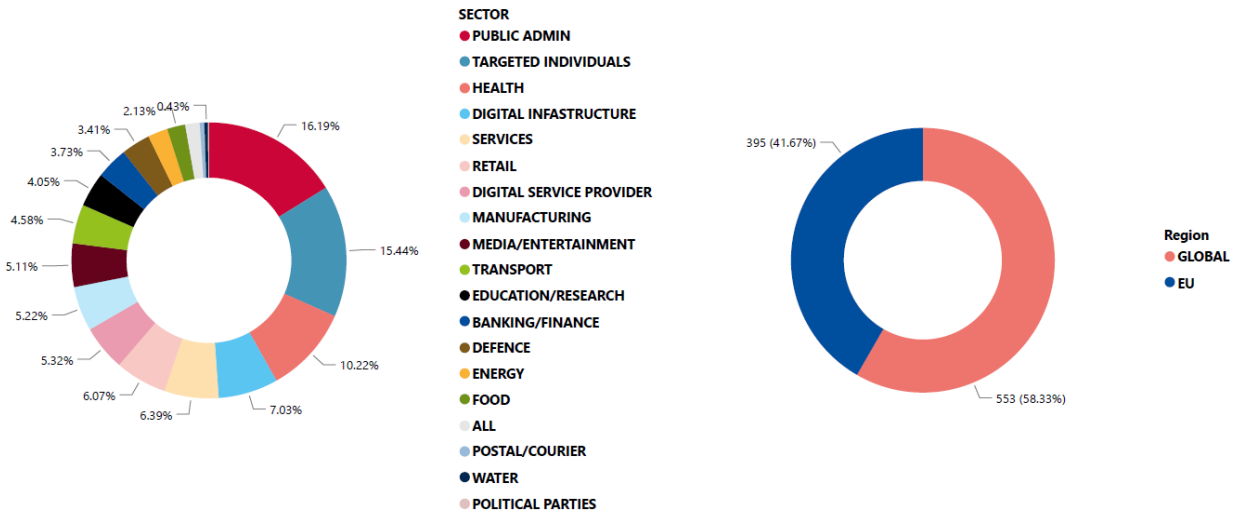


Figure 35: Break down of Sectors with threat type and region



7.1 TRENDS

The Data Never Sleeps infographic, version 10.0[550], shows that the increase in data collection, sharing and analysis has grown continuously over the last 10 years. For instance, every minute, users post 575k tweets, upload 500 hours of videos in YouTube, send 231.4 million emails and 16 million messages, stream 452k hours of Netflix movies, make 5.9 million searches in Google, to name but a few. These trends are all increasing and according to Statista the entire world produced and consumed a total of 97 zettabytes in 2022 and this is predicted to grow to 181 zettabytes per year by 2025.

[550] https://www.domo.com/learn/infographic/data-never-sleeps-10.

Data becomes an invaluable target for cybercriminals who may want to affect the operations of a system or obtain financial gain. Since 2004, the total number of breached accounts has reached 16 billion (number accessed 9 June 2023), with 5.7 billion having a unique email address[551] according to Surfshark. In more detail, each email address is breached three times on average with 73 unique addresses breached per 100 people and 209 accounts breached per 100 people on average. These numbers confirm Microsoft's statement that: *Data breaches are inevitable*[552].

To counteract this worrisome scenario, data breach and privacy regulations continue to expand, including GDPR, as do more stringent regulations[553]. Gartner predicted that *Through 2023, government regulations requiring organisations to provide consumer privacy rights will cover 5 billion citizens and more than 70% of global GDP*[554].

In the following, we provide an overview of trends in data attacks.

7.2 ATTACK VECTORS, ASSETS, MOTIVATIONS AND TARGETS

According to the Identity Theft Resource Center (ITRC)[555] and Verizon, the attack vectors built on social engineering (e.g. phishing, pretexting) and ransomware remain in the top spot[556] [557]. According to the ITRC[558], phishing, smishing and BEC remained the first attack vectors, while supply chain attacks surpassed malware-based data breaches by 133% affecting 10 and 4.3 million victims respectively. The number of data breaches related to unprotected cloud databases decreased of 75%, while physical attacks decreased to a total of 46 attacks over the year. System and human errors also dropped reaching the same numbers observed in 2020 but still reaching the third spot. Verizon observed that 50% of social engineering was based on pretexting, which moves from fear and urgency to building a realistic story creating a false sense of trust in the target. Ransomware accounted for 24% of all attacks, with *more than 62% of all incidents committed by organised crime actors and 59% of all incidents with a financial motivation*, only preceded by the use of stolen credentials (more than 40%) and followed by phishing and pretexting.

According to Verizon[559], 83% of the attacks involved external actors, often organised crime groups with financial goals; however, it is important to note that the role of internal actors in data breaches was not negligible and accounts for 18% of cases including both voluntary misuse and inadvertent human errors. In general, 74% of the breaches involved the human element (65% according to Thales[560]) and almost all attacks (95%) had a financial motivation, an increase of 5% over the previous year. Espionage was the second motivation in the ranking, accounting for around 5%. The number of breaches involving cryptocurrencies saw a fourfold increase compared to the previous year.

The ITRC[561] saw healthcare (344 breaches), financial services (268 breaches) and manufacturing & utilities (249 breaches) as the domains receiving the highest number of compromises, while technology took the first spot (by far) regarding the number of victims (248 million) followed by hospitality (69 million). With respect to 2021, the largest growth in compromises occurred in Healthcare, the largest growth in victims occurred in financial services. Verizon ranks public administration (584 breaches), financial and insurance (480 breaches), and healthcare (436 breaches) according to data breaches (known incidents with confirmed data disclosure)[562]. Healthcare, financial services and public administration were also in the top three spots according to Tenable[563], while discrete attention was given to education with particular reference to K12-institutions[564]. K-12 institutions retain data that belong to children and teenagers that must be protected to the highest standards possible.

[551] https://surfshark.com/research/data-breach-monitoring.
[552] Microsoft Digital Defense Report 2022.
[553] Cyber: The changing threat landscape, Risk trends, responses and the outlook for insurance.
[554] https://www.gartner.com/en/newsroom/press-releases/2022-06-21-gartner-unveils-the-top-eight-cybersecurity-predictio.
[555] https://www.idtheftcenter.org/.
[556] https://www.verizon.com/business/resources/T14a/reports/2023-data-breach-investigations-report-dbir.pdf.
[557] 2022 ITRC Annual Data Breach Report.
[558] 2022 ITRC Annual Data Breach Report.
[559] https://www.verizon.com/business/resources/T14a/reports/2023-data-breach-investigations-report-dbir.pdf.
[560] Thales, 2023 Data Threat Report: Global Edition.
[561] 2022 ITRC Annual Data Breach Report.
[562] https://www.verizon.com/business/resources/T14a/reports/2023-data-breach-investigations-report-dbir.pdf.
[563] Tenable Research, TENABLE 2022 THREAT LANDSCAPE REPORT A guide for security professionals to navigate the modern attack surface
[564] EDUCATION THREAT LANDSCAPE REPORT: '13,800 public school districts with 55 million students are under cyber threat in the US.

Servers, persons and development users remained in the first three spots for the main target assets, with the same ordering and similar shares as in 2021[565] as reported by Verizon. The same discussion holds for the types of assets, where web applications, mail and desktop or laptop computers remain in the first three spots in the rankings.

7.3 DATA COMPROMISE SIMILAR TO 2022 BUT INCREASE IN 2023

The central role of data in our society has produced a sharp increase in the quantity of data collected and in the importance of proper data analysis. The price we pay for such importance has been a continuous and unstoppable increase in data compromises up to 2021 which stayed almost the same in 2022 but started to grow again for 2023.

In 2022, for the first time in the last few years, data compromises observed by ITRC did not increase with respect to the previous year, showing almost the same number: 1802 total compromises in 2022, 1862 total compromises in 2021[566]. The ITRC mentioned the war in Ukraine as a possible distracting factor for cybercriminals; it also mentioned the volatility of cryptocurrency as a factor causing a refocusing of cybercriminals targets (i.e. phishing-based scams using stolen data and supply chain attacks). During the second half of 2022 ITRC saw a sharp increase in the number of data compromises, with a 21% increase compared to the first half. However, Tenable Research noted a decrease in the number of breaches[567], thus making it difficult to ascertain the real situation.

This decreasing trend for 2022 was also supported by Tenable and Surfshark. According to Tenable Research, the total number of records exposed decreased sharply from 40 billion in 2021 to 2.3 billion in 2022, accompanied by a sharp decrease in the number of files exposed, 1.8 billion in 2021 against 389 million in 2022. In this context, the total quantity of data exposed remained stable, 260 TB in 2021 compared to 257 TB in 2022. According to Surfshark, 310 million accounts were leaked in 2022, a third of the number leaked in 2021[568].

However, regrettably, this declining trend came to a halt in 2023, as indicated by global data breach statistics from vendors (as also illustrated in Figure 35). Leaked accounts experienced a nearly threefold surge in the second quarter of 2023 compared to the preceding quarter. This concerning upswing in data breaches underscores the inadequacy of existing data protection measures, with sensitive information remaining vulnerable as cybercriminals persistently gain access to it in greater numbers. In Q2 2023, North America bore the brunt of breaches, followed by Europe and Asia (as also illustrated in Figure 36)[569] [570].

7.4 IDENTITY THEFT AND SYNTHETIC IDENTITY

As reported by CERT-EU, *identity abuse essentially consists of using valid accounts and legitimate applications to perpetrate malicious activities in a persistent and stealthy way. Attackers abuse the inherent trust in any action associated with authenticated users or authorised applications. Identity abuse can be seen as an extension of the living-off-the land (LOTL) tactic, where an attacker makes use of legitimate tools to remain undetected, whereas, through identity abuse, the attacker will additionally make use of legitimate accounts. Observed tactics showed the unprecedented level of sophistication the adversaries leveraged to abuse their victims' identities for lateral movement and stealthy operations. They remained undetected for more than six months in the network of hundreds of compromised organisations*[571].

Due to the increase in data breaches, personal and sensitive data has been easily accessible to malicious actors via online forums and the dark web. This has had a cascading effect on identity theft. The ITRC's *2022 Trends in*

[565] https://www.verizon.com/business/resources/T14a/reports/2023-data-breach-investigations-report-dbir.pdf.
[566] 2022 ITRC Annual Data Breach Report.
[567] Tenable Research, TENABLE 2022 THREAT LANDSCAPE REPORT A guide for security professionals to navigate the modern attack surface.
[568] https://surfshark.com/blog/data-breach-recap-2022.
[569] https://surfshark.com/research/study/data-breach-statistics-2023-q1.
[570] https://www.zdnet.com/article/data-breaches-grow-nearly-three-times-with-us-accounts-most-compromised/.
[571] https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-CERT-EU-Threat_Landscape_Report-Volume1.pdf#page=13&zoom=auto,-274,51.

Identity[572] and *2022 Consumer Impact*[573] reports illustrated the substantial impact of identity scams and fraud: 40% of consumers claimed their personal information had been stolen, compromised or misused.

The Federal Trade Commission in the USA reported similar trends, noting a monetary loss of USD 8.8 million due to fraud, an increase of 30%. Among these frauds, in 2022, there were over 1.1 million reports of identity theft received through the FTC's IdentityTheft.gov website[574].

7.5 LACK OF TRANSPARENCY IN DATA BREACH NOTICES

In 2022 there was a substantial decrease in the number of data breach notices, resulting in an important lack of transparency[575]. If almost 100% of notices mentioned attack vectors/details in 2018-2020, decreasing to 93% in 2021, in 2022 this number took a huge hit to 58%. This was even more important when considering the victim count, i.e. 34% of notices in 2022. This trend is very risky and can impact the ability of businesses to determine the risk of any breach and the countermeasures to take against it. Possible reasons are recent court decisions in the USA that point to the need to share the minimum amount of information possible. This resulted in companies withholding information and now they sometimes struggle to determine the cause and target of an attack.

According to the ITCR, *in the U.S. there were an average of 7 breach notices issued each business day in 2022. Compare that to the 356 breach notices issued each day in the European Union during 2021, the last year for which data is available*[576]. This clarifies the importance of legislation in supporting victims of attacks to be transparent for the benefit of society as a whole.

Thales additionally claimed that 32% of the respondents involved in their cloud security study[577] had to issue a breach notification to a government agency, customers, partners or employees, creating substantial concerns on sensitive data. Tenable research confirmed the transparency issue[578], claiming that the disclosure process is time consuming and requires months or years to be completed. Also, the variety of laws and reporting requirements might inhibit reporting.

7.6 CLOUD COMPUTING AND DATA BREACHES

The continuous and inexorable migration of services and data to the cloud requires a careful consideration of data breach attacks in the cloud[579] [580] [581]. In addition, Thales notes that multi-cloud is growingly becoming the norm and must be carefully considered[582].

According to the 2022 Thales Cloud Security Report[583], 66% of interviewed organisations store 21% to 60% of their sensitive data in the cloud. Also, 75% of organisations claimed that more than 40% of their sensitive data are stored in the cloud[584]. While the cloud is commonly considered a secure environment, 45% of the 2,800 respondents claimed a data breach or failed an audit involving data and applications in the cloud; 35% was reported in 2021. These numbers may be due to the increasing adoption and complexity of cloud computing solutions (e.g. multi-cloud adoption by almost 79% of respondents)[585], as well as an increasing focus of cybercriminals on cloud infrastructures and platforms.

In this context, Tenable Research, in its threat landscape report[586], identified cloud misconfiguration as one of the most relevant causes of data breaches. Both Microsoft and Amazon reported data breaches of sensitive customer information due to misconfigurations of their environments. For example, Microsoft disclosed a notice on a

[572] https://www.idtheftcenter.org/post/2022-trends-in-identity-report-most-contacts-about-compromised-identities-victims-google-voice-scam/#:~:text=In%202022%2C%20the%20ITRC%20had,than%20one%20(1)%20percent.
[573] https://www.idtheftcenter.org/post/identity-theft-resource-center-2022-consumer-impact-report-reveals-effects-social-media-account-takeover/.
[574] https://www.ftc.gov/news-events/news/press-releases/2023/02/new-ftc-data-show-consumers-reported-losing-nearly-88-billion-scams-2022.
[575] 2022 ITRC Annual Data Breach Report.
[576] 2022 ITRC Annual Data Breach Report.
[577] 2022 Thales Cloud Security Study: The Challenges of Data Protection in a Multicloud World.
[578] Tenable Research, TENABLE 2022 THREAT LANDSCAPE REPORT A guide for security professionals to navigate the modern attack surface.
[579] 2022 Thales Cloud Security Study: The Challenges of Data Protection in a Multicloud World.
[580] Tenable Research, TENABLE 2022 THREAT LANDSCAPE REPORT A guide for security professionals to navigate the modern attack surface.
[581] Seqrite, 2023 Cybersecurity Trend Forecast.
[582] Thales, 2023 Data Threat Report: Global Edition.
[583] 2022 Thales Cloud Security Study: The Challenges of Data Protection in a Multicloud World.
[584] Thales, 2023 Data Threat Report: Global Edition.
[585] Thales, 2023 Data Threat Report: Global Edition.
[586] Tenable Research, TENABLE 2022 THREAT LANDSCAPE REPORT A guide for security professionals to navigate the modern attack surface.

misconfigured and unsecured Azure endpoint that could be exploited to access the business transaction data of Microsoft and its customers[587]. Amazon also experienced a data security incident due to an unsecured Elasticsearch database (215+ million entries), which allowed Amazon Prime users to view data[588].

7.7 DATA ATTACKS ON MACHINE LEARNING

Machine Learning (ML) models are at the core of modern distributed systems and are increasingly becoming targets of malicious attacks[589]. Trustworthy and high-quality data are a pre-requisite for implementing safe autonomic and adaptive systems. The risks introduced by malicious data manipulation in general, and data poisoning and adversarial attacks in particular, raise[590] serious concerns. As already discussed in ETL 2022, data poisoning and adversarial attacks become fundamental threats to data-driven systems where data integrity is not the only property to be protected and guaranteed but includes data provenance, non-repudiation and accountability which should be supported, all backed by data quality and guarantees of trustworthiness.

According to various research works[591] [592] [593], machine learning models can be attacked by poisoning the data used for training the models. Poisoning attacks are training-time attacks that inject poisoned data points into the training set [594]. They aim to reduce the accuracy of the model (and in turn of the overall system) or cause the misclassification of specific data points at inference time[595]. The resulting model will then learn a behaviour that is different from the real behaviour of the target system, forcing the latter to take wrong decisions. The danger of data poisoning is well-known today.

This was also predicted in 2021 when Johannes Ullrich, Dean of Research at SANS Technology institute said at RSA: 'One of the most basic threats when it comes to machine learning is one of the attackers actually being able to influence the samples that we are using to train our models'[596]. Mark Greisinger also remarked that: 'Data poisoning attacks, which exploit machine learning and AI by tainting training data for criminal ends, are widely considered to be the next big cybersecurity threat'[597]. Researchers from Google, ETH Zurich, NVIDIA, and Robust Intelligence recently demonstrated a poisoning attack where poisoned data are added in web-scale datasets used to train the largest machine-learning models[598] [599]. In 2016, Microsoft AI-enabled chatbot Tay was targeted by internet trolls that launched a coordinated data-poisoning attack. Tay's learning mechanism based on retraining caused Tay to tweet inappropriate content[600].

In addition to data poisoning, adversarial attacks are also growing and represent a major threat in ML/AI domains[601]. They can occur at specially-crafted data points causing faulty or wrong inference. Their goal is to confuse ML models in misclassifying such data points[602], substantially affecting their ability to support sound and effective decision-making. In this context, a collaboration between Microsoft and MITRE resulted in the development of Arsenal, a tool to prepare security teams against adversarial attacks on ML systems[603]. It is an automated adversarial attack library, which allows security practitioners to emulate, with low ML/AI knowledge, attacks on systems that contain ML.

Finally, model stealing or extraction aims to reconstruct a black-box model or extract data from it[604]. In this context, membership inference attacks aim to recover the training set from a deployed ML model. A fundamental work in 2017

[587] https://www.thestack.technology/microsoft-data-breach-azure-bluebleed/
[588] https://techcrunch.com/2022/10/27/amazon-prime-video-server-exposed/
[589] Deliverable D4.3, EU H2020 project CONCORDIA, https://www.concordia-h2020.eu/wp-content/uploads/2022/07/CONCORDIA-D4.3.pdf.
[590] https://securityintelligence.com/articles/data-poisoning-ai-and-machine-learning/.
[591] https://www.concordia-h2020.eu/wp-content/uploads/2020/06/D4.1_Ready_for_Submission_D4.1-final_revised.pdf.
[592] https://arxiv.org/abs/2007.07646.
[593] https://www.nature.com/articles/s42256-021-00390-3
[594] https://www.concordia-h2020.eu/wp-content/uploads/2020/06/D4.1_Ready_for_Submission_D4.1-final_revised.pdf.
[595] https://arxiv.org/abs/2209.14013.
[596] https://securityintelligence.com/articles/data-poisoning-big-threat/.
[597] https://netdiligence.com/blog/2023/03/understanding-data-poisoning-attacks/.
[598] https://www.zdnet.com/article/the-next-big-threat-to-ai-might-already-be-lurking-on-the-web/.
[599] https://arxiv.org/abs/2302.10149.
[600] https://www2.deloitte.com/us/en/insights/industry/public-sector/adversarial-ai.html.
[601] https://venturebeat.com/2021/05/29/adversarial-attacks-in-machine-learning-what-they-are-and-how-to-stop-them/.
[602] https://www2.deloitte.com/us/en/insights/industry/public-sector/adversarial-ai.html.
[603] https://www.helpnetsecurity.com/2023/03/03/microsoft-mitre-plug-in/.
[604] https://venturebeat.com/2021/05/29/adversarial-attacks-in-machine-learning-what-they-are-and-how-to-stop-them/.

allowed the presence of a specific data point in the training set to be inferred by examining model predictions only[605]. This attack was later executed on large models[606], introducing major privacy and economic risks.

7.8 THE SURGE OF AI CHATBOTS

The disruptive impact and the exponential adoption of generative artificial intelligence chatbots such as OpenAI ChatGPT, Microsoft Bing and Google Bard, all built around data sharing and analysis, are changing the way in which we work, live and play[607].

AI chatbots and language models require huge amounts of data to be properly trained and achieve high-quality data generation. Thus, they are becoming a preferred target for cybercriminals as they are very susceptible to data poisoning[608] [609].

Florian Tramèr, one of the researchers demonstrating poisoning attacks on 10 popular data sets,[610] including LAION, FaceScrub and COYO, has claimed that 'The large machine-learning models that are being trained today—like ChatGPT, Stable Diffusion or Midjourney—need so much data to [train] that the current process of collecting data for these models is just to scrape a huge part of the Internet'. This poses huge challenges in quality control especially on text-based machine learning. Tramèr continued claiming: 'Where I see the biggest incentive, and the biggest risk, is once we start using these text models in applications like search engines. Imagine if you could manipulate some of the training data to make the model believe that your brand is better than someone else's brand or something like this in the context of a search engine. There could be huge economic incentives to do this'[611].

AI chatbots are also becoming targets of data breach attacks. For instance, ChatGPT was the victim of a data breach where some user payment information may have been released to other users[612]. On the other side, they can be powerful weapons in the hands of cybercriminals who can use them to spread manipulated information, deepfakes, poisoned data and phishing[613]. The disruptive adoption of generative AI and AI chatbots is rapidly changing the threat landscape, where the ability to detect AI-generated content or AI-based interaction becomes a matter of urgency. AI detection tools will have the critical role of being the last barrier protecting people who are unable to distinguish a true fact from a false one[614].

This new scenario poses a new wave of risks that require global cooperation and discussions on inclusive AI governance, as stressed during the last G7 summit[615]. Also, one hundred top experts recently released a 'statement on AI risk', warning about the risk of extinction from AI[616]. In response to this, the EU has put forward a proposal to regulate AI – the so called 'AI Act'[617]. The proposal has a risk-based approach that evaluates, among other criteria, the risks posed by AI systems to health and safety or the fundamental rights of natural persons and imposes obligations accordingly. Other countries, such as China and the USA, are also working on regulating AI[618] [619].

The need for tools to counteract AI-generated disinformation in the age of ChatGPT is becoming a necessity[620].

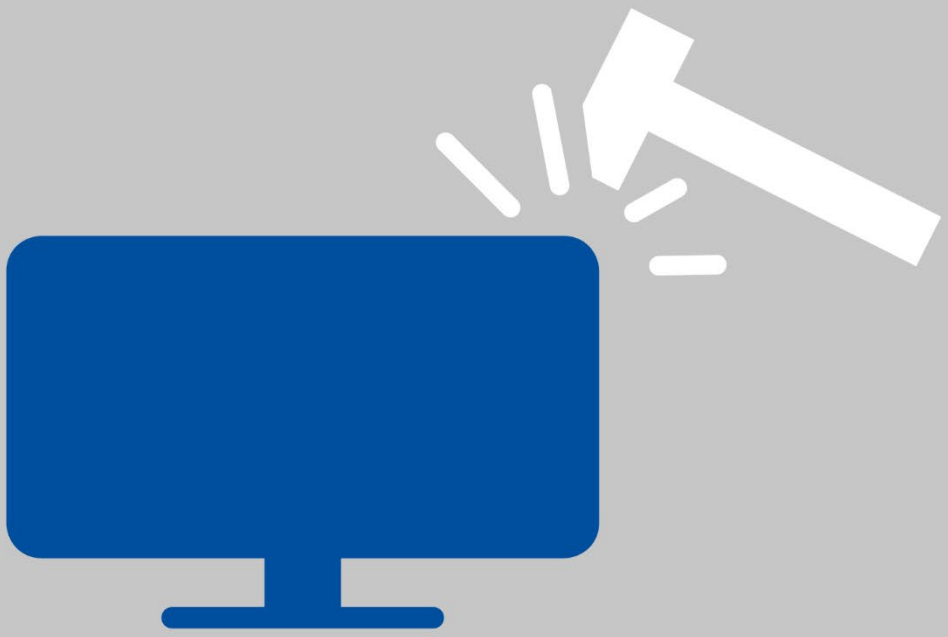
7.9 ADDITIONAL TRENDS

- According to Tenable, 2.29 billion records were exposed in 2022 in data breaches[621].

[605] R. Shokri, M. Stronati, C. Song, V. Shmatikov. 'Membership Inference Attacks Against Machine Learning Models', in Proc. of IEEE S&P 2017, San Jose, CA, USA, May 2017.
[606] N. Carlini, F. Tramèr, E. Wallace, M. Jagielski, A. Herbert-Voss, K. Lee, A. Roberts, T. Brown, D. Song, Ú. Erlingsson, A. Oprea, C. Raffel. 'Extracting Training Data from Large Language Models', in Proc. of USENIX 2021, Virtual, August 2021.
[607] https://www.zdnet.com/article/chatgpt-vs-bing-chat-vs-google-bard-which-is-the-best-ai-chatbot/.
[608] https://towardsdatascience.com/exploring-the-vulnerability-of-language-models-to-poisoning-attacks-d6d03bcc5ecb.
[609] https://www.economist.com/science-and-technology/2023/04/05/it-doesnt-take-much-to-make-machine-learning-algorithms-go-awry.
[610] https://arxiv.org/abs/2302.10149.
[611] https://spectrum.ieee.org/ai-cybersecurity-data-poisoning.
[612] https://www.cshub.com/data/news/openai-confirms-chatgpt-data-breach.
[613] https://securityintelligence.com/articles/chatgpt-and-the-race-to-secure-your-intellectual-property/.
[614] https://gizmodo.com/chatgpt-ai-12-companies-deepfake-video-image-detectors-1850480813.
[615] https://www.consilium.europa.eu/en/press/press-releases/2023/05/20/g7-hiroshima-leaders-communique/.
[616] https://www.safe.ai/statement-on-ai-risk#open-letter.
[617] https://digital-strategy.ec.europa.eu/en/policies/european-approach-artificial-intelligence.
[618] https://carnegieendowment.org/2023/07/10/china-s-ai-regulations-and-how-they-get-made-pub-90117.
[619] https://www.whitehouse.gov/ostp/ai-bill-of-rights/.
[620] https://gizmodo.com/chatgpt-ai-12-companies-deepfake-video-image-detectors-1850480813.
[621] Tenable Research, TENABLE 2022 THREAT LANDSCAPE REPORT A guide for security professionals to navigate the modern attack surface.

- ITRC noted that supply chain attacks were increasing in 2022 with more than 10 million victims and 1 700 targeted entities[622].
- According to the ITRC, name, full SSN, date of birth, current home address and driver licence or state ID number are the top five attributes of data breaches[623].
- Tenable found that over 3% of data breaches disclosed in 2022 were due to an unsecured database, with over 800 million records exposed[624].
- Breach of data or customers data is the most common motivation behind phishing attacks[625] according to Proofpoint.
- Acronis in its *End-of-Year Cyberthreats Report* claims that the average cost of a data breach will go beyond $5 Million in 2023[626].
- According to IBM, the mean or average time to identify and contain a data breach was 277 days in 2022, a decrease of 10 days with respect to 2021, including 207 days for breach identification and 70 days for breach containment.
- AI is increasingly being adopted as an attack vector and is a dangerous source of attacks. For instance, AI can be used to find vulnerabilities on a target system or used as an infiltration tool[627] [628].
- Russia, the US and Taiwan are in the first three spots for the number of accounts leaked in Q1 2023[629] notes Surfshark. By comparison, Russia, the US and France were the first three in the ranking in 2022[630]. These numbers show a clear link between data breaches and hacktivism.

[622] 2022 ITRC Annual Data Breach Report.
[623] 2022 ITRC Annual Data Breach Report.
[624] Tenable Research, TENABLE 2022 THREAT LANDSCAPE REPORT A guide for security professionals to navigate the modern attack surface.
[625] Proofpoint, 2023 State of the Phish: An in-depth exploration of user awareness, vulnerability and resilience.
[626] https://www.globenewswire.com/news-release/2022/12/19/2576273/0/en/Acronis-End-of-Year-Cyberthreats-Report-Finds-Average-Cost-of-Data-Breaches-Expected-to-Surpass-5-Million-Per-Incident-in-2023.html.
[627] https://www.unite.ai/how-hackers-are-wielding-artificial-intelligence/.
[628] Experian 2023 Data Breach Industry Forecast.
[629] https://surfshark.com/research/study/data-breach-statistics-2023-q1.
[630] https://surfshark.com/blog/data-breach-recap-2022.



8. THREATS AGAINST AVAILABILITY: DENIAL OF SERVICE

Availability is the target of a plethora of threats and attacks, among which Distributed Denial of Service (DDoS) stands out.

Distributed Denial of Service (DDoS) targets system and data availability and, though it is not a new threat (it celebrated its 20th anniversary in 2019), it plays a significant role in the cybersecurity threat landscape[631] [632]. Attacks occur when users of a system or service are not able to access relevant data, services or other resources. This can be accomplished by exhausting the service and its resources or by overloading the network infrastructure[633].

DDoS attacks can be built on web-based attacks, which are often distributed through web applications and use cloud-edge continuum as a primary threat vector. For instance, web-based attacks can be adopted to build a botnet on the cloud that is then used to carry out a denial-of-service attack aimed at making a system unavailable[634].

In the last few years, COVID-19 first and Russia's invasion of Ukraine after that substantially modified the threat landscape and all of society, with an increase in state-sponsored attacks and in attacks on the critical infrastructures of countries, as a fifth dimension of the war. The year 2022 saw a return of the hacktivist (with political motivations), which went beyond the Russia-Ukraine conflict and embraced other 'conflicts' including Taiwan-China[635] and USA-Israel-Iran[636]. In this context, defence mechanisms and strategies increased their robustness and ability to counteract attacks at unprecedented rates, while malicious actors and groups demonstrated an impressive ability in advancing their technical skills and adapting better to the new norm.

As already observed in ETL2022, Ransom Denial of Service (RDoS) attacks continue to have an important impact and combine the dangers of a traditional DDoS, while substantially reducing the need for resources to carry out an attack. Groups of cybercriminals (e.g. Fancy Bear, Cozy Bear, Lazarus Group, Armada Collective, Phantom Squad and REvil) analyse target businesses to find those with weak and vulnerable systems[637]. They then threaten these businesses by sending a letter of extortion demanding a ransom to not attack the system[638] [639]. The simplicity of RDoS attacks and extortion tools built on DDoS-as-a-Service (aka DDoS-for-Hire) are the basis for the adoption of RDoS[640]. Thanks to DDoS-as-a-Service, in fact, launching a RDoS attack is increasingly simple while it is still difficult to spot its origin. Spreading malware or ransomware instead requires an important effort in terms of time and planning[641].

In this reporting period, a significant upsurge in Distributed Denial of Service (DDoS) incidents became apparent with the turn of the year, as depicted in Figure 36. This increase can be attributed to the growing influence of hacktivism among groups opposing various regimes and the ongoing geopolitical tensions worldwide, which have intensified this trend on a larger scale.

[631] Federal Office for Information Security (BSI), The State of IT Sec in Germany, September 2020.
[632] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020.
[633] CISA, Understanding Denial-of-Service Attacks, November 2019. https://www.uscert.gov/ncas/tips/ST04-015.
[634] ENISA Threat Landscape 2022.
[635] CrowdStrike, 2023 GLOBAL THREAT REPORT.
[636] https://www.akamai.com/resources/research-paper/the-evolution-of-ddos-return-of-the-hacktivists.
[637] https://www.radware.com/security/threat-advisories-and-attack-reports/ransom-denial-of-service-rdos-2022/.
[638] Sergiu Gatlan, 'FBI: Thousands of orgs targeted by RDoS extortion campaign,' September 2020, https://www.bleepingcomputer.com/news/security/fbi-thousands-of-orgs-targeted-by-rdos-extortion-campaign/.
[639] CloudBric, DDoS Extortion Campaigns (Ransom DDoS, or RDoS) To Watch Out For, https://www.cloudbric.com/blog/2020/11/ddos-rdos-extortion-ransomware-campaign/.
[640] https://www.networkcomputing.com/network-security/ransom-ddos-phenomenon-pay-or-get-knocked-offline.
[641] Neustar Security, Cyber Threats & Trends: Securing Your Network Pandemic-Style, 2020, https://www.cdn.neustar/resources/whitepapers/security/neustar-cyber-threats-trends-2020-report.pdf.

From a regional perspective, a notable finding is that a higher proportion of DDoS attacks were directed at European Union (EU) member states as demonstrated in Figure 37.

Figure 36: Time series of major Incidents observed by ENISA (July 2022-June 2023)

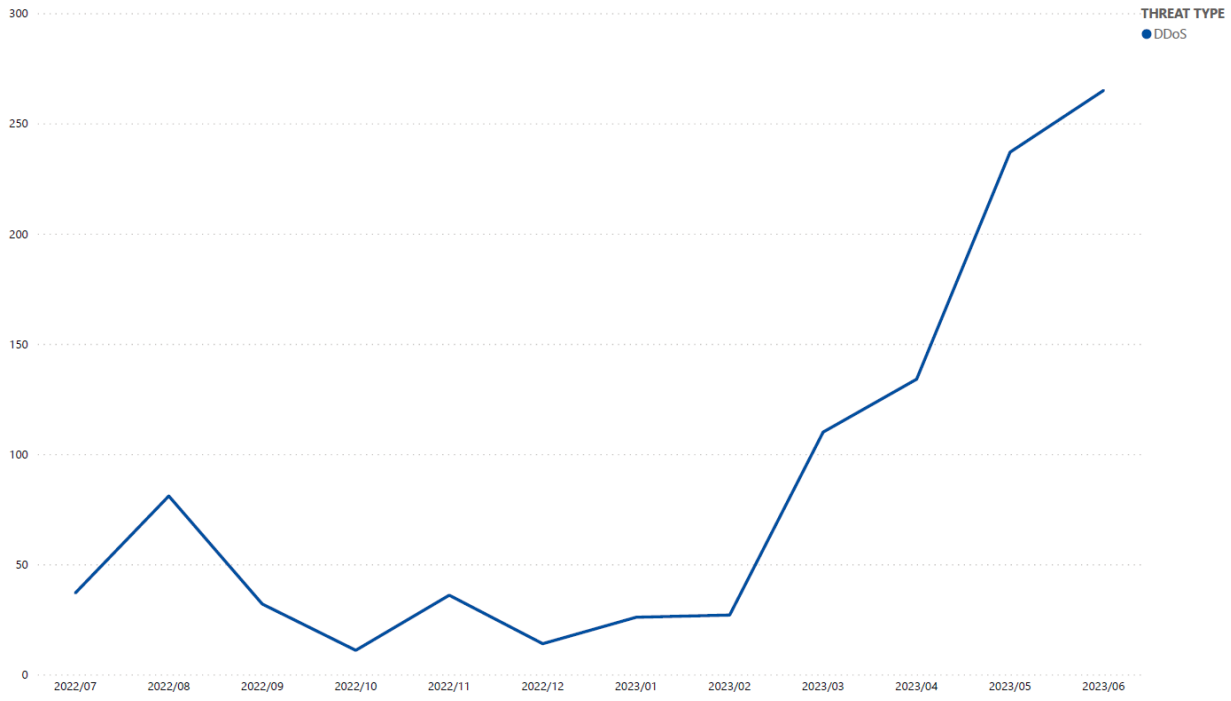
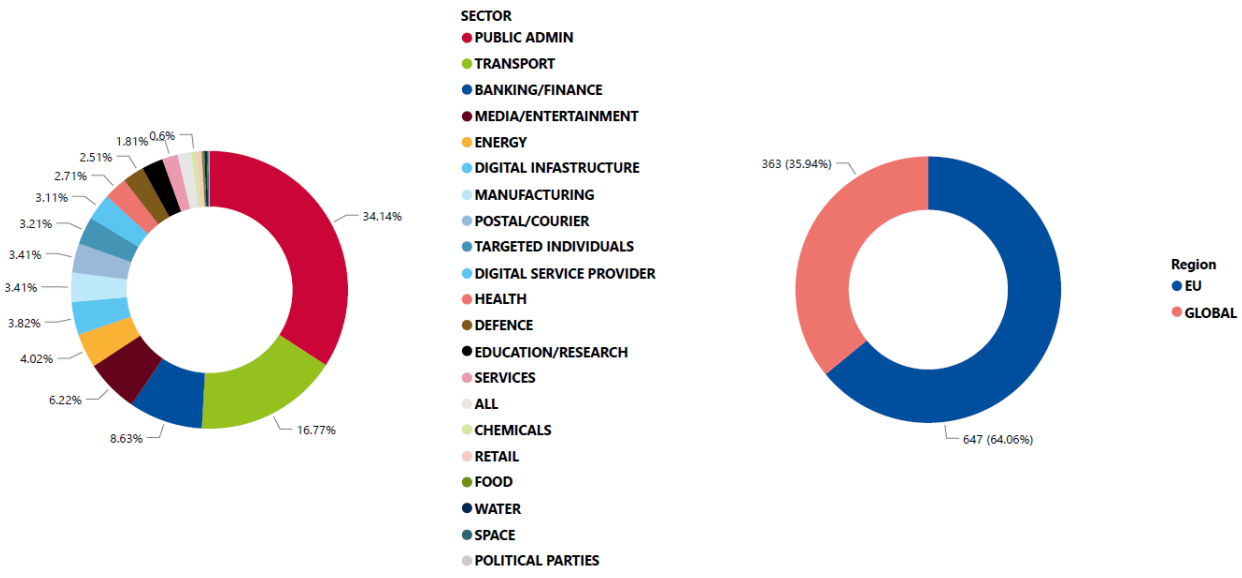


Figure 37: Break down of Sectors by threat type and region



DDoS is one of the most common and recurring threat to IT systems as it targets their availability by exhausting resources and causes decreased performance, loss of data and service outages[642]. In the last couple of years, DDoS moved to mobile and sensor-based scenarios, embracing the cloud-edge continuum, where the availability of devices and sensors have become the preferred target of attack due to their limited resources (e.g. battery). DDoS attacks have maintained a stable form over the years, though some interesting points on their evolution may be noted.

We recall that, in 2022, while the COVID-19 pandemic still had an important impact on DDoS, Russia's invasion of Ukraine monopolised and influenced DDoS like never before. DDoS threats finally become the fifth dimension of warfare, following battles across air, sea, land and even space[643]. During 2022-2023, this trend was reinforced with the comeback of hacktivism. As we observed in 2021-2022, the levels of threats and extortion exploded, moving DDoS towards being state-sponsored attacks. In this context, cloud computing was increasingly used both as a threat vector for DDoS attacks on one hand and as a primary target of the attacks on the other hand[644]. During 2022-23, the trend in the increasing number of DDoS attacks continued, as well as the movement towards application layer (OSI Layer 7[645]) attacks. In addition, DDoS is increasingly being used as a smokescreen,z to cover other types of attacks.

8.1 ATTACKS ARE GETTING LARGER AND MORE COMPLEX, AND MORE INEXPENSIVE

The trend in the increasing complexity of DDoS attacks was also confirmed this year. According to Netscout 'Attackers are constantly innovating and adapting new techniques, including the use of server-class botnets, DDoS-for-Hire services and an increased use of direct-path attacks that continually perpetuate the advance of the threat landscape'[646]. Also in 2022, the availability of DDoS tools, often developed for politically-motivated attacks, increased the strength and duration of financially-motivated attacks[647] [648] [649].

DDoS-for-Hire allows large-scale attacks to be launched by unskilled users having access to DDoS services. Providers can launch attacks on their clients' behalf or provide tools for launching them[650]. DDoS-for-Hire combined with the simplicity of building botnets thanks to the availability of a multitude of insecure devices is a perfect mix for implementing large and disruptive attacks. Larger volumes with greater intensity are pushing the scenario to its extreme[651]. The dimension of the problem is also demonstrated by the efforts undertaken in trying to limit DDoS-for-Hire. Europol announced in December 2022 that a joint international law enforcement operation had taken control of about 50 sites that were offering DDoS-for-Hire services to threat actors. The operation called Power Off involved law enforcement from the USA, the UK, the Netherlands, Poland and Germany[652].

Attacks are increasing both in terms of size and complexity with respect to the previous year[653] [654], reaching 13 million attacks worldwide[655]. According to Cloudfare[656], larger, longer lasting volumetric attacks surged with an increasing number of attacks over 100Gbps and lasting more than three hours. Multiple attacks have been observed exceeding 1Tbps, with the largest attack observed by Cloudfare peaking at 2.5Tbps[657]. The latter was based on a Mirai botnet variant and aimed at the Minecraft server Wynncraft and was implemented by a multi-vector attack consisting of UDP and TCP floods. According to StormWall[658], the number of DDoS attacks globally saw a 74% increase in 2022, reaching a rate limit of 2Tbps and up to three days in duration. Also, Akamai observed the largest application layer

642 H2020 EU Project CONCORDIA, Deliverable D4.1 - 1st year report on cybersecurity threats, https://www.concordia-h2020.eu/wp-content/uploads/2020/06/D4.1_Ready_for_Submission_D4.1-final_revised.pdf.
643 Vova Kamenker, DDoS Threats: The Fifth Dimension of Warfare, September 2021, https://blog.mazebolt.com/ddos-threats-the-fifth-dimension-of-warfare.
644 Tom Emmons. 2021: Volumetric DDoS Attacks Rising Fast, March 2021, https://blogs.akamai.com/2021/03/2021-volumetric-ddos-attacks-rising-fast.html.
645 OSI Model https://en.wikipedia.org/wiki/OSI_model.
646 https://www.rcrwireless.com/20220322/internet-of-things/netscout-nearly-10-million-ddos-attacks-in-2021.
647 https://www.infosecurity-magazine.com/blogs/2022-ddos-yearinreview/.
648 Microsoft Digital Defense Report 2022.
649 Insikt Group, THREAT ANALYSIS 2022 Annual Report.
650 Microsoft Digital Defense Report 2022.
651 https://www.akamai.com/resources/research-paper/the-evolution-of-ddos-return-of-the-hacktivists.
652 Cyber Security Brief (December 2022), January 3, 2023 - Version: 1.0, TLP: CLEAR.
653 https://blog.cloudflare.com/ddos-threat-report-2022-q3/.
654 https://blog.cloudflare.com/ddos-threat-report-2022-q4/.
655 https://www.netscout.com/threatreport/ddos-threat-intelligence-report/#netscout-visibility.
656 https://blog.cloudflare.com/ddos-threat-report-2022-q4/.
657 https://www.akamai.com/resources/research-paper/the-evolution-of-ddos-return-of-the-hacktivists.
658 https://www.infosecurity-magazine.com/blogs/2022-ddos-yearinreview/.

attack at 46 million requests per second against Google Cloud[659] and the largest attack on a European firm at 704.8 mega-packets per second[660].

Despite the increasing trend in size and complexity, Microsoft observed that most of the attacks (89%) had short durations (less than an hour) and 26% lasted between one and two minutes. In 2022, Microsoft mitigated 1 435 attacks a day, with a max 2 215 attacks on 22 September 2022 and a minimum of 680 attacks on 22 August 2022. The total of mitigated attacks was 520,000 during the entire year of 2022. Again, current trends show that DDoS attacks are becoming more frequent, more sophisticated and more inexpensive to launch.

According to F5Labs[661], during 2022 volumetric attacks account for a major part of large attacks (1gbps and 10gbps), protocol and application attacks fall into a lower band (100mbps-1gbps), while multi-vector attacks are more scattered. F5 predicts DDoS attacks will likely grow in the future, a trend that have been already observed by DDoS Guard[662].

8.2 DDOS ATTACKS ARE INCREASINGLY BUILT ON IOT DEVICES

ETL2021 and ETL2022 observed: '**Traditional DDoS is moving towards mobile networks and IoT.** Sensors and devices are in fact a suitable target of DDoS attacks due to their limited resources that often result in poor security. Devices are simple to corrupt, often coming with misconfigurations (e.g. weak passwords)[663]. At the same time, the increasing complexity of these mobile systems make the shortage of the users' security skills increasingly relevant. In this context, DDoS aims to threaten the availability of components as well as to disrupt the operation of other networks or systems but they also have the potential to threaten the safety of the users. The increasing number of devices and applications connected to the cloud gives adversaries a larger playing field on which to target attacks.'

This trend is confirmed also in this last reporting period by Microsoft that notes that DDoS attacks consistently used IoT devices[664]. Several attacks adapted existing malware (e.g. Mirai) and botnets to involve IoT[665]. Mirai has been used to launch state-sponsored attacks, showing its ability to adapt to changing environments and IoT devices. New botnets have been defined, such as Zerobot and MCCrash; these are extending the threat landscape in the context of IoT malware[666].

It is important to note that, according to Cloudfare in 2023 Q1, hyper-volumetric DDoS attacks were increasingly leveraged on botnets based on virtual private servers rather than a multitude of IoT devices[667]. Fewer devices but more powerful!

8.3 DDOS AND CYBERWARFARE: THE RETURN OF THE HACKTIVIST

2022 was the year of the return of the hacktivist[668]. The DDoS landscape was initially affected by the geopolitical changes introduced by Russia's invasion of Ukraine on 24 February 2022, which then affected the entire reporting period last year[669]. A significant part of the DDoS-related attacks concerned this event and involved actors at different layers, from state-sponsored to simple users, devoting their resources to the cyberwar.

This year the trend continued and strengthened. Hacktivism however targeted not only the Russia-Ukraine conflict, but also other areas such as Taiwan-China[670] and US-Israel-Iran[671] [672]. A range of DDoS attacks causing outages was launched in August 2022 ahead of former US House Speaker Nancy Pelosi's arrival in Taiwan[673] [674]. According

[659] https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps.
[660] https://www.akamai.com/resources/research-paper/the-evolution-of-ddos-return-of-the-hacktivists.
[661] https://www.f5.com/labs/articles/threat-intelligence/2023-ddos-attack-trends.
[662] https://ddos-guard.net/en/blog/ddos-attack-trends-2022.
[663] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020.
[664] Microsoft Digital Defense Report 2022.
[665] SONICWALL CYBER THREAT REPORT 2023 CHARTING CYBERCRIME'S SHIFTING FRONTLINES.
[666] https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights/.
[667] https://blog.cloudflare.com/ddos-threat-report-2023-q1/.
[668] https://www.akamai.com/resources/research-paper/the-evolution-of-ddos-return-of-the-hacktivists.
[669] https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights/.
[670] CrowdStrike, 2023 GLOBAL THREAT REPORT.
[671] https://www.akamai.com/resources/research-paper/the-evolution-of-ddos-return-of-the-hacktivists.
[672] Insikt Group, THREAT ANALYSIS 2022 Annual Report.
[673] https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights/.
[674] https://www.imperva.com/resources/resource-library/reports/ddos-threat-landscape-report-2023/

to DDoS Guard[675], hacktivism was the most important motivation for DDoS attacks, though it began chaotically before organising into ideological groups that launched professional attacks.

State-sponsored hacktivism was strongly connected with cyberwarfare and the emergence of new advanced persistent threat groups such as Killnet, Anonymous Sudan and IT Army of Ukraine[676]. Attacks linked to the Russia-Ukraine war continued. Killnet attacked many countries imposing sanctions on Russia and belonging to the NATO alliance, government and private websites belonging to Romania (April), Italy (May), Lithuania (June), Norway (June) and Japan (September), and multiple US-based sites, such as the US Treasury, a financial institution and numerous airports (October and November). CISCO's *Talos 2022 Year in Review* noted that attacks by Killnet were mostly unsophisticated suggesting their intent was more to raise media attention for their cause and distribute Russian propaganda and narratives[677] [678].

8.4 DDOS ATTACKS AS A SMOKESCREEN AND HORIZONTAL ATTACKS

According to Imperva[679], DDoS attacks are increasingly becoming a distracting tactic, which are followed by more impactful attacks. For instance, Imperva observed DDoS attacks followed by Account Takeover attacks (ATO), Bot attacks or attacks on API endpoints to infiltrate sensitive data: '[…] how large service disruptions often came in parallel with other attack vectors, where, whether intentional or not, DDoS was used as a smokescreen to pivot the defending team's attention away from a more sophisticated and precise simultaneous offense, such as ATO (Account Takeover) or phishing'[680]. This scenario often sees DDoS as a decoy for more serious types of attacks such as malware or espionage, increasing business risks impacting reputation, compliance and supply chain operations[681].

On the other hand, attackers are increasingly launching DDoS attacks against multiple unrelated targets at once, rather than selecting a high-value one[682]. This multi-target attack might be more difficult to counteract thus increasing the impact on the target. For example, an attacker can launch multiple DDoS attacks targeting a whole range of IP addresses or a specific organisation's different active services. This type of attack, also known as a **carpet-bombing attack**, increased by 69% in 2022[683] as per Netscout.

8.5 RANSOM DENIAL OF SERVICE (RDOS)

Threat actors continued leveraging **Ransom Denial of Service (RDoS)** to conduct extortion-based DoS attacks that are financially motivated. RDoS aims to identify vulnerable systems that become the target of the attack and put in place different activities that result in a final request to pay a ransom. RDoS can come in two flavours: i) attack first, ii) extort first. Type i) describes a scenario where a DDoS attack is implemented and a ransom is demanded to stop it. Type ii) describes a scenario where an extortionary letter and proof of harm in the form of a small-scale DoS attack is sent with a demand for a ransom. RDoS attacks are even more dangerous than traditional DDoS since they can be completed even if the attacker does not have sufficient resources[684]. RDoS is a complex attack that mixes several approaches and techniques such as denial of service, ransomware, identity spoofing to name just a few[685].

RDoS has moved tactics from double-extortion to quadruple-extortion[686] [687] [688] [689]. In triple-extortion tactics, *threat actors encrypt and steal data, and also threaten to engage in a distributed denial of service (DDoS) attack against the*

[675] https://ddos-guard.net/en/blog/ddos-attack-trends-2022.
[676] The Imperva Global DDoS Threat Landscape Report 2023.
[677] CISCO Talos 2022 Year in review.
[678] Insikt Group, THREAT ANALYSIS 2022 Annual Report.
[679] https://www.the-imperva-global-ddos-threat-landscape-report-2023.
[680] https://www.imperva.com/blog/lift-the-ddos-smokescreen-investigate-underlying-attacks/.
[681] https://www.akamai.com/resources/research-paper/the-evolution-of-ddos-return-of-the-hacktivists.
[682] https://www.akamai.com/blog/security/ddos-attacks-in-2022-targeting-everything-online.
[683] https://www.netscout.com/threatreport/ddos-threat-intelligence-report/.
[684] CloudBric, DDoS Extortion Campaigns (Ransom DDoS, or RDoS) To Watch Out For, https://www.cloudbric.com/blog/2020/11/ddos-rdos-extortion-ransomware-campaign/.
[685] Neustar, Pay Or Else: DDoS Ransom Attacks.
[686] Unit42_Ransomware_Threat_Report_2022_1650614560.
[687] IBM_X_Force_Threat_Intel_Index_2022.
[688] ISSUE 8: FINDINGS FROM 2ND HALF 2021 NETSCOUT THREAT INTELLIGENCE REPORT
[689] The Global Economic Forum, The Global Risks Report 2022 17th Edition, 2022 https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf.

affected organisation[690] [691] [692]. In quadruple extortion attacks,[693] *ransomware cybercriminals extend the range of the attack to business partners and clients to increase pressure on the victim, with the possibility of business disruptions caused by the ransomware attack*. In 2022, RDoS was still at the forefront of denial-of-service attacks. According to Cloudfare, in 2022, an average of 13% of its customers suffered an RDoS attack, a figure that was stable with respect to 2021[694]. This percentage was found by asking Cloudfare customers receiving a DDoS attack whether they had also received a ransom note, and 13% in Q2, 14% in Q3 and 16% in Q4 answered in the affirmative. In 2023 Q1 16% of customers suffering a DDoS attack were the target of an RDoS attack. Also, Akamai agrees on the centrality of ransomware in DDoS attacks[695].

The simplicity of RDoS attacks and extortion tools built on DDoS-as-a-Service (aka DDoS-for-Hire) are the basis for the adoption of RDoS[696]. According to NETSCOUT Security's *Trends to Watch in 2023*[697], RDoS will maintain its importance and be a primary trend in 2023.

8.6 APPLICATION ATTACKS ARE INCREASING

Application attacks have been continuously increasing over the last few years. According to Imperva[698], application attacks increased by an exponential 82%. Application attacks are almost reaching the lead in the number of attacks which are still led by multi-vector attacks. Application attacks usually come with low-bandwidth peaks compared to protocol and volumetric attacks. DNS request flooding was the prime attack vector (93.4%), due to the low resource use of such requests with respect to other vectors such as HTTP GET Flooding.

A prominent pro-Russian hacktivist group known as Killnet launched a sophisticated L7 DDoS attack on a large European organisation. The attack aimed to overwhelm the company's servers with massive amounts of traffic, making it difficult for users to access the website, with attack traffic peaking at 120K RPS[699]. These attacks primarily targeted HTTP/HTTPS protocols and might be evidence of the increasing trends towards web applications L7 attacks[700]. They are difficult to detect and mitigate because they replicate the behaviour of normal users, use multiple vectors and support retooling.

Similar trends were observed by DDoS Guard, along with the important impact of application attacks on the DDoS landscape[701][702]. Netscout noticed a 487% increase in HTTP/HTTPS attacks since 2019, spanning financial, government and media sites[703]. Netscout also noted that *DNS query floods have more than tripled since they really became weaponised in 2019, a 243% increase in the adoption of this attack technique. The average daily attack count for 2022 was approximately 850 attacks, a 67 percent increase over an average of 522 a day in 2021*[704].

According to Imperva[705], the largest application layer DDoS attack in 2022 was a ransom DDOS attack launching 3.9 million requests per second (rps). API DDoS attacks are also becoming a preferred approach[706]. Google counteracted an L7 attack that peaked at 46 million rps[707].

[690] IBM_X_Force_Threat_Intel_Index_2022.
[691] BleepingComputer, 'US and Australia warn of escalating Avaddon ransomware attacks', https:// www.bleepingcomputer.com/news/security/us-andaustralia-warn-of-escalating-avaddon-ransomwareattacks/, 2021.
[692] Insikt Group, THREAT ANALYSIS 2022 Annual Report.
[693] The Global Economic Forum, The Global Risks Report 2022 17th Edition, 2022. https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf.
[694] https://blog.cloudflare.com/ddos-threat-report-2022-q4/.
[695] https://www.akamai.com/resources/research-paper/the-evolution-of-ddos-return-of-the-hacktivists.
[696] https://www.networkcomputing.com/network-security/ransom-ddos-phenomenon-pay-or-get-knocked-offline.
[697] https://www.netscout.com/blog/security-trends-watch-2023.
[698] https://www.imperva.com/blog/imperva-releases-its-global-ddos-threat-landscape-report-2023/.
[699] https://www.f5.com/company/blog/f5-distributed-cloud-services-stands-up-to-l7-ddos-attacks.
[700] https://www.f5.com/labs/articles/threat-intelligence/2023-ddos-attack-trends.
[701] https://ddos-guard.net/en/blog/ddos-attack-trends-2022.
[702] https://ddos-guard.net/info/protect?id=40954.
[703] https://www.netscout.com/threatreport/ddos-threat-intelligence-report/.
[704] https://www.netscout.com/threatreport/ddos-threat-intelligence-report/.
[705] https://www.imperva.com/blog/imperva-releases-its-global-ddos-threat-landscape-report-2023/.
[706] https://www.imperva.com/resources/resource-library/reports/ddos-threat-landscape-report-2023/
[707] https://cloud.google.com/blog/products/identity-security/how-google-cloud-blocked-largest-layer-7-ddos-attack-at-46-million-rps.

8.7 TCP VS UDP ATTACKS

2022 saw a sharp increase in TCP-based attacks reaching the first spot of the ranking according to Microsoft[708]. Microsoft noted that TCP attacks were the most frequent DDoS attacks at 63% of all attack traffic in 2022. Still, UDP accounted for a significant portion of attack traffic at 22% of all attacks, combining UDP flood and amplification attacks.

Akamai confirmed an important trend on TCP, i.e. identifying port 443 as the most targeted, followed by port 80. Other ports of interest for TCP/UDP attacks were port 4500 (IPSEC/VPN), port 22 (SFTP) and port 53 (DNS).

Netscout stated that four out of five attack vectors are TCP based (i.e. TCP ACK, TCP SYN, TCP SYN/ACK Amp, TCP RST). Direct path attacks complement volumetric DDoS attacks in causing disruption. TCP direct-path attacks have increased by 18% since 2020, while reflection/amplification attacks decreased by the same amount, a difference of 2 million attacks[709].

8.8 THE CLOUD AND DDOS

As discussed in ETL2022, the rapid adoption of the cloud and its movement towards edge computing increased the attack surface and the opportunity for cybercriminals[710]. This migration has been further boosted by remote working, online education, business resilience and environmental sustainability caused by COVID-19. The price we pay for such convenience is an increased risk of DDoS attacks targeting cloud resources.

A new attack called Denial of Wallet (DoW) was observed during the last year. Similar to DDoS, which aims to cause disruption by shutting a target down, DoW aims to cause financial disruption by targeting cloud-based infrastructures and serverless computing[711]. There is currently no bulletproof countermeasure against DoW.

On the other hand, the cloud is a powerful tool in the hands of cybercriminals who can benefit from highly scalable and reliable command-and-control infrastructures and botnets[712]. In 2022, F5Labs launched Distributed Cloud Services which was used to counteract several attacks on web applications and APIs, and increase security at the edge[713]. A variety of defences are used such as traffic filtering, IP intelligence and rate limiting on one hand, and real-time threat intelligence and L7 DDoS auto-mitigation capabilities on the other hand. Within Distributed Cloud Services, F5 Distributed Cloud DDoS Mitigation protects against L3-L7 attacks on enterprises and hosting service providers[714].

The cloud is the hosting infrastructure for many DDoS Protection Providers such as for instance Cloudflare, Akamai, Project Shield and AWS Shield to name but a few.[715]

8.9 DDOS ATTACKS SPREAD

8.9.1 Geographical Spread

The geographical spread of DDoS attacks in 2022, as analysed in StormWall's *DDoS Year-in-Review* report, indicates that the USA (18.3%) and China (10.7%) confirm the trends of past years and are at the top of the ranking as target countries of DDoS attacks, followed by India, Russia, and the UK[716].

[708] David Warburton, 2022 Application Protection Report: DDoS Attack Trends, March 2022, https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-ddos-attack-trends.
[709] https://www.netscout.com/threatreport/ddos-threat-intelligence-report/.
[710] Accenture-2021-Cyber-Threat-Intelligence-Report fornito da ENISA.
[711] https://portswigger.net/daily-swig/denial-of-wallet-attacks-how-to-protect-against-costly-exploits-targeting-serverless-setups.
[712] Accenture-2021-Cyber-Threat-Intelligence-Report Volume 2, https://www.accenture.com/_acnmedia/PDF-173/Accenture-Cyber-Threat-Intelligence-Report-Vol-2.pdf.
[713] https://www.f5.com/company/blog/f5-distributed-cloud-services-stands-up-to-l7-ddos-attacks.
[714] https://www.f5.com/pdf/solution-overview/f5-distributed-cloud-ddos-mitigation.pdf.
[715] https://www.enterprisenetworkingplanet.com/security/best-ddos-protection-services/.
[716] https://www.infosecurity-magazine.com/blogs/2022-ddos-yearinreview/.

In 2022-2023, Cloudfare analysed the geographical spread of DDoS attacks distinguishing between the application (L7) and network/transport (L3/L4) layers. In Q3 2022 and Q1 2023 [717], they calculated the percentage of attack traffic in a given country divided by the total traffic worldwide with the following results[718] [719] [720].

- **Application Layer (L7):** In Q3 2022, US and China were as usual in the top spots as both targets (US first and China second) and sources (US third and China first) of application-layer attacks. India took the second position as a source country. Ukraine saw an increase of 67% Quarter on Quarter and a decrease of 50% YoY as a target country, while Russia saw an increase of 31% QoQ and of 2,400% YoY. They both saw a decrease as a source of attack QoQ and an increase YoY. In Q1 2023, the USA took the second spot as an attack target and first spot as an attack source, while Israel takes the lead ('perhaps related to judicial reform and the counter protests, or the ongoing tensions in the West bank'[721]) as attack targets and China the second spot as attack sources. In absolute volumes, the most HTTP DDoS attack traffic (source) came from the USA, followed by China and Germany. Germany, Brazil and Russia appear in most of the top-ten rankings.
- **Network Layer (L3):** In Q3 2022, Singapore (15.3%) and the USA (8.4.%) were in the top two spots as targets of network-layer attacks, with China in third position with only 2.1%. Azerbaijan, Tunisia, Zimbabwe, Germany and South Korea showed the highest percentage of DDoS attack traffic (19%+). In Q1 2023, the same three positions with regards to Q3 2022 as target countries were occupied by the same countries but in a different order: China (17.9%), Singapore (17.3%) and the USA (4.2.%). Germany, Taiwan and South Korea appear in most of the top-ten rankings.

8.9.2 Industrial Sector Spread

F5Labs observed that technology reached first spot as the most attacked industrial sector with almost 35% of attacks, while the finance, banking and insurance sectors came in second with over 30% of attacks. Government and education reached the third (>15%) and fourth (<5%) spots respectively[722]. When the attacks were divided by DDoS type, F5Labs found that volumetric attacks were consistent among the various sectors except for education. Multi-vector and application attacks accounted for most of the attacks, showing similar trends as the technology and finance, banking and insurance sectors. The finance, banking and insurance sectors were mostly targeted by application attacks. This is due to attackers aiming to deny access to services or to increasingly effective defences against volumetric and protocol attacks. Multi-vector attacks are massive in the education sector.

Cloudfare also analysed the spread in the industrial sector of DDoS at the application (L7) and network/transport (L3/4) layers[723] [724]. In Q4 2022 Cloudfare changed the formula for calculating the percentage of attack traffic to the rate between attack requests from industry X and all requests from industry X. At the application layer, the aviation and aerospace industries took the lead with approximately 35% of the traffic going to the industry as part of HTTP DDoS attacks. The events services industry followed with over 16% of its traffic as HTTP DDoS attacks. Media and publishing, wireless, government relations and non-profit industries followed. In Q1 2023, the non-profit industry took the lead, followed by accounting firms. Considering the total attack bandwidth, Internet companies had the largest amount followed by the marketing and advertising industry, computer software, gaming and gambling and telecommunications. At the network layer, in Q4 2022, the education management industry corresponded to industry with the most network-layer DDoS attack traffic, followed by information technology and services, and public relations and communications, and then with a substantial margin by finance, gaming and gambling and medical practice. In Q1 2023 gaming and gambling was in the first spot followed by telecommunications and information technology and services.

StormWall found that the financial services were the most important targets of DDoS attacks with 34% of the attacks received, a twelvefold increase with respect to 2021. This domain is the most rewarding in terms of money.

[717] https://blog.cloudflare.com/ddos-threat-report-2023-q2/.
[718] https://blog.cloudflare.com/cloudflare-ddos-threat-report-2022-q3/.
[719] https://blog.cloudflare.com/ddos-threat-report-2023-q1/.
[720] Since Q4 2022, Cloudfare also considered a new formula for calculating the geographical spread as the percentage of attack traffic in a given country divided by the total traffic in the same country. Interested readers may refer to the reports by Cloudfare.
[721] https://blog.cloudflare.com/ddos-threat-report-2023-q1/.
[722] https://www.f5.com/labs/articles/threat-intelligence/2023-ddos-attack-trends.
[723] https://blog.cloudflare.com/ddos-threat-report-2022-q4/.
[724] https://blog.cloudflare.com/ddos-threat-report-2023-q1/.

Telecommunications were the target for 26%, with a fourfold increase due to remote working. Retail and ecommerce took the third position with 17%. Entertainment, insurance and education followed.

Akamai saw a sharp increase in the volume of DDoS attacks against financial institutions due to hacktivism (see Section 1.2.3) and DDoS extortion attacks with a financial motivation (see Section 1.2.5). In particular, the number of attacks increased by 22% (73% in Europe).

8.10 ATTACK VECTORS

According to Microsoft the rise in TCP attacks had the consequence of making TCP attack vectors the most common, including TCP SYN, TCP ACK, TCP floods and the like. UDP retained a goodly share with UDP flood and UDP amplification attacks. Packet anomalies were an important attack vector accounting for 15% of the attacks. Finally, the remaining attack vectors focused on reflected amplification attacks built on CLDAP, NTP and DNS[725].

Cloudfare observed an impressive increase in the number of attacks using BitTorrent protocol as the attack vector. This type of attack increased by 1221% in Q3 2022[726]. In the same period, SYN floods and DNS attacks accounted for 71% of the DDoS attack vectors, with SYN flood in the first spot[727]. SYN flood maintained the first spot in Q4 2022[728], while DNS attacks took the lead in Q1 2023 (30%), with SYN flood in second place (22%) and UDP-based in third place (21%)[729].

According to Imperva[730], the largest L3/4 DDoS attack in 2022 was in July 2022 and peaked at 1373 gigabits per second (Gbps).

Stormwall observed that 78% of the attacks targeted the application layer (HTTP/HTTPS), 17% targeted the transport layer (TCP/UDP) and 3% targeted the DNS. In this context, the decrease in the cost of organising a botnet made HTTP flood a preferred attack vector.

F5Labs observed that multi-vector attacks led the ranking, followed by application attacks that almost reached the same cardinality. Protocol attacks remained stable at about 10% of events observed, while volumetric attacks had a hit probably due to their requirements in terms of resources[731].

As discussed in Section 1.2.4, DDoS often become an attack vector itself for other attacks[732].

8.11 ADDITIONAL FACTS AND NUMBERS

- According to Microsoft, spoofed floods consumed most of the attack volume with 53%[733].
- According to F5Lab[734], the peak of DDoS bandwidth increased by 216% in 2020.
- According to F5Labs[735], we should expect an increase in attacks combining application and multi-vector attacks.
- According to DDoS Guard[736], the duration of DDoS attacks has decreased while their frequency has increased.
- DDoS attacks are increasingly used for reconnaissance[737].
- Attacks increasingly follow commercial seasonality such as, for instance, the days of quarterly and semi-annual reporting by financial institutions, holidays and billing payments[738].
- Constant DDoS attacks are now the norm[739] according to DDoS Guard.

[725] https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights/.
[726] https://blog.cloudflare.com/cloudflare-ddos-threat-report-2022-q3/.
[727] https://blog.cloudflare.com/cloudflare-ddos-threat-report-2022-q3/.
[728] https://blog.cloudflare.com/ddos-threat-report-2022-q4/.
[729] https://blog.cloudflare.com/ddos-threat-report-2023-q1/.
[730] https://www.imperva.com/blog/imperva-releases-its-global-ddos-threat-landscape-report-2023/.
[731] https://www.f5.com/labs/articles/threat-intelligence/2023-ddos-attack-trends.
[732] https://www.the-imperva-global-ddos-threat-landscape-report-2023.
[733] https://www.microsoft.com/en-us/security/blog/2023/02/21/2022-in-review-ddos-attack-trends-and-insights/.
[734] https://www.f5.com/labs/articles/threat-intelligence/2023-ddos-attack-trends.
[735] https://www.f5.com/labs/articles/threat-intelligence/2023-ddos-attack-trends.
[736] https://ddos-guard.net/en/blog/ddos-attack-trends-2022.
[737] https://www.the-imperva-global-ddos-threat-landscape-report-2023.
[738] https://ddos-guard.net/en/blog/ddos-attack-trends-2022.
[739] https://ddos-guard.net/en/blog/ddos-attack-trends-2022.

- According to Netscout Security's *Trends to Watch in 2023*[740], 'DDoS attack traffic is increasingly originating from within the same network it is targeting'. Inbound DDoS attacks are flanked by outbound and cross-bound attacks.
- According to Akamai, in 2022, the top five attack vectors accounted for 55% of all attacks, while it was 90% in 2010. This illustrates the increased maturity, variety and complexity of attacks[741].
- Airports have become a more preferred target for cyberattacks in Europe since the war in Ukraine began. More than 30 airports in total have been hit by DDoS in total[742].
- Social media platforms have then been exploited as a way to involve thousands of people in becoming DDoS hackers, providing DDoS attacks that are easy to execute[743].

[740] https://www.netscout.com/blog/security-trends-watch-2023.
[741] https://www.akamai.com/resources/research-paper/the-evolution-of-ddos-return-of-the-hacktivists.
[742] https://www.bitdefender.com/blog/hotforsecurity/pro-russian-killnet-group-hits-us-airline-websites-with-ddos-attack/.
[743] Microsoft Digital Defense Report 2022.

9. THREATS AGAINST AVAILABILITY: INTERNET THREATS

Today more than ever the use of the Internet and the free flow of information is fundamental and impacts the lives of all of us. Access to the Internet has become an essential need: to work, study, exercise our freedom of expression, political freedom and social interactions. However, this right is often not guaranteed. Threats to Internet availability refer to intentional or unintentional disruptions of Internet or electronic communications that result in Internet outages, blackouts, shutdowns or censorship. Internet disruptions can be due to government-directed Internet shutdowns, power outages, cable cuts, cyberattacks, technical problems, natural phenomena and military actions[744]. Today these threats are diversifying and growing.

This report will cover the topic of threats that impact the availability of internet. We note that DDoS and other cyberattacks are covered in separate sections and only briefly mentioned here due to their individual impact on the threat landscape.

9.1 INTERNET SHUTDOWNS AT AN ALL-TIME HIGH

An internet shutdown is *an intentional disruption of Internet or electronic communications, rendering them inaccessible or effectively unusable, for a specific population or within a location, often to exert control over the flow of information*[745] [746].

Access Now[747] assesses that in 2022, we reached an all-time record high for intentional Internet shutdowns with 187 events across 35 countries, an increase of 323% over 2021. Threats to Internet availability are keeping up their momentum, especially in the post-covid era, due to the increasing reliance of human activities and society on Internet technologies boosted by AI/ML and 5G/6G. Eighty disruptions were recorded in the period January to May 2023[748].

According to Access Now[749], *not only are shutdowns resurging after a decrease at the height of the pandemic, but they're also lasting longer, targeting specific populations and are being wielded when people need a connection the most — including during humanitarian crises, mass protests and active conflict and war.* Internet shutdowns are becoming increasingly targeted and sophisticated[750]. Layered tactics are used including shutdowns, censorship and surveillance. In 2022, 133 of the 187 total shutdowns occurred during some form of violence, compared to 112 in 2021, 99 in 2020 and 75 in 2019[751]. In 48 cases, Internet shutdowns occurred during grave human rights abuses and violence, including murder, torture, rape or apparent war crimes by governments, militaries, police or security forces.

Access Now also found a notable rise has been observed in the length of the shutdowns. In 33 of 35 countries targeted for shutdowns, repeated attacks have been observed since 2016. In addition, 16 attacks lasted across 2021 and 2022, and 16 attacks across 2022 and 2023, a 100% increase with respect to 2020 and 2021. Specific examples also show the extent of this phenomena, for instance, more than two years of a full communication blackout in Ethiopia and 500 plus days of shutdown in Myanmar.

744 https://blog.cloudflare.com/q1-2023-internet-disruption-summary/.
745 https://www.accessnow.org/campaign/keepiton/.
746 https://www.mediadefence.org/resource-hub/emerging-trend-internet-shutdowns/
747 https://www.accessnow.org/internet-shutdowns-2022/.
748 https://www.accessnow.org/internet-shutdowns-2022/.
749 https://www.accessnow.org/internet-shutdowns-2022/.
750 https://www.accessnow.org/internet-shutdowns-2022/.
751 https://www.accessnow.org/internet-shutdowns-2022/.

Cloudfare also monitored Internet disruption, in general, and government-directed disruption in particular[752] [753] [754]. In the periods Q3-2022 and Q1-2023, government-directed attacks continued with governments using Internet shutdowns to impose control, reduce democracy and hide violations of human rights. Disruptions to Internet and mobile networks continued in Iran to counter protests over the death of Mahsa Amini while in police custody, both globally and locally[755]. Surfshark (mainly monitoring disruptions to network connections and disruptions to social media/messaging apps) claimed that attacks affected 4.2 billion people in 2022 and involved 32 countries with 112 attacks (including long-term attacks). The attacks to Internet connections had an average duration of 33 hours, 113 days to social media[756]. These types of attacks decreased with respect to 2021[757]. Local Internet shutdowns outperformed nationwide events and social media disruption. Facebook, Instagram and TikTok were the three main social media targeted by disruption[758].

Surfshark has been providing a tool for monitoring Internet disruptions due to protests, elections, other political turmoil and Internet law since 2015, including disruptions to network connections and disruptions to social media and messaging apps. Since 2015, Surfshark observed 113 attacks in Africa, 591 in Asia, 15 in Europe (most of them in Russia), 9 in North America, 42 in South America, and 0 in Oceania[759].

According to Surfshark, national protest and political turmoil were the most prominent triggers[760]. In 2022, shutdowns during protests reached a level that is comparable to the level reached before the pandemic. Sixty-two shutdowns were observed, 19 of which were countrywide. The remaining were divided between regional (17) and local (25) and aimed to hide rights abuses or maintain authoritarian control. In addition to this, shutdowns (33 in 2022) were being increasingly used as a military strategy. Techniques include blackouts, air strikes and platform blocks that have an immense impact on people, whose desperation and insecurity are increased by Internet and telecommunications blackouts.

Shutdowns are also imposed during student and public examinations (12 in 2022) and during elections (5 in 2022), specifically targeting Brazil, India, Kazakhstan, Turkmenistan and Uganda.

In terms of geographical spread, according to Cloudflare shutdowns were spread all over the world in 2022 and 2023[761] [762] [763]. The Asia Pacific region retained the record for the number of shutdowns (102), with a decreasing trend with respect to 2021, but still very peculiar and common for the area, as well as being intertwined with censorship attacks. India was the world leader with 84 shutdowns. Shutdowns mostly targeted mobile communications (80%), possibly affecting up to 1.2 billion mobile internet users in the region.

Eastern Europe and Central Asia grew with shutdowns rising from 7 in 2021 to 36 in 2022 as observer by Cloudfrare. This was mainly due to the 22 shutdowns imposed on Ukraine by the Russia invasion and mostly targeting (77.3%) communications infrastructure. The top three triggers were conflict (22), control (5) and protest (4). Shutdowns (9) decreased by half in Africa, while maintaining the lead regarding long-lasting attacks. Half of the shutdowns masked human rights abuses, 44.5% of shutdowns were related to protests while 33.3% targeted platforms. In addition, the Middle East and North Africa accounted for 37 shutdowns, half of which (18) were in Iran during the protests for women's rights and regime change in that country. Services were targeted by 24.3%, blocking access to messaging and social media platforms. Finally, three shutdowns were observed in Latin America and the Caribbean, one in Brazil and two in Cuba.

[752] https://blog.cloudflare.com/q1-2023-internet-disruption-summary/.
[753] https://blog.cloudflare.com/q4-2022-internet-disruption-summary/
[754] https://blog.cloudflare.com/q3-2022-internet-disruption-summary/
[755] Insikt Group, THREAT ANALYSIS 2022 Annual Report.
[756] https://surfshark.com/blog/internet-censorship-2022.
[757] https://surfshark.com/blog/internet-censorship-2022.
[758] https://surfshark.com/blog/internet-censorship-2022.
[759] Numbers retrieved at the time of publication by: https://surfshark.com/research/internet-censorship.
[760] https://surfshark.com/blog/internet-censorship-2022.
[761] https://blog.cloudflare.com/q1-2023-internet-disruption-summary/.
[762] https://blog.cloudflare.com/q4-2022-internet-disruption-summary/.
[763] https://blog.cloudflare.com/q3-2022-internet-disruption-summary/.

9.2 INTERNET DISRUPTIONS

Internet disruptions may also be due to natural events, power outages, cable cuts, cyberattacks, technical problems and military actions[764]. They are quickly summarised in the following paragraphs.

9.3 CABLE CUTS, POWER OUTAGES AND TECHNICAL PROBLEMS

Cable cuts, power outages and technical problems are at the basis of many of the Internet disruptions observed over the years. Sometimes these disruptions are due to intentional, government-directed actions already discussed in the previous section. Here, we consider unintentional events.

Cable cuts can be both terrestrial and submarine, and are important threats to Internet availability. The submarine threat[765] is now under scrutiny due to the sabotage of the sub-sea Nord Stream natural gas pipelines, which brought to the public's attention the important role submerged cables play in the operation of the Internet. Disruptions due to cable damages or cuts has been reported in Iran, Pakistan, Haiti, the UK, Bolivia, Anguilla, Bangladesh and Venezuela[766] [767] [768].

Power outages often disrupted connectivity in Venezuela as monitored by the independent @vesinfiltro account on X (formerly Twitter). The same thing happened in Oman in Q3 2022 impacting energy, aviation and telecommunication services, in Pakistan affecting more than 220 million people, in the USA with a local impact due to gunfire, in Kenya and in Bermuda. In Argentina, soaring temperature caused a multi-hour, large-scale power outage[769] [770] [771].

Finally, technical problems affected Internet availability due to misconfigurations and routing problems and can be often used as an explanation for a disruption, such as the one in Canada caused by technical problems (router malfunction) at Rogers, one of the Canada's largest ISPs[772] [773] [774].

9.4 NATURAL DISASTERS

Natural disasters, including earthquakes and hurricanes, can cause damage to electrical power grids and telecommunications infrastructure. In Q3 2022, two earthquakes with a magnitude of over 7 hit Papua New Guinea and Mexico causing a traffic drop of 26% and 50% respectively. Later in 2022, outages due to an earthquake happened in the Solomon Islands. The most relevant and disruptive event happened in Turkey in 2023, with thousands of deaths and injuries, and traffic losses of 63 to 94%[775] [776] [777] as reported by Cloudflare. In New Zealand, hurricanes, cyclones and other weather events caused disruptions including what was called the 'country's biggest weather event in a century' and caused days of disruption[778].

9.5 CYBERATTACKS

Cyberattacks against system availability are common and involve any type of system, from services to the Internet itself. Within the category of cyberattacks targeting Internet availability and fostering censorship lie DDoS attacks and attacks to the main Internet services (e.g. Domain Name System – DNS)[779]. However, several techniques are in the hands of cybercriminals trying to disrupt Internet communications, from packet interception and manipulation to performance degradation, packet dropping via network degradation and adversarial route announcements to name but a few. In addition, attacks on Internet availability are often coupled with the manipulation of information trying to discredit protest movements and parties against regimes (see the following chapter for more details).

[764] https://blog.cloudflare.com/q1-2023-internet-disruption-summary/.
[765] https://www.enisa.europa.eu/publications/undersea-cables.
[766] https://blog.cloudflare.com/q1-2023-internet-disruption-summary/.
[767] https://blog.cloudflare.com/q4-2022-internet-disruption-summary/.
[768] https://blog.cloudflare.com/q3-2022-internet-disruption-summary/.
[769] https://blog.cloudflare.com/q1-2023-internet-disruption-summary/.
[770] https://blog.cloudflare.com/q4-2022-internet-disruption-summary/.
[771] https://blog.cloudflare.com/q3-2022-internet-disruption-summary/.
[772] https://blog.cloudflare.com/q1-2023-internet-disruption-summary/.
[773] https://blog.cloudflare.com/q4-2022-internet-disruption-summary/.
[774] https://blog.cloudflare.com/q3-2022-internet-disruption-summary/.
[775] https://blog.cloudflare.com/q1-2023-internet-disruption-summary/.
[776] https://blog.cloudflare.com/q4-2022-internet-disruption-summary/.
[777] https://blog.cloudflare.com/q3-2022-internet-disruption-summary/.
[778] https://www.dailymail.co.uk/sciencetech/article-11748949/Map-reveals-Cyclone-Gabrielles-trail-destruction.html.
[779] https://datatracker.ietf.org/doc/draft-irtf-pearg-censorship/.

Among cyberattacks, when BGP attacks are used to disrupt Internet communications and packet routing, they assume critical importance. **BGP Hijacking** allows attackers to reroute Internet traffic. This is achieved by falsely announcing ownership of IP prefixes, groups of IP addresses. The consequence is that Internet data use a malicious route to reach their destination. BGP hijacking can result in incorrect routing, data monitoring, interception, blackholing or redirection to another website. With blackholing, the data is dropped from the network. Wrong BGP announcements can have a significant impact as they may spread beyond the original target area.

As an erroneous announcement of ownership can also result from a misconfiguration, it is not always straightforward to tell whether a BGP hijacking incident is indeed malicious or whether it is unintentional (**BGP Route Leak**). In addition, BGP configuration changes could result in erroneous **BGP withdrawals**. In the reporting period[780] [781] [782], Qrator observed a stable number of unique BGP Route Leaking ASes (Autonomous Systems) ranging between 2740 and 3030. The number of unique BGP Hijacking ASes varied from 13.5k (Q3 2022), 10.0k (Q4 2022), 13.0k (Q1 2023), an increase of 30% with respect to Q4 2022, reaching the same numbers as in Q3 2022. Considering the total numbers of leaks and hijacks originated by an AS, Qrator observed a stable number of BGP Hijackings ranging between 2.4 million and 3 million. The number of BGP route leaks started at around 12 million in Q3 2022, a similar value to Q1 2022 and a fourfold increase with respect to Q2 2022. A sharp fourfold decrease was then observed in Q4 2022 with a return to substantial values of 9 million in Q1 2023.

9.6 PHYSICAL TAKE-OVER AND DESTRUCTION OF INTERNET INFRASTRUCTURE

Since the invasion of Ukraine, Russia has been actively taking over internet infrastructure by diverting traffic over Russian networks. For example, after taking over the city of Kherson, Russia forced local internet providers to give over control of the networks and then physically rerouted mobile and internet traffic over Russian-owned network infrastructure. This allowed Russia to block access to social media, prevent information leakage and have more control over the narrative surrounding its war. It also empowered the country to perform surveillance activities over the communication flows.

Ukraine cellular networks were actively shut down, forcing Ukrainian residents to use Russian mobile service providers. There are also reports of communication infrastructure being actively destroyed. According to the Ukrainian government, around 15% of the internet infrastructure had been destroyed as of June 2022[783] [784].

In the last seven months, multiple Internet disruptions were caused by infrastructure damage and power outages related to the war. For instance, power outages were at the basis of Internet disruptions in Kharkiv in September 2022[785]. In Q4 2022, The Ukraine's electrical infrastructure was damaged by Russian missile strikes, resulting in power outages and disruptions to Internet connectivity. In October 2022, several power stations were destroyed in Kyiv resulting in a 25% decrease in Internet traffic, while the decrease in the whole Ukraine was around 50% in November 2022. The same trend due to military actions was observed in 2023, with disruptions in Odessa and multiple locations around Ukraine[786] [787] [788].

9.7 ACTIVE INTERNET CENSORSHIP

Internet censorship can be defined as *the practice, typically conducted by a national or regional government, of deliberately hindering the general public's access to certain websites or online information*[789]. Internet censoring can be implemented in various ways including DNS tampering, IP blocking and keyword filtering[790]. Different organisations monitor the trends in Internet Censorship such as OONI, Freedom House and Reporters Without Borders.

According to the Freedom House[791], in 2022, global Internet freedom declined for the 12th consecutive year with the biggest decrease observed in Russia after the invasion of Ukraine. This trend is representative of a more general

[780] https://blog.qrator.net/en/q3-2022-ddos-attacks-and-bgp-incidents_158/.
[781] https://blog.qrator.net/en/q4-2022-ddos-attacks-and-bgp-incidents-report_163/.
[782] https://blog.qrator.net/en/q1-2023-ddos-attacks-and-bgp-incidents_171/.
[783] https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html.
[784] https://www.reuters.com/world/europe/russia-reroutes-internet-traffic-occupied-ukraine-its-infrastructure-2022-05-02/.
[785] https://blog.cloudflare.com/q3-2022-internet-disruption-summary/.
[786] https://blog.cloudflare.com/q1-2023-internet-disruption-summary/.
[787] https://blog.cloudflare.com/q4-2022-internet-disruption-summary/.
[788] https://blog.cloudflare.com/q3-2022-internet-disruption-summary/.
[789] https://worldpopulationreview.com/country-rankings/countries-that-censor-the-internet.
[790] https://datatracker.ietf.org/doc/draft-irtf-pearg-censorship/.
[791] https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet.

trend where governments are increasingly trying to break the Internet in more controllable subspaces. Seventy-six per cent of the 4.5 billion users of the Internet live in countries where individuals have been arrested or imprisoned for their online content, while 51% of users live in countries where access to social media was temporarily or permanently restricted[792]. The worst countries for censorship (11% not assessed) are China (for the 8th consecutive year), Myanmar, Iran, Cuba, Vietnam, Russia, Saudi Arabia, Pakistan, Egypt, Ethiopia and Uzbekistan. In this worrisome scenario, a positive trend has been observed: 26 countries (a record) experienced an improvement in freedom, including the USA that observed its first marginal improvement over 6 years.

Trends in the censorship of the Internet in 2022 were hugely affected by Russian's invasion of Ukraine in February 2022[793]. Thousands of websites were blocked in Russia, and access to social media has also been impeded. Access to reliable information about the war was forbidden in Russia, limiting individual's rights to connect with users across the world. High-profile news and social media websites have been blocked, including Instagram, Facebook, Twitter, Google News, BBC News, NPR, Die Welt, The Telegraph, Bellingcat and Amnesty International. A thousand of these websites are Ukrainian[794].

Open Observatory of Network Interference (OONI), a global community that has been measuring Internet censorship since 2012[795], recently analysed the status of freedom in Russia and found that 494 domains were blocked in the area of international and Russian human rights, independent journalism and social media[796]. OONI also analysed the status of freedom in Southeast Asia, and found that no countries there had achieved the status of a free Internet[797].

[792] https://worldpopulationreview.com/country-rankings/countries-that-censor-the-internet.
[793] https://freedomhouse.org/report/freedom-net/2022/countering-authoritarian-overhaul-internet.
[794] https://www.top10vpn.com/research/websites-blocked-in-russia/.
[795] https://ooni.org/.
[796] https://ooni.org/post/2023-russia-a-year-after-the-conflict/.
[797] https://ooni.org/post/2022-imap-8-research-reports-southeast-asia/.

10. INFORMATION MANIPULATION AND INTERFERENCE

Foreign Information Manipulation and Interference (FIMI) describes a mostly non-illegal pattern of behaviour that threatens or has the potential to negatively impact values, procedures and political processes. Such activity is manipulative in character, conducted in an intentional and coordinated manner. Those who undertake such activity may be state or non-state actors, including their proxies inside and outside their own territory[798]. The current chapter focuses on information manipulation and interference regardless of its origin.

ENISA's Threat Landscape (ETL) report has been tracking information manipulation as 'Disinformation – Misinformation' since 2021. In this edition of the ETL, we opted for the more general term of **information manipulation** to reflect a broader set of potential threats. Accordingly, the threat of information manipulation persisted in this year's edition, establishing itself as a stable trend. Although disinformation is a prominent part of information manipulation, 'information manipulation' puts emphasis on the behaviour as opposed to the truthfulness of the content and has therefore been preferred over the term 'disinformation'[799]. The notion of manipulative behaviour is consistent with the other threat categories in the ETL, given that it clearly indicates intent to conduct malicious actions that have an adverse impact. Hence, it is considered more fitting to the definition of what constitutes a cybersecurity threat.

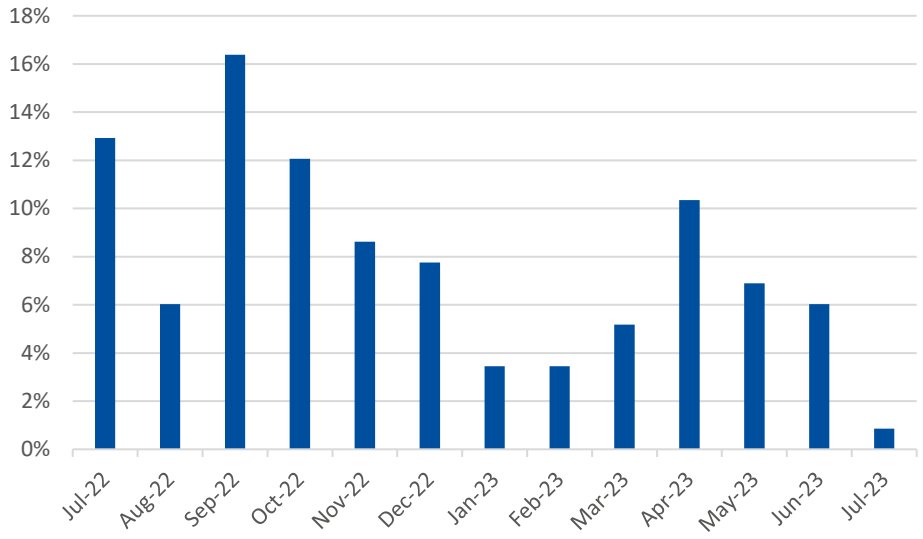
The link between information manipulation and cybersecurity is often debated. Acknowledging its existence does not imply that cybersecurity alone could solve the problem of information manipulation. Still, it is argued that cybersecurity practices can contribute to a sounder environment for information, which in turn will be beneficial for the efforts of cybersecurity professionals.

We argue that information manipulation and relevant operations should be considered as a cybersecurity threat, since such operations directly affect at least one of the three components of the information security model and in particular that of integrity of information[800] [801]. Moreover, by means of information manipulation and distortion of the information space, the operational response to crises may be misled and hampered. Information manipulation is frequently the steppingstone or one of the elements of more elaborate hybrid attacks that involve other cybersecurity threats, e.g. DDoS attacks. Information manipulation operations frequently abuse and exploit other cybersecurity principles (such as authenticity and accountability) and leverage on other types of cybersecurity tactics, techniques and procedures (as discussed extensively throughout this chapter), thus justifying the need to consider information manipulation in the context of ETL as one of the prime categories of threats.

The figure below shows the timeline of information manipulation events that we have observed throughout the period under review. The following sections give an overview of information manipulation and identify trends.

[798] https://www.eeas.europa.eu/eeas/tackling-disinformation-foreign-information-manipulation-interference_en.
[799] Many of the sources consulted refer to 'disinformation', 'misinformation', 'influence operations', 'information warfare' etc. Although these terms do not encompass *exactly* the same notion, in the absence of a common taxonomy, the overarching term 'information manipulation' is used for simplicity.
[800] In the MITRE ATT&CK Framework, the definition of the cybersecurity tactic of data manipulation is 'adversaries may insert, delete or manipulate data in order to influence external outcomes or hide activity, thus threatening the integrity of the data'. The notion of information manipulation is thus directly related to the aforementioned adversarial tactic in cybersecurity.
[801] Other components might be affected as well, for example 'hack-and-leak operations' have an impact on confidentiality.

Figure 38: Distribution of information manipulation incidents during the period of reference



Methodological note for this chapter:

Data: Most of the events analysed have been shared by the European External Action Service (EEAS) Strategic Communications division. The division focuses on Foreign Information Manipulation and Interference (FIMI) and on activities traceable to specific strategic actors or regions. The incidents have been filtered with keywords related to cybersecurity (e.g. 'phishing', 'defacement'). Most of them refer to activities suspected to be linked or that are linked to Russia's war of aggression against Ukraine. Whereas attribution remains challenging, the narratives and the motivations exhibited by adversaries seem to point to strategic threat actors. This is by no means a formal attribution, just a likely provenance. This focus might be due to data collection (focusing on strategic issues), and/or to the geopolitical context, possibly leading to a surge in information manipulation and/or in Tactics Techniques and Procedures (TTPs) combining cybersecurity and information manipulation.

Important: This does not necessarily imply that a given incident or source of information is linked to the Russian government or editorially in favour of the Russian government, nor that it has intentionally sought to disinform.

Analysis: This chapter analyses incidents both with the DISARM (DISinformation Analysis & Risk Management) Red framework[802], describing behaviours for manipulating information, and the MITRE ATT&CK Framework. This combined approach was proposed for the first time in the 2022 ENISA-EEAS joint report 'Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape'[803].

[802] The framework can be found at this link: https://www.disarm.foundation/framework. The framework has been updated in September 2023 with 41 new techniques and 7 updated techniques. Since the analysis for the current chapter had been carried beforehand, these updates are not reflected here.
[803] https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape.

10.1 GENERAL TRENDS

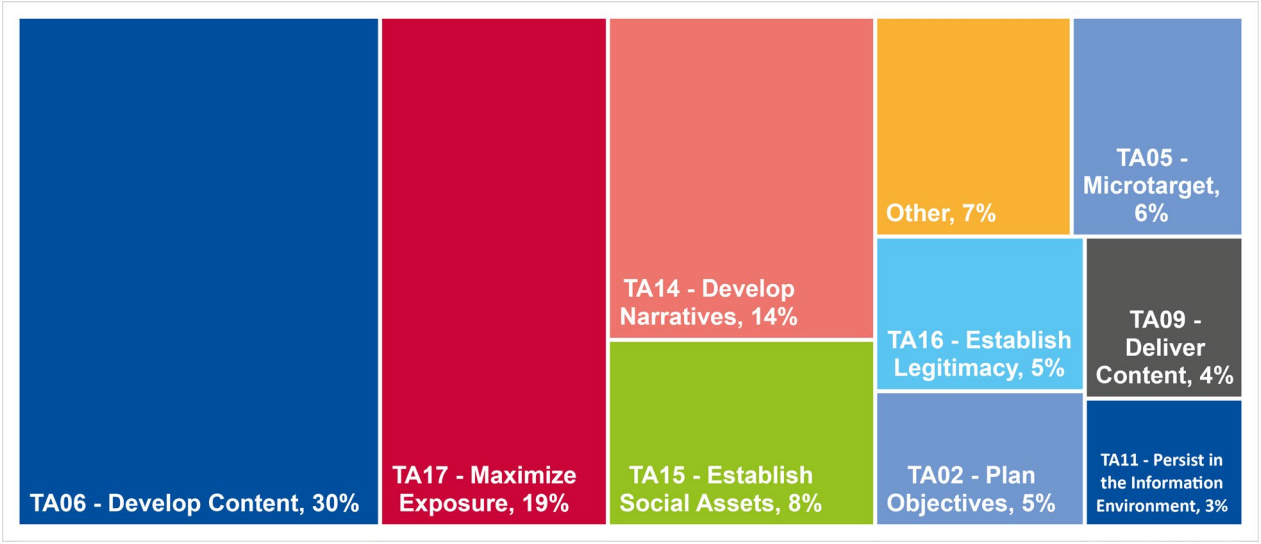
In terms of information manipulation, unsurprisingly, the most recurrent tactic is that of content development, followed by the maximisation of exposure and the development of narratives.

Table 5: Definitions of the top-3 DISARM tactics (in order of recurrence) [804]

DISARM Tactic	Definition
TA06 - Develop Content	Create or acquire text, images and other content
TA17- Maximise Exposure	Maximise exposure of the target audience to incident or campaign content via flooding, amplifying and cross-posting.
TA14 - Develop Narratives	Promote beneficial master narratives to achieve long-term strategic narrative dominance. From a misinformation campaign or cognitive security perspective the tactics around master narratives centre more precisely on the day-to-day promotion and reinforcement of this messaging. Tactically, their promotion covers a broad spectrum of activities both on- and offline.

The figure below shows the distribution of the most recurrent tactics according to the DISARM framework. The analysis has been carried out by associating several tactics to each incident.

Figure 39: Distribution of information manipulation tactics according to the DISARM framework



According to the MITRE ATT&CK framework, that is from a cybersecurity perspective, information manipulation has been supported mainly by tactics for the development of resources, which amount to approximately half of the tactics used, followed by tactics related to impact and defence evasion.

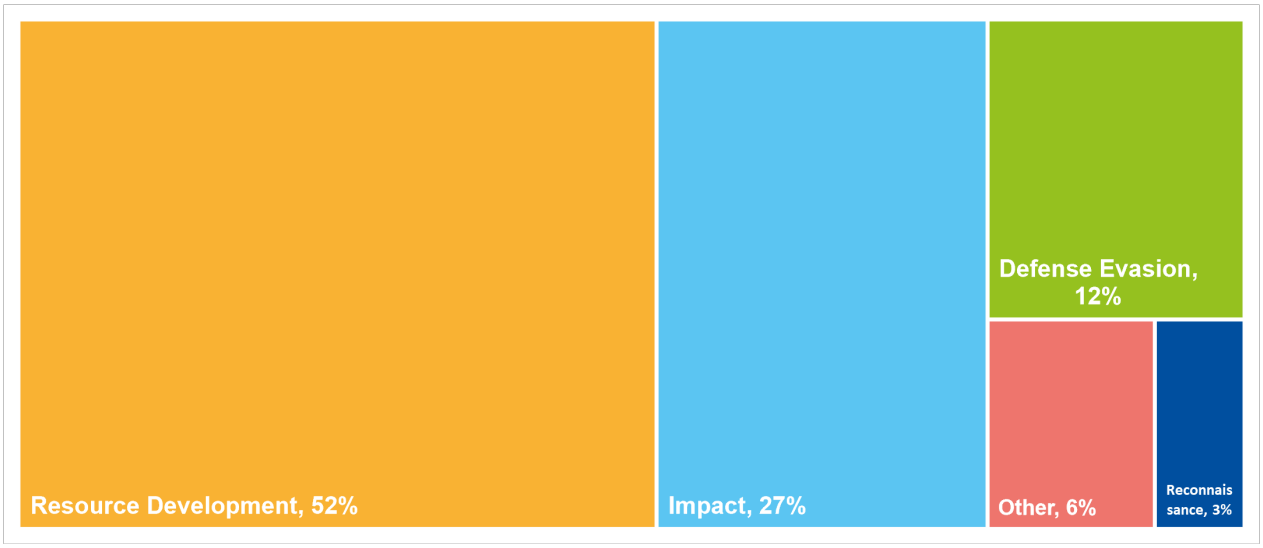
[804] For the full definitions, refer to https://www.disarm.foundation/framework.

Table 6: Definitions of the top-3 MITRE ATT&CK tactics (in order of occurrence) [805]

MITRE ATT&CK Tactic	Definition
Resource Development	Resource Development consists of techniques that involve adversaries creating, purchasing, compromising or stealing resources that can be used to support targeting.
Impact	The adversary is trying to manipulate, interrupt or destroy targeted systems and data.
Defence evasion	The adversary is trying to avoid being detected.

The figure below shows the distribution of the most recurrent tactics. The analysis has been conducted by associating several tactics to each incident.

Figure 40: Distribution of tactics according to the MITRE ATT&CK framework



In the following sections the most recurrent tactics, for both the DISARM and MITRE ATT&CK frameworks, are broken down into techniques and contextualised into specific trends.

10.2 INFORMATION MANIPULATION AS A KEY ELEMENT OF RUSSIA'S WAR OF AGGRESSION AGAINST UKRAINE

The vast majority of events analysed refer to activities suspected to be directly or indirectly linked to Russia's war of aggression against Ukraine. While this could be a bias induced by the data collection[806], information manipulation has been an essential and well-established component of Russian security strategies[807] [808]. Also, compared to the 2022 ENISA-EEAS joint report 'Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape'[809], the number of analysed events for the given period has grown significantly. Hence it is highly likely that the stage centre position taken by the conflict in the events analysed reflects an actual trend, namely the exploitation of information manipulation in the war of aggression. Still, it is to be noted that information manipulation campaigns associated with other countries were also present, as pointed out in section 2.1.

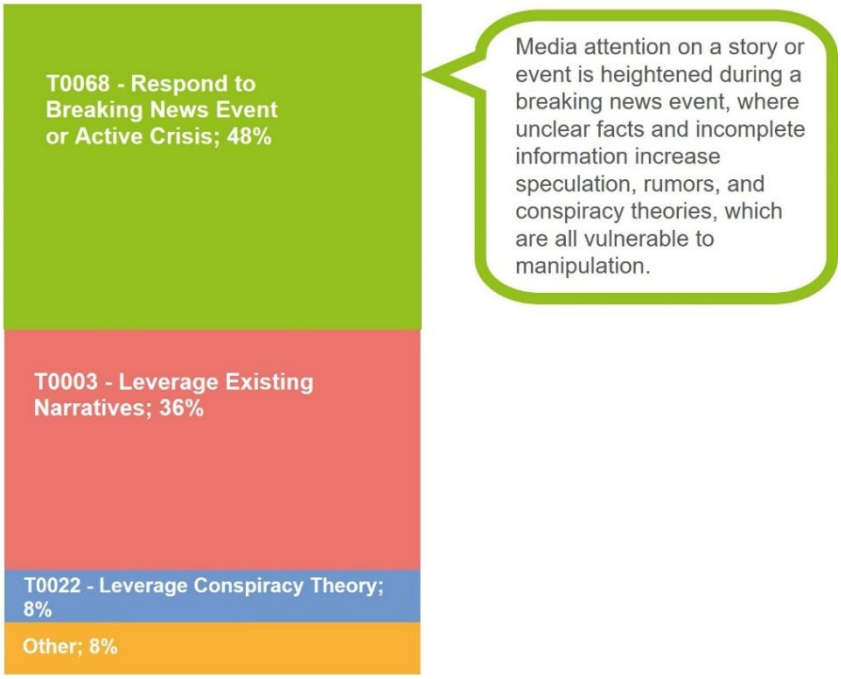
As with any other tool in a conflict, the use of information manipulation has been adapted to the circumstances and the goals of the phase the conflict is in. Microsoft has identified three phases in the first year of 'hybrid warfare', each

[805] For the full definitions, refer to: https://attack.mitre.org/.
[806] See the methodological note in the box at the beginning of the chapter.
[807] No Water's Edge: Russia's Information War and Regime Security (2023, Carnegie Endowment for International Peace).
[808] https://raport.valisluureamet.ee/2023/en/russian-armed-forces/1-3-russia-continues-to-look-for-a-weak-link-in-ukrainian-cyberspace/.
[809] https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape.

characterised by specific narratives: the first where cyber and influence operations would be functional in the invasion, the second targeting Kyiv's foreign and domestic support, and the third intensifying cyber and influence operations to augment Russia's political and military actions[810].

A closer look at the DISARM tactic TA14 – Develop Narratives, which is the third most recurrent tactic (see Figure 40), shows that the most used technique is to react to breaking news events or active crises (technique T0068). For example, a significant number of incidents concerned the damage to the Nord Stream 1 and 2 pipelines in September 2022, when there was a peak in the manipulation of information relating to the events analysed. The EUvsDisinfo database references at least 159 pieces of disinformation related to the Nord Stream events[811].

Figure 41: Distribution of techniques within the tactic TA14 – Develop Narratives



In addition, information manipulation was also adapted to the geography of the conflict. For example, we observed campaigns serving broader geopolitical purposes, such as strengthening Russia's influence in Africa[812] or collusion between the state media ecosystems of China and Russia, aligning on anti-Western narratives[813]. Indeed, microtargeting in the form of the creation of localised content a recurrent DISARM tactic (see Figure 40), whose creation and diffusion is also facilitated by Russia's use of its diplomatic network[814]. NewsGuard has identified 386 Russia-Ukraine disinformation sites in languages such as English, French, German and Italian[815].

Finally, we observe the use of doxing, which is the intentional leaking of a person's private information online without their consent to expose and demoralise Ukrainian and pro-Ukrainian fighters and activists[816].

[810] A Year of Russian Hybrid Warfare in Ukraine (2023, Microsoft) - https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf (Accessed 20/08/2023).
[811] https://euvsdisinfo.eu/disinformation-cases/?text=Nord%20Stream&date (Accessed 16/08/2023).
[812] https://www.reuters.com/world/africa-france-targets-russian-wagner-disinformation-2023-06-21/.
[813] https://euvsdisinfo.eu/1st-eeas-report-on-foreign-information-manipulation-and-interference-threats-towards-a-framework-for-networked-defence/.
[814] https://www.politico.eu/article/russia-diplomats-disinformation-war-ukraine/ (Accessed 03/10/2023)
[815] https://www.newsguardtech.com/special-reports/russian-disinformation-tracking-center/ (Accessed 16/08/2023).
[816] https://www.bbc.com/news/world-63491977.

10.3 EXPLOITING THE 'CYBERSECURITY NARRATIVE'

As explained above, information manipulation can serve several specific purposes, such as framing the public perception of an event or a public figure. However, information manipulation can be a goal in itself: it underpins the strategy of creating 'epistemological confusion that causes people to question the idea of objective truth'[817].

In this context, we observe that narratives built around public perception of cyberattacks and of cybersecurity practices (e.g. OSINT investigations and civilian hacktivism) are used to add legitimacy to false claims and hence contribute towards the manipulation and confusion of public opinion.

In some cases, alleged cyberattacks against public institutions or public officials, as well as entities or people perceived as authoritative, have been referenced as sources of information that support specific narratives. Such information gains credibility because of the legitimacy of the subjects that were allegedly hacked. For example, one of the conspiracy theories blaming the UK for the damage to the Nord Stream pipelines revolved around a message allegedly sent by UK officials to their US counterparts 'confirming' the UK's involvement[818] [819]. The credibility of the theory also relied on reports of an alleged hack of UK officials' phones which, however, would have been discovered before the events and therefore could not have been at the origin of the SMS[820] [821]. As to Russia, alleged or actual 'hack-and-leak' operations are not new[822]; however, their regularity highlights their effectiveness in amplifying existing divisions by allegedly exposing sensitive information[823].

In other cases, investigation methods that the public commonly associates with cybersecurity practices are used to enhance the credibility of research leading to (false) findings. For example, the popular 'fact-checking' Telegram account 'War on Fakes', which disseminates fakes news and propaganda about the Russian war of aggression against Ukraine[824], appropriates the authority of 'investigative aesthetics' by mimicking the techniques of open-source intelligence (OSINT) to expose the supposed untruths in the media coverage[825].

Although the examples above contribute to polluting the information environment, their target is the general public. However, we also observed narratives built around threat actors and their actions which instead target other threat actors and the cybersecurity community, hence impacting situational awareness in a more direct manner e.g. with false claims of attacks to gain visibility (see the next section) or with communications to gain credit[826].

10.4 INFORMATION MANIPULATION FUELLING 'HACKTIVISM'

Traditionally, hacktivism has been associated to political or social activism[827]. After some years of sporadic activity, hacktivism has re-gained traction in the context of the Russian invasion of Ukraine, with both pro-Russian and pro-Ukrainian hacktivists (but not only) making the headlines for their actions[828]. According to Radware, from February 18 until April 18, 2023, over 1,800 denial-of-service attacks were claimed by hacktivists across 80 Telegram channels[829]. Our analysis shows that the great majority of information manipulation incidents that were linked to a DDoS attack (actual or claimed) were carried out by self-proclaimed hacktivists.

In this context, hacktivism seems to be linked to information manipulation and interference on different levels. Firstly, in some instances it has been found that threat actors in Russian military intelligence might be linked to hacktivists'

[817] https://networkcultures.org/tactical-media-room/2022/07/22/weaponized-osint-the-new-kremlin-sponsored-participatory-propaganda/ (Accessed 16/08/2023). Note: the quote refers to participatory propaganda, however it is argued that it applies to information manipulation in general.
[818] https://www.open.online/2022/11/03/russia-vs-regno-unito-nord-stream-liz-truss-messaggio-blinken/.
[819] https://www.rainews.it/articoli/2022/11/-tutto-fatto-mosca-svela-un-presunto-sms-di-truss-a-blinken-dopo-lesplosione-del-nord-stream-209f449d-7ce2-4b62-aca2-f61ef0b7c9cc.html.
[820] https://www.theguardian.com/technology/2022/oct/29/government-urged-to-investigate-report-liz-truss-phone-was-hacked (Accessed 10/08/2023).
[821] https://www.dailymail.co.uk/news/article-11377539/Russia-claims-British-PM-texted-Blinken-shortly-Nord-Stream-pipeline-explosion.html (Accessed 23/08/2023).
[822] Rid T., Active Measures: The Secret History of Disinformation and Political Warfare, 2020.
[823] A Year of Russian Hybrid Warfare in Ukraine (2023, Microsoft) - https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf (Accessed 20/08/2023).
[824] Official Journal of the EU, 28/07/2023 (https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=OJ:L:2023:190I:FULL).
[825] https://networkcultures.org/tactical-media-room/2022/07/22/weaponized-osint-the-new-kremlin-sponsored-participatory-propaganda/ (Accessed 16/08/2023).
[826] https://thecyberexpress.com/baphomet-goes-ahead-breachforums-plans/ (Accessed 25/08/2023).
[827] https://www.merriam-webster.com/dictionary/hacktivism.
[828] https://www.wired.co.uk/article/hacktivism-russia-ukraine-ddos (Accessed 17/08/2023).
[829] https://www.radware.com/security/threat-advisories-and-attack-reports/hacktivism-unveiled-april-2023/ (Accessed 11/08/2023).

activities, suggesting that hacktivism has been used to extend the perception of Russia's cyber-capabilities[830] or as a cover for state-backed activities[831]. Secondly, the hyper-mediatisation of attacks perpetuated by hacktivists, functional to their general goal of raising awareness of a certain topic, pollutes the information environment as, for example, some groups claim credit for attacks claimed by other groups[832] or without substantial proof for their claims (see attacks targeting OT in section 2.4.3).

While the actual magnitude[833] and harm[834] [835] of the 'hacktivist phenomenon' have been questioned, the information sphere is affected anyway, since the public is more likely to respond to the effects of a cyberattack rather than the attack itself[836]. Thirdly, hacktivism in a conflict situation might work as a propaganda tool and incite the involvement of civilians in the hostilities[837]. One notable example is NoName057's DDoSia project, a toolkit to crowdsource DDoS attacks, also mentioned in section 2.4.1, leveraging politically-driven hacktivists willing to download and install a bot on their computers to launch denial-of-service attacks[838] [839]. In early January, the threat actor put out a call for hero' hacktivists offering financial incentives paid out in cryptocurrency[840].

10.5 MAXIMISATION OF EXPOSURE THROUGH A WIDESPREAD DIGITAL PRESENCE

The most recurrent MITRE ATT&CK tactic is the development of resources in support of adversarial operations ('Resource development') (see Figure 41). The figure below shows the share of the most recurrent techniques for resource development, i.e. the establishment of accounts and the acquisition of infrastructure.

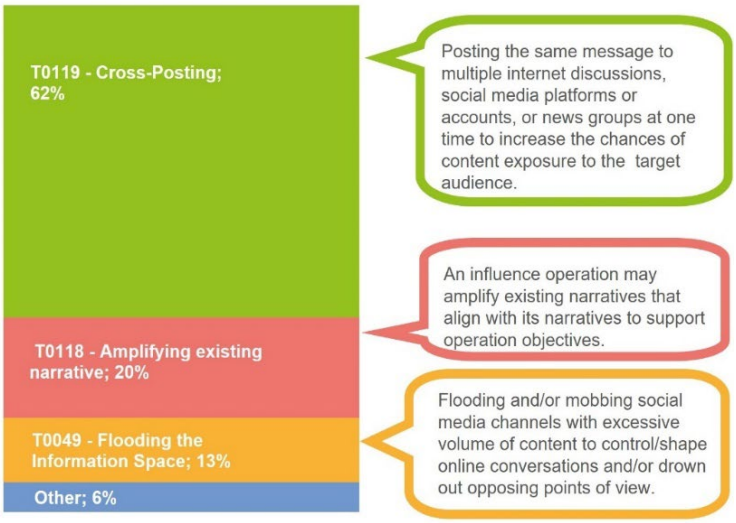
Figure 42: MITRE ATT&CK - Distribution of techniques within the MITRE tactic – Resource Development

[830] A Year of Russian Hybrid Warfare in Ukraine (2023, Microsoft) - https://www.microsoft.com/en-us/security/business/security-insider/wp-content/uploads/2023/03/A-year-of-Russian-hybrid-warfare-in-Ukraine_MS-Threat-Intelligence-1.pdf (Accessed 20/08/2023).
[831] https://www.scmagazine.com/feature/hacktivism-is-it-fashionable-again-or-just-a-sly-cover (Accessed 11/08/2023)..
[832] Hacktivism Unveiled, April 2023 Insights Into the Footprints of Hacktivists (radware.com) (Accessed 16/08/2023).
[833] Getting Bored of Cyberwar: Exploring the Role of Civilian Hacktivists in the Russia-Ukraine Conflict (2022) - https://arxiv.org/abs/2208.10629.
[834] https://www.sentinelone.com/labs/noname05716-the-pro-russian-hacktivist-group-targeting-nato/ (Accessed 11/08/2023).
[835] For example, research found that NoName057, one of the most notorious hacktivist groups, has a '40% success rate, and companies with well-protected infrastructure can withstand their attack attempts'. Also, '20% of the successes claimed by the group may not be their doing'. https://press.avast.com/noname05716-pro-russian-hacker-group-targeting-sites-in-ukraine-and-supporting-countries-with-ddos-attacks (Accessed 11/08/2023).
[836] https://www.researchgate.net/publication/336149510_The_Social_and_Psychological_Impact_of_Cyber-Attacks.
[837] 'Cyber Dimensions of the Armed Conflict in Ukraine – Q1 2023' (CyberPeace Institute, 2023) - https://cyberpeaceinstitute.org/news/publications/cyber-dimensions-of-the-armed-conflict-in-ukraine-q1-2023/.
[838] https://blog.sekoia.io/following-noname05716-ddosia-projects-targets/#h-conclusion.
[839] https://www.sentinelone.com/labs/noname05716-the-pro-russian-hacktivist-group-targeting-nato/ (Accessed 11/08/2023).
[840] https://cybernews.com/cyber-war/new-undercover-intel-noname-russian-hacktivist-operations/ (Accessed 17/08/2023).

This reflects the fact that 'at the most fundamental level […] any online operation has to be able to get online'[841] and that information manipulation does not necessarily require extreme technological sophistication and benefits greatly from a diffused and pervasive presence. As to Russia, the OECD notes that its efforts to spread disinformation rely on a mix of fake and artificial accounts, anonymous websites and state media sources, as well as on feed-back loops between social media and traditional media[842].

The above is coherent with the findings of this report. The DISARM tactic to maximise exposure (TA17 – Maximise Exposure), which is the second most recurrent DISARM tactic (see Figure 40), encompasses cross-posting as the most-used technique, followed by the amplification of an existing narrative and the flooding of the information space.

Figure 43: DISARM - Distribution of techniques within the tactic TA17 – Maximise exposure



It is important to stress that the acquired infrastructure and the accounts established might not be authentic: in particular, the use of botnets and of typosquatting to mimic legitimate media outlets or entities (e.g. governmental organisations) or people has observed.

Among the events analysed in which information was manipulated, the MITRE ATT&CK technique of masquerading, intended as the 'manipulation of an artifact's feature to make it appear legitimate, was used as the main technique to evade defences and avoid being detected'[843]. In the context of this chapter, the definition is stretched[844] to also include attempts to conceal identity and undermine accountability. In particular, in several instances, content was presented as coming from a seemingly legitimate source[845] [846]. As another example, the technique was used to circumvent the EU's ban on broadcasting RT/Russia Today in the EU, e.g. by using mirror domains[847].

[841] 'Phase-based Tactical Analysis of Online Operations' (Carnegie Endowment for International Peace, 2023) - https://carnegieendowment.org/2023/03/16/phase-based-tactical-analysis-of-online-operations-pub-89275 (Accessed on 11/10/2023).
[842] https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/ (Accessed 16/08/2023).
[843] Masquerading is a MITRE ATT&CK technique falling under the tactic – Defence evasion.
[844] MITRE ATT&CK further explains masquerading as occurring 'when the name or location of an object, legitimate or malicious, is manipulated or abused for the sake of evading defences and observation. This may include manipulating file metadata, tricking users into misidentifying the file type, and giving legitimate tasks or services names'.
[845] https://www.rand.org/news/press/2022/09/14.html.
[846] https://www.euronews.com/my-europe/2022/10/28/fake-euronews-video-about-russian-art-auction-spreads-online.
[847] https://edmo.eu/2022/12/01/with-a-few-simple-steps-how-rt-de-circumvents-the-eu-sanctions/.

In our analysis, the MITRE ATT&CK tactic 'Defence Evasion' is the third most recurrent MITRE ATT&CK tactic. (See Figure 41) and the technique Masquerading is the only technique identified under this tactic.)

Example: RRN – A complex and persistent campaign of information manipulation[848]

A notable example is the campaign of information manipulation labelled 'RRN' identified by VIGINUM, the French governmental agency tasked with protecting against and the monitoring of foreign digital interferences. Typosquatting was one of the modus operandi of the campaign: between June 2022 and May 2023 VIGINUM observed the registration of 355 domain names impersonating the identity of media outlets in France and in nine states in Europe, the Americas and the Middle East. The URLs of these websites were spread via networks of inauthentic social media accounts, including bots. Several methods were used to establish boundaries around target users, avoid mapping of the infrastructure by third parties and circumvent moderation rules. Using sponsored content that could only be seen by a targeted group of users chosen by a page's administrator, the perpetuators leveraged the geofencing technique to redirect users to specific content depending on their location. Also, URLs were redirecting traffic several times before reaching their target site.

10.6 'CHEAP FAKES' AND AI-ENABLED MANIPULATION OF INFORMATION

In line with our observations from the 2021 and 2022 reports, AI-enabled manipulation of information continues to be a concern. In the past months, the debate on the use of AI to manipulate information has heated up both within and beyond the circle of industry professionals[849]. In particular, they have been fuelled by the emergence of easy-to-access and easy-to-use AI tools able to generate very realistic images or authoritative-sounding text based on user prompts. It is worth noting that, according to some experts, the generation of false or misleading content using AI (e.g. deepfakes) might not be the main issue: for example, people and organisations developed 'defensive mechanisms' to react to the novelty represented by photo editing applications in the past. However, the speed, volume and scale at which false or misleading content is generated and diffused remains worrisome[850] [851]. In particular, the diffusion and effectiveness of campaigns could be amplified by the ability of AI to provide one-to-one interactive disinformation and tailored disinformation[852] [853].

The graph below summarises the potential impact of AI on the three dimensions of campaigns of information manipulation, namely the actors waging the campaigns, their behaviours and the content[854].

[848] An overview of the campaign, as well as the technical report can be found here: https://www.sgdsn.gouv.fr/publications/maj-19062023-rrn-une-campagne-numerique-de-manipulation-de-linformation-complexe-et (Accessed 18/08/2023). The technical report is also published in STIX via GitHub: https://github.com/VIGINUM-FR/Rapports-Techniques

[849] For example, concerns about AI-enabled disinformation have been raised also in the context of the negotiations on the proposed EU Regulation on AI (so called 'AI Act'): https://www.politico.eu/article/eu-plan-regulate-chatgpt-openai-artificial-intelligence-act/?utm_source=substack&utm_medium=email (Accessed 31/07/2023).

[850] https://reutersinstitute.politics.ox.ac.uk/news/will-ai-generated-images-create-new-crisis-fact-checkers-experts-are-not-so-sure (Accessed on 31/07/2023).

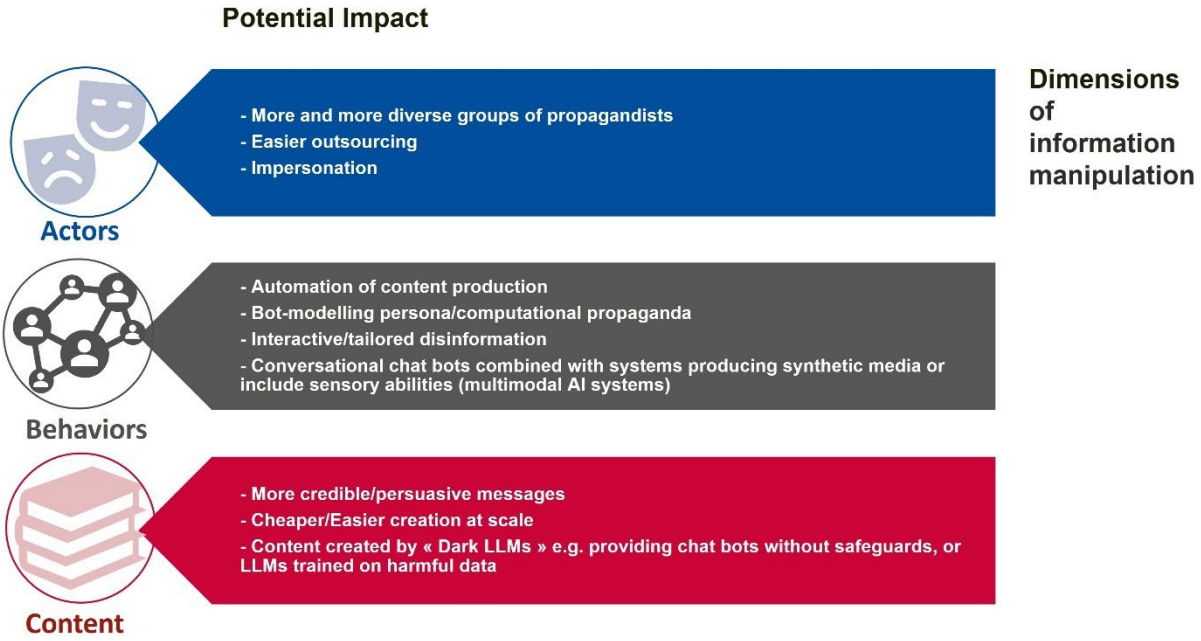
[851] https://www.wired.com/story/400-dollars-to-build-an-ai-disinformation-machine/ (Accessed 03/10/2023)

[852] https://www.washingtonpost.com/technology/2023/05/16/sam-altman-open-ai-congress-hearing/

[853] https://www.theguardian.com/technology/2023/may/20/elections-in-uk-and-us-at-risk-from-ai-driven-disinformation-say-experts (Accessed 18/08/2023).

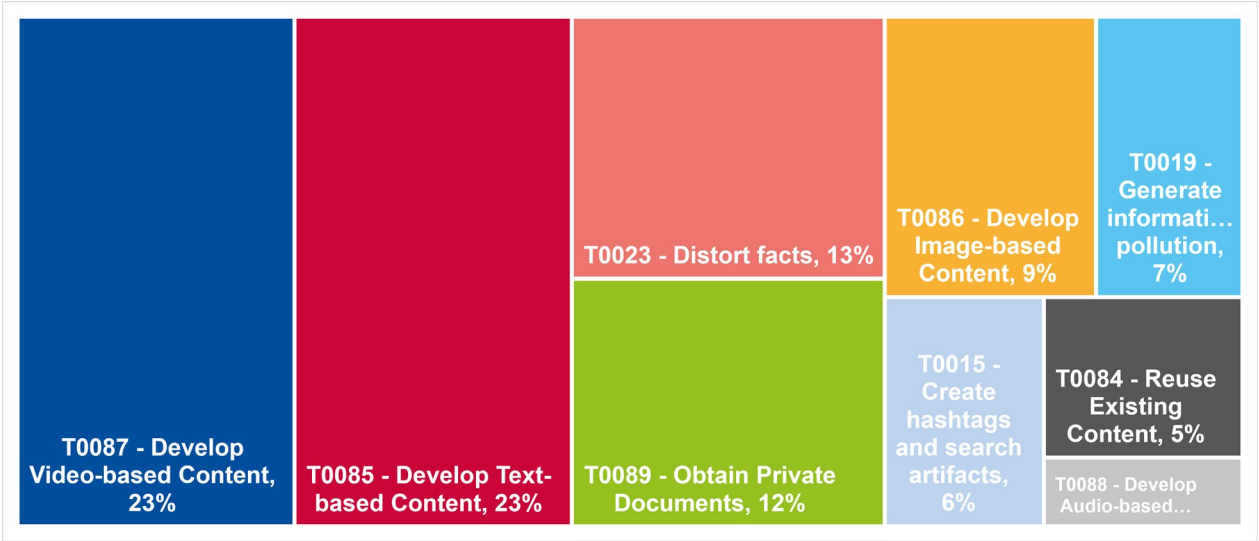
[854] The graph is adapted from the following paper, which focuses on generative language models: Generative Language Models and Automated Influence Operations: Emerging Threats and Potential Mitigations' (2023) – https://doi.org/10.48550/arXiv.2301.04246. It has been complemented with additional sources: ENISA Threat Landscape (2021, 2022); ENISA Foresight Cybersecurity Threats for 2030; S. Altman Congress Hearing (2023); ChatGPT - The impact of Large Language Models on Law Enforcement (Europol, 2023).

Figure 44: Potential impact of AI on the manipulation of information



Unsurprisingly, the development of content is the most recurrent DISARM tactic (see Figure 40), with the development of video- and text-based content amounting to almost half of the techniques used. According to MITRE ATT&CK data manipulation accounts for more than 20% of all techniques identified[855] and it is the most used technique within the MITRE ATT&CK impact tactic.

Figure 45: DISARM - Distribution of techniques within the tactic TA06 – Develop content



The power of a deepfake on a large scale was evident in May when a fake image of an explosion in the Pentagon on Twitter influenced stock markets and impacted Wall Street[856].

[855] MITRE ATT&CK's definition of data manipulation is 'adversaries may insert, delete or manipulate data in order to influence external outcomes or hide activity, thus threatening the integrity of the data. In the context of this chapter, data manipulation has been applied to, for example, reframed content, content misleadingly showing as originating from a legitimate source.
[856] https://www.euronews.com/next/2023/05/23/fake-news-about-an-explosion-at-the-pentagon-spreads-on-verified-accounts-on-twitter.

However, despite the fact that several apparent AI-enabled deepfake videos have emerged particularly in the context of the war of aggression towards Ukraine[857] [858], the incidents analysed have not revealed sufficient information to assess conclusively whether the potential misuse of AI on an exponential scale has to date materialised. When it comes to behaviours, the incidents analysed show that the creation of inauthentic accounts and the use of bots to spread manipulated information are common, as previously discussed. Concerning the content, while information manipulation has often included allegedly leaked documents or images, these seem to be rather 'cheap fakes' or 'shallow fakes' (intended as mis-contextualised or repurposed media or media created with cheap software tools) in continuation with the past[859]. While it is not clear that, in these cases, AI has been leveraged, it cannot be excluded; AI-generated websites and information sites operating with little to no human oversight are an existing practice[860].

In parallel, technologies to detect and counter the use of AI for the manipulation of information have been researched and developed[861] [862]. In particular, there is the notion that AI-based tools will be key in the defence against AI-enabled disinformation, possibly leading to an 'arms race' between detection and manipulation tools[863] [864], although the outcome is still to be seen[865].

10.7 COMMODIFICATION OF INFORMATION MANIPULATION

The 2021 and 2022 ETLs explained the rise of 'Disinformation-as-a-Service' or 'Disinformation-for-Hire, where third parties deliver targeted attacks on behalf of clients. The trend continues to be observed.

Earlier this year, for example, a journalistic investigation revealed a team of Israeli contractors who claim to have manipulated more than 30 elections, on behalf of intelligence agencies, political campaigns and private companies, via hacking and automated disinformation on social media. According to the investigation, the team seems to avail of software that controls more than 30,000 fake social media profiles[866] and uses hacking to penetrate Telegram and Gmail accounts[867].

Also, Russia's military aggression sheds more light on other business cases, for example: 'information laundering' to pump out propaganda through a third party and dissimulate Russian-affiliated sources[868], information manipulation as part of mercenary services[869] [870], as well as information manipulation as part of a broader service portfolio[871].

Lastly, another way of monetising the manipulation of information seems to be through advertisements: since internet business models reward engagement above all else and false information attracts more engagement than factual information[872]. The Global Disinformation Index estimates that the 40 US news websites on which disinformation narratives relating to the integrity of elections are most frequently published generate at least $42.7m per year in digital advertising revenue[873].

[857] https://www.bbc.com/news/technology-60780142.
[858] https://www.politico.eu/article/fake-vladimir-putin-announces-russia-under-attack-ukraine-war/.
[859] Deepfakes are solvable—but do not forget that 'shallow fakes' are already pervasive | MIT Technology Review.
[860] Tracking AI-enabled Misinformation: Over 350 'Unreliable AI-Generated News' Websites (and Counting), Plus the Top False Narratives Generated by Artificial Intelligence Tools - NewsGuard (newsguardtech.com) (Accessed 31/07/2023).
[861] https://www.europarl.europa.eu/RegData/etudes/STUD/2019/624279/EPRS_STU(2019)624279_EN.pdf.
[862] https://cordis.europa.eu/project/id/101070190.
[863] https://blogs.microsoft.com/eupolicy/2023/05/16/tech-talk-cyber-influence-cybersecurity-ai-dtac/ (accessed 31/07/2023).
[864] https://sites.google.com/view/blrm-fakenews/a-i-detection (accessed 31/07/2023).
[865] https://euvsdisinfo.eu/interview-with-ai-ethicist-dr-benjamin-lange/.
[866] https://www.theguardian.com/world/2023/feb/15/aims-software-avatars-team-jorge-disinformation-fake-profiles.
[867] https://www.theguardian.com/world/series/disinfo-black-ops (Accessed 16/08/2023).
[868] https://www.bbc.com/news/world-65150030 (Accessed 16/08/2023).
[869] https://www.consilium.europa.eu/en/press/press-releases/2023/04/13/russia-s-war-of-aggression-against-ukraine-wagner-group-and-ria-fan-added-to-the-eu-s-sanctions-list/?utm_source=dsms-auto&utm_medium=email&utm_campaign=Russia%27s%20war%20of%20aggression%20against%20Ukraine%3A%20Wagner%20Group%20and%20RIA%20FAN%20added%20to%20the%20EU%27s%20sanctions%20list#:~:text=The%20Wagner%20Group%20%2D%20already%20subject,and%20financed%20by%20Yevgeniy%20Prigozhin.
[870] https://www.reuters.com/world/europe/russias-prigozhin-admits-links-what-us-says-was-election-meddling-troll-farm-2023-02-14/.
[871] The Russian company 'Struktura National Technologies' (Struktura) is a company created in 2009 that specialises in the development of IT tools. A solution for «monitoring and analysing the information space» is just one among its developed products. https://www.sgdsn.gouv.fr/publications/maj-19062023-rrn-une-campagne-numerique-de-manipulation-de-linformation-complexe-et (Accessed 18/08/2023).
[872] https://www.oecd.org/ukraine-hub/policy-responses/disinformation-and-russia-s-war-of-aggression-against-ukraine-37186bde/ (Accessed 16/08/2023).
[873] https://www.disinformationindex.org/research/2022-11-08-ad-funded-elections-integrity-disinformation/.

10.8 POLITICAL INITIATIVES AND WORK ON THE GROUND

In parallel with the trends highlighted, numerous high-level political initiatives to counter the manipulation of information are gaining momentum.

At the international level, for example, both the G7 Hiroshima Summit[874] and the Ministerial meeting of the Trade and Technology Council[875] identified, in May 2023, foreign information manipulation and interference as a key issue to be addressed.

At the EU level, several actions have been undertaken, to name a few.

- The Code of Practice on Disinformation, through which relevant players in the industry agreed on self-regulatory standards against disinformation, has been revised and a strengthened version was presented in June 2022[876].
- The EU Regulation known as the 'Digital Services Act' (DSA) entered into force in November 2022. Among other requirements, the DSA contains measures to counter illegal content online, as well as imposing obligations on very large online platforms to mitigate several risks, including those of disinformation or the manipulation of elections[877].
- In the context of Russia's invasion of Ukraine, in July 2023, the Council decided to impose restrictive measures against seven Russian individuals and five entities responsible for conducting a digital campaign of information manipulation[878]. This followed other measures, such as the 2022 sanctions suspending the broadcasting activities of Sputnik and RT/Russia Today in the EU[879].

On a more technical level, we noted the emergence of different analytical frameworks to support a structured data collection and/or structured analysis of information manipulation in its various conceptualisations. Besides the DISARM framework, which has been used in this chapter, numerous new initiatives have been put forward, for example:

- in November 2022 the NATO Strategic Communications Centre of Excellence proposed a capability assessment framework for countering disinformation, information influence and foreign interference[880];
- the 1st EEAS Report on Foreign Information Manipulation and Interference Threats, establishing analytical workflows and processes to enable quantifiability of threats and interoperability of FIMI research[881].
- the OASIS Open project "Common Data Model for Defending Against Disinformation (DAD-CDM)" was launched to develop an open standard for data entities and objects needed to capture, analyse and exchange threat, source and mitigation data relating to disinformation. The project aims to extend STIX for FIMI[882].
- the European Commission's Joint Research Centre and the European Centre of Excellence for Countering Hybrid Threats have proposed a Comprehensive Resilience Ecosystem (CORE) to counter hybrid threats, including disinformation[883];
- the publication of "Guidelines for Public Interest OSINT Investigations" ("OSINT Guidelines") by like-minded organisations. The guidelines provide organisations conducting open-source investigations with a framework of good practices in methodology, tools, skills, documentation and working environments[884].

[874] https://www.consilium.europa.eu/media/64497/g7-2023-hiroshima-leaders-communiqu%C3%A9.pdf.
[875] https://ec.europa.eu/commission/presscorner/detail/en/statement_23_2992.
[876] https://digital-strategy.ec.europa.eu/en/policies/code-practice-disinformation (Accessed 19/08/2023).
[877] https://ec.europa.eu/commission/presscorner/detail/en/QANDA_20_2348 (Accessed 19/08/2023).
[878] https://www.consilium.europa.eu/en/press/press-releases/2023/07/28/information-manipulation-in-russia-s-war-of-aggression-against-ukraine-eu-lists-seven-individuals-and-five-entities/.
[879] https://www.consilium.europa.eu/en/press/press-releases/2022/03/02/eu-imposes-sanctions-on-state-owned-outlets-rt-russia-today-and-sputnik-s-broadcasting-in-the-eu/.
[880] https://stratcomcoe.org/publications/a-capability-definition-and-assessment-framework-for-countering-disinformation-information-influence-and-foreign-interference/255.
[881] https://www.eeas.europa.eu/eeas/1st-eeas-report-foreign-information-manipulation-and-interference-threats_en
[882] https://github.com/DAD-CDM
[883] https://publications.jrc.ec.europa.eu/repository/handle/JRC129019.
[884] https://obsint.eu/

- a newly published research paper designed an Online Operations Kill chain, an analytical framework that can be applied to a wide range of online operations from cyber-attacks to influence operations[885].

[885] https://carnegieendowment.org/2023/03/16/phase-based-tactical-analysis-of-online-operations-pub-89275.

11. SUPPLY CHAIN ATTACKS

A **supply chain attack** targets the relationship between organisations and their suppliers. For this ETL we use the definition used in the ENISA Threat Landscape for Supply Chain Attacks report[886] where an attack is considered a supply chain attack when it consists of a **combination** of at least **two attacks;** more specifically, a first attack on a supplier that is then used to attack a target to gain access to its assets. This target can be the final customer or another supplier. Thus, for an attack to be classified as a supply chain attack, both the supplier and the customer have to be targets.

This definition also **excludes** those incidents where, for example, developer libraries were compromised but without the goal of targeting a **specific** victim. We will cover these incidents briefly because of the abundance of reports of these incidents as 'supply chain attacks' but we do not consider them as part of this threat landscape.

As stated in the previous reporting period, threat actors have realised that the critical role hardware and software suppliers play provides them with ample means to use one incident to have an impact at multiple organisations. This was painfully demonstrated during the supply chain attacks following the start of the war in Ukraine, especially by the compromise of 3CX VoIP software[887]. And although supply chain attacks can be used to initiate some form of disruption, there is an increased tendency to employ them for intelligence gathering.

Despite the actions taken by the industry to protect supply chains, during the reporting period we witnessed several incidents. More specifically, the following trends are emerging.

11.1 SUPPLY CHAIN ATTACKS RELATED TO THE WAR IN UKRAINE

The war in Ukraine continues to have an effect on supply chain security. The NSA[888] concluded that hackers associated with Russia are targeting Ukrainian and European supply chains to **disrupt the flow of humanitarian goods** and **lethal aid** into Ukraine. A prime example is the Prestige ransomware campaign[889] against organisations in the transportation and coordination industries and the modified[890] version of the GoMet[891] **backdoor** destined for a large software development company whose software is used in state organisations within Ukraine. An even bolder move is the distribution[892] of trojanised installers of the Windows 10 operating system distributed via Torrent sites. The installers use the Ukrainian language pack and are designed to target Ukrainian users in order to conduct **reconnaissance** and **data theft**. Based on reports, the victims were 'handpicked' and included Ukrainian government organisations. In another twist, there is news[893] that Ukrainian radio stations were hacked to spread lies about Ukrainian President Zelensky.

Shortly after the war broke out everyone was concerned about highly disruptive and destructive cyberattacks against Ukraine's critical infrastructure. Although Russia associated groups have increased[894] the volume of their attacks, there are few reports of a major incident to date. It is very likely that the volume of attacks, including those aimed at supply chains, will persist and possibly worsen. We expect that supply chain attacks related to the war will primarily

[886] ENISA Threat Landscape for Supply Chain Attacks https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks.
[887] https://www.wired.com/story/3cx-supply-chain-attack-times-two/
[888] Cyberscoop - NSA sees 'significant' Russian intel gathering on European, USA supply chain entities – https://cyberscoop.com/nsa-russian-ukraine-supply-chain-ransomware/.
[889] Microsoft - New Prestige' ransomware impacts organisations in Ukraine and Poland - https://www.microsoft.com/en-us/security/blog/2022/10/14/new-prestige-ransomware-impacts-organizations-in-ukraine-and-poland/.
[890] Cisco Talos - Attackers target Ukraine using GoMet backdoor - https://blog.talosintelligence.com/attackers-target-ukraine-using-gomet/.
[891] https://github.com/Laeeth/GoMet.
[892] Mandiant - Trojanised Windows 10 Operating System Installers Targeted Ukrainian Government - https://www.mandiant.com/resources/blog/trojanized-windows-installers-ukrainian-government.
[893] Cybernews - Ukrainian radio stations hacked to spread lies about Zelensky's health - https://cybernews.com/cyber-war/ukrainian-radio-stations-hacked-to-spread-lies-about-zelenskys-health/.
[894] Google TAG - Fog of war: how the Ukraine conflict transformed the cyber threat landscape - https://blog.google/threat-analysis-group/fog-of-war-how-the-ukraine-conflict-transformed-the-cyber-threat-landscape/.

focus on **espionage** as a means to gain a strategic advantage or on disinformation campaigns or focus on **disruption** via wipers and DDoS attacks.

11.2 TARGETING IDENTITY PROVIDERS

With the variety of applications and systems where users need to authenticate, organisations are evaluating options for managing access with, for example, managed identity providers. Attackers noticed this need and included these **identity providers** in their list of targets.

One of the prime targets is Okta. Okta suffered a major breach in March 2022 but the misfortune has continued. Attackers got hold of the source code of some of Okta's components on two occasions[895] [896], but according to the company there was no impact on its customers. Research[897] revealed weaknesses that can cause an Okta administrator to give themselves or someone else elevated rights as an impersonated user in another application or environment. This is an effective method of bypassing multi-factor authentication (MFA) as you are not forced to provide MFA verification under the context of the impersonated user. To accomplish this attack, miscreants still have to gain the initial credentials. One way to achieve this is via a campaign dubbed 0ktapus[898] where fraudsters conduct a **phishing campaign** to obtain Okta **identity credentials** and **multi-factor authentication codes**.

Attackers have used relatively low-skill methods to compromise a large number of well-known organisations. Various targeted phishing domains supported the Oktapus campaign, some using keywords such as 'okta', 'help', 'vpn' and 'sso'. Organisations such as Cloudflare[899], Doordash[900] and Twillio[901] reported being the target of such attacks. Signal[902] indicated that because of the breach at Twilio, attackers could have attempted to re-register a phone number to another device or could have learned that a number was registered to Signal. A great lesson learned is that although implementing MFA is strongly advised, there are ways for attackers to overcome this barrier with relatively simple tools.

Entrust, a company that provides identities, payments and data protection solutions, fell victim[903] to the ransomware gang LockBit. LockBit in turn accused Entrust of counterattacking[904] them, or at least DDoSsing their leak site. Symantec discovered[905] several popular banking apps relying on a vulnerable SDK for authentication. It is not uncommon to outsource the authentication components of an application but in this case Symantec discovered that within the SDK there were **cloud credentials** that could place entire infrastructures at risk. Additionally, biometric digital fingerprints for authentication and personal data from users were also exposed in the cloud. The Dutch company ID-ware fell victim[906] to a ransomware incident. ID-ware provides smartcards that can be used to verify your identity to get access to facilities.

It is likely we will continue to see attacks on identity providers and associated services. It is very likely that threat actors will focus on **disruption** and **stealing data**. And although authentication details are an alluring target, personal data or data on access rights are useful as well. Despite the fact that there are plenty of security measures to enhance the protection of managed identities, attackers will attempt to find ways to work around them. Previously we have seen attackers target identity providers via Golden SAML or Golden Ticket attacks, and although technically different, this is a continuation on the same theme.

[895] Auth0 - Auth0 Code Repository Archives From 2020 and Earlier - https://auth0.com/blog/auth0-code-repository-archives-from-2020-and-earlier/.
[896] Okta - Okta Code Repositories - https://sec.okta.com/articles/2022/12/okta-code-repositories.
[897] Permiso – You down with IDP? Impersonate me! – https://permiso.io/blog/s/down-with-idp-impersonate-me/.
[898] Group IB - Roasting Oktapus: The phishing campaign going after Okta identity credentials - https://www.group-ib.com/blog/0ktapus/.
[899] Cloudflare - The mechanics of a sophisticated phishing scam and how we stopped it - https://blog.cloudflare.com/2022-07-sms-phishing-attacks/.
[900] Doordash - How we're responding to a third-party vendor phishing incident - https://doordash.news/get-the-facts/how-were-responding-to-a-third-party-vendor-phishing-incident/.
[901] Twilio - Incident Report: Employee and Customer Account Compromise - https://www.twilio.com/blog/august-2022-social-engineering-attack.
[902] Signal - Twilio Incident: What Signal Users Need to Know - https://support.signal.org/hc/en-us/articles/4850133017242.
[903] Bleeping Computer - LockBit claims ransomware attack on security giant Entrust, leaks data - https://www.bleepingcomputer.com/news/security/lockbit-claims-ransomware-attack-on-security-giant-entrust-leaks-data/.
[904] VXUnderground - https://twitter.com/vxunderground/status/1561262483448512513.
[905] Symantec - Mobile App Supply Chain Vulnerabilities Could Endanger Sensitive Business Information - https://symantec-enterprise-blogs.security.com/blogs/threat-intelligence/mobile-supply-chain-aws.
[906] Security.NL - https://www.security.nl/posting/770260/Priv%C3%A9data+duizenden+rijksambtenaren+gelekt+na+inbraak+op+servers+ID-ware.

11.3 ATTACKS ON SOFTWARE SUPPLY CHAINS

According to numerous reports, an astonishing 61% of companies have been impacted[907] by a software supply chain attack in the last twelve months and the total cost[908] of these attacks on businesses will grow by 76% in 2026 compared to 2023. Blackberry found that four in five IT decision-makers say[909] their organisation was notified of an attack or vulnerability in its software supply chain in the last twelve months. Apart from an ever-increasing list of interdependencies between applications, this research points out that the **sprawl of applications** makes it more difficult for organisations to stay in control of the applications they have deployed. The simple logic that the more applications you have, the more vulnerable you are, is certainly true. The number of vulnerabilities found in software and software libraries remains very high. In a lot of cases these vulnerabilities are **exploited indiscriminately**, meaning threat actors did not really consider the type of organisations to which they accidently gained access. In our definition of a supply chain attack the vendor (in this case the software supplier) must be breached with the intention of using that breach as a foothold into another environment. This means that those incidents that happened by 'sheer luck' do not classify as a software supply chain attack.

One incident [910] [911] where our definition is certainly applicable is the breach of the 3CX VoIP software. Financially motived hackers associated with North Korea used **compromised software** to go after just a handful of **crypto** firms, despite the potentially massive breadth of that attack. The 3CX Desktop app is enterprise software that provides communications for its users including chat, video calls and voice calls. The incident started with a previous software supply chain attack. In this prelude, attackers trojanised an installer for software provided by Trading Technologies. This trojanised version led to a backdoor, granting them access to the 3CX environment. Armed with this access, the attackers navigated within the 3CX network, harvested credentials and compromised the build environment for Windows and Mac, leading to a trojanised installer of the 3CX application. This trojanised installer in turn lead to a backdoor that further downloaded additional malicious code, eventually leading a data miner to the **steal browser information** of victims within the targeted environments. In summary, the incident was the result of two **cascading software supply chain compromises**.

We previously witnessed software supply chain attacks via the software update mechanism with NotPetya. During this reporting period there was continuing[912] [913] [914] activity by threat actors making use of software update mechanisms to deliver malware to victims.

Unfortunately, the software supply chain problem is not something that will be fixed overnight but there are actions by the industry to **tackle the problem** by improving **tooling**[915], raising **awareness**[916] and by sharing **best practices**[917] [918] [919]. Advanced monitoring and approaches to foster transparency such as the Software Bill of Materials[920] are of course supporting the strengthening of supply chains' cybersecurity.

[907] Capterra - Three in Five Businesses Affected by Software Supply Chain Attacks in Last 12 Months - https://www.capterra.com/resources/software-supply-chain-attacks/.
[908] Juniper - Vulnerable Software Supply Chains are a Multi-billion Dollar Problem - https://www.juniperresearch.com/whitepapers/vulnerable-software-supply-chains-problem.
[909] BlackBerry - Four in Five Software Supply Chains Exposed to Cyberattack in the Last 12 Months - https://blogs.blackberry.com/en/2022/10/four-in-five-software-supply-chains-exposed-to-cyberattack-in-last-12-months.
[910] Mandiant - 3CX Software Supply Chain Compromise Initiated by a Prior Software Supply Chain Compromise; Suspected North Korean Actor Responsible - https://www.mandiant.com/resources/blog/3cx-software-supply-chain-compromise.
[911] CISA - Supply Chain Attack Against 3CXDesktopApp - https://www.cisa.gov/news-events/alerts/2023/03/30/supply-chain-attack-against-3cxdesktopapp.
[912] ESET - Fantasy – a new Agrius wiper deployed through a supply-chain attack - https://www.welivesecurity.com/2022/12/07/fantasy-new-agrius-wiper-supply-chain-attack/.
[913] ESET - Evasive Panda APT group delivers malware via updates for popular Chinese software - https://www.welivesecurity.com/2023/04/26/evasive-panda-apt-group-malware-updates-popular-chinese-software/.
[914] ESET – ESET Research: Chinese-speaking Evasive Panda group spreads malware via updates of legitimate apps and targets NGO in China – https://www.eset.com/int/about/newsroom/press-releases/research/eset-research-chinese-speaking-evasive-panda-group-spreads-malware-via-updates-of-legitimate-apps-an/.
[915] OWASP - OWASP Foundation Announces CycloneDX Project Momentum with Contribution from IBM to Advance Software Supply Chain Security - https://owasp.org/blog/2023/03/01/ibm-contributes-two-open-source-projects-sbom-utility-and-license-scanner-to-cyclonedx.html.
[916] ENISA - Developing National Vulnerabilities Programmes - https://www.enisa.europa.eu/publications/developing-national-vulnerabilities-programmes.
[917] Fortra - What is CSAF (Common Security Advisory Framework)? - https://www.tripwire.com/state-of-security/what-csaf-common-security-advisory-framework.
[918] CIRCL - Open-source software security and threat detection - https://cra.circl.lu/pres/circl-misp-c4dt-presentation.pdf.
[919] Canadian Centre for Cyber Security - Protecting your organisation from software supply chain threats – ITSM.10.071 - https://www.cyber.gc.ca/en/guidance/protecting-your-organization-software-supply-chain-threats-itsm10071.
[920] https://www.cisa.gov/sbom

We expect that, despite the initiatives to solve the problem, the software supply chain **will remain vulnerable to attacks**. In general these attacks are opportunistic and not targeted. The objectives of these attacks are broad, ranging from cryptomining, ransomware, data exfiltration to espionage. The attack against 3CX however underlined the potential reach of these attacks. It also showed that determined and creative threat actors can exploit the weaknesses in the chain to achieve their objectives and remain undetected for a relatively long period of time.

11.4 IT SUPPLIERS AND MANAGED SERVICE PROVIDERS

It should come as no surprise that there was continual activity of supply chain attacks via IT suppliers. In general, these attacks cause **disruption**[921], sometimes with consequences felt by entire societies such as the widespread standstill[922] of the DSB train network. In some cases, threat actors move beyond disruption and attempt to **collect sensitive** customer **information** including user and server credentials. Mercury IT, a New Zealand-based managed service provider, was the victim[923] of a ransomware attack by Lockbit. The Lockbit gang did not limit itself to **disruption** by locking up systems, they also **stole** some confidential data belonging to the company's customers. The incident led to a public statement from the Office of the Privacy Commissioner in New Zealand on a plan[924] to start an investigation.

An increased[925] number of threat actors are targeting vulnerable **regional managed service providers** (MSPs) to conduct supply chain attacks against small and medium business (SMBs). These regional MSPs protect a large number of organisations but do not always have the resources to staff their security environment. The threat actors noticed this **imbalance** between potential **opportunities to gain access** into environments and the **level of the defensive measures** in place. One example are the campaigns from Muddywater, an actor associated with Iran, targeting Israeli regional MSPs via a phishing campaign.

Organisations expect their IT partner to be on top of security problems and to follow-up on changes in the threat landscape. Unfortunately, they often face similar problems as the organisations they work for, a shortage of staff, limited resources and complex environments. We expect that attacks on IT suppliers and MSPs will only expand, putting both service providers and their customers at risk. Attacks will not only focus on disruption but very likely also on the theft of information.

11.5 ATTACKS ON THE HARDWARE SUPPLY VECTOR

Adversaries linked to China were overwhelmingly targeting[926] Taiwan-based technology organisations during 2022. This behaviour is **consistent** with China's **economic espionage missions** in support of its goals for technological independence and dominance. In general it is to be expected that the various **geopolitical tensions** in the region will only increase[927] related targeting operations. To anticipate the fallout from such tensions, the European Commission launched[928] its Semiconductor Alert System, a new pilot system to monitor the semiconductor supply chain. This allows it to raise awareness of critical disruptions along the value chain for semiconductors and to react to potential crisis situations via the European Semiconductor Expert Group.

A ransomware incident[929] [930] with Micro-Star International or MSI could be a prelude for future supply chain attacks. The attackers not only obtained the company image signing keys but they also got hold of the private **encryption key** for Intel Boot Guard that is distributed by MSI to its customers. To complicate the problem further, there is no process to invalidate these stolen keys. The simple fact is that attackers can create fake update utilities and rogue firmware

[921] Heise - Cyber-Angriff auf IT-Dienstleister Materna https://www.heise.de/news/Cyber-Angriff-auf-IT-Dienstleister-Materna-8155606.html.
[922] Reuters – Danish train standstill on Saturday caused by cyberattack – https://www.reuters.com/technology/danish-train-standstill-saturday-caused-by-cyber-attack-2022-11-03/.
[923] Insurance Business - Loot from NZ ransomware attack being sold on dark web - https://www.insurancebusinessmag.com/nz/news/cyber/loot-from-nz-ransomware-attack-being-sold-on-dark-web-431229.aspx.
[924] NZ Privacy Commissioner – considers action on ransomware attack – https://www.privacy.org.nz/publications/statements-media-releases/new-news-page-5/.
[925] Proofpoint - Account Compromise, Financial Theft, and Supply Chain Attacks: Analysing the Small and Medium Business APT Phishing Landscape in 2023 - https://www.proofpoint.com/us/blog/threat-insight/small-and-medium-business-APT-phishing-landscape-in-2023.
[926] Crowdstrike - 2023 Global Threat Report - https://www.crowdstrike.com/global-threat-report/.
[927] PWC - Cyber Threats 2022: A Year in Retrospect - https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/pdf/2022-year-in-retrospect-report.pdf.
[928] EC - European Chips Act: Commission launches pilot system to monitor semiconductor supply chain - https://digital-strategy.ec.europa.eu/en/news/european-chips-act-commission-launches-pilot-system-monitor-semiconductor-supply-chain.
[929] Bleeping Computer - Money Message ransomware gang claims MSI breach, demands $4 million - https://www.bleepingcomputer.com/news/security/money-message-ransomware-gang-claims-msi-breach-demands-4-million/.
[930] Ars Technica - Leak of MSI UEFI signing keys stokes fears of 'doomsday' supply chain attack - https://arstechnica.com/information-technology/2023/05/leak-of-msi-uefi-signing-keys-stokes-concerns-of-doomsday-supply-chain-attack/.

and they will successfully pass all verifications setup by MSI. Because this happens outside an operating system, it would be extremely hard for malware protection solutions to detect malicious activity related to these changes. Luckily, the abuse is technically complex and an attacker needs to have local access to a vulnerable system. According[931] to the Dutch NCSC however it is not inconceivable that the leaked keys will be misused in targeted attacks.

We expect that attacks against hardware supply vendors, especially those in the semiconductor sector, will only increase in volume and sophistication, certainly given geopolitical tensions. Previous events demonstrated that a **disruption in the fabrication of critical components** for the technology on which our society relies can have severe consequences.

11.6 THIRD-PARTY CONNECTED APPS

According to Adaptive Shield, there is an average[932] of 4 371 connected apps in a typical 10 000 Software-as-a-Service or SaaS user organisations connected to both Microsoft Office 365 and Google Workspace. Over 89% of third-party apps connected to Google Workspace and 67% of apps connecting to M365 represent a high or medium risk to a company's data. Unfortunately, a lot of these third-party connected apps are granted **high-risk permissions**, which allows them to access or manipulate corporate data. Whereas connected apps mostly concern all employees, there is a section of the workforce that faces a risk specific for their work environment. IT teams and developers are increasingly[933] authorising third-party apps to access the organisation's code repositories. These integrations are often done with good intentions and boost productivity but are not always properly controlled by security teams.

The high volume of applications connected to third parties will cause a lot of headaches to companies, especially if they are granted elevated privileges.

11.7 USE OF EMPLOYEES AS ENTRY POINTS

Incidents during the reporting period indicate that threat actors focus on employees as an entry point in organisations.

A major incident that made headlines was the breach[934] [935] of LastPass. The company suffered from a severe **data breach** caused by two related security incidents that allowed threat actors to **access encrypted password vaults**. In this incident one of the LastPass engineers had their personal home computer hacked and infected with a keylogger. This allowed the attackers to steal credentials and access some of the password manager's source code and proprietary information. Consequently, the attackers accessed a third-party cloud storage service used by LastPass and were able to gain access to certain elements of customers' information.

Another incident concerned[936] [937] a **data breach** at CircleCI, provider of the popular CI/CD platform. Attackers gained access to a laptop belonging to a CircleCI engineer and used malware to steal an MFA backed single sign-on (SSO) session cookie. This cookie allowed the attackers to impersonate the engineer in a remote session and gave them access to CircleCI production systems. Eventually this resulted in the exfiltration of a subset of customer data, including tokens and keys.

Threat actors will continue to target employees with elevated privileges such as developers or system administrators. This can be via their personal devices outside business hours when they are maybe less vigilant or via social media channels.

[931] NCSC-NL - https://advisories-ncsc-nl.translate.goog/advisory?id=NCSC-2023-0235&_x_tr_sl=auto&_x_tr_tl=en&_x_tr_hl=en-US.
[932] Adaptive Shield - Uncovering the Risks & Realities of Third-Party Connected Apps - https://www.adaptive-shield.com/saas-to-saas-3rd-party-app-risk-report-2023.
[933] Astrix - Insecure third-party connections to your GitHub may trigger a supply chain attack - https://astrix.security/insecure-third-party-connections-to-your-github-may-trigger-a-supply-chain-attack/.
[934] LastPass – Security Incident Update and Recommended Actions – https://blog.lastpass.com/2023/03/security-incident-update-recommended-actions/.
[935] Ars Technica - LastPass says employee's home computer was hacked and corporate vault taken - https://arstechnica.com/information-technology/2023/02/lastpass-hackers-infected-employees-home-computer-and-stole-corporate-vault/.
[936] CircleCI – CircleCI incident report for January 4, 2023 security incident – https://circleci.com/blog/jan-4-2023-incident-report/.
[937] SC Media - Three lessons for DevOps from the CircleCI breach - https://www.scmagazine.com/perspective/devops/three-lessons-for-devops-from-the-circleci-breach.

11.8 LOG4SHELL

The Log4Shell vulnerability was one of the prime vulnerabilities identified during the previous reporting period. And although according to our definition of supply chain attacks, Log4Shell is not considered as a supply chain attack, we included it in our reporting. The vulnerability **has remained a significant threat** for organisations. Threat actors continue abusing the vulnerability for initial access[938] [939] [940], often via exposed VMware Horizon or unified access gateways. The Log4Shell vulnerability is something we will have to learn to live with and take into account when building our defences. As such, Log4Shell is declared[941] an 'endemic vulnerability'.

11.9 USE OF AI TO IMPROVE SOFTWARE SUPPLY CHAIN

During this reporting period artificial intelligence (AI) or Large Language Models (LLMs) received a lot of attention. There are not many public reports where this technology was used during supply chain attacks but the few that exist do provide interesting ways for the affected parts of the supply chain to improve their development environment.

A number of AI coding tools, such as GitHub Copilot[942] or Amazon CodeWhisperer[943] exist that can be used by developers to improve their code. And while we tend to focus on the code-generation capabilities of these tools, there are better and more reliable areas for using them: **software testing**. In general software testing is time-consuming and sometimes done hastily as it can slow down the development process. And it is exactly in this area that AI coding tools can be of great value, taking away some of the tedious tasks. This does not mean that testing should only be done by AI. These solutions are to be considered[944] as complementary tools to improve software supply chain security, both for code testing and for identifying logical flaws.

[938] CISA - Iranian Government-Sponsored APT Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvester - https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-320a.
[939] Cisco Talos - Lazarus and the tale of three RATs - https://blog.talosintelligence.com/lazarus-three-rats/.
[940] CISA - Malicious Cyber Actors Continue to Exploit Log4Shell in VMware Horizon Systems - https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-174a.
[941] CSRB - Review of the December 2021 Log4j Event - https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf.
[942] https://github.com/features/copilot.
[943] https://aws.amazon.com/codewhisperer/.
[944] InfoSecurity - ChatGPT Leveraged to Enhance Software Supply Chain Security - https://www.infosecurity-magazine.com/news/chatgpt-software-supply-chain/.

A ANNEX: MAPPING TO MITRE ATT&CK FRAMEWORK

RANSOMWARE

The current table highlights the techniques in the MITRE ATT&CK® Framework associated with ransomware software, ransomware groups or both, according to Ransomware techniques in ATT&CK[945]. Note that this is a dynamic representation based on actual observations. These can change over time as groups evolve and use new techniques. Every threat actor uses its own specific tools and attack patterns. This overview groups all common techniques, starting from initial access.

Tactic	Technique	Mitigation
TA0001: Initial Access	T1190: Exploit Public-Facing Application T1133: External Remote Services T1566: Phishing T1199: Trusted Relationship	M1048: Application Isolation and Sandboxing M1050: Exploit Protection M1030: Network Segmentation M1026: Privileged Account Management M1051: Update Software M1016: Vulnerability Scanning M1042: Disable or Remove Feature or Program M1035: Limit Access to Resource Over Network M1032: Multi-factor Authentication M1049: Antivirus/Antimalware M1031: Network Intrusion Prevention M1021: Restrict Web-Based Content M1054: Software Configuration M1017: User Training M1018: User Account Management
TA0002: Execution	T1106: Native API T1047: Windows Management Instrumentation	M1040: Behaviour Prevention on Endpoint M1038: Execution Prevention M1026: Privileged Account Management M1018: User Account Management
TA0003: Persistence	T1197: BITS Jobs T1554: Compromise Client Software Binary T1136: Create Account T1133: External Remote Services	M1037: Filter Network Traffic M1028: Operating System Configuration M1018: User Account Management M1045: Code Signing M1030: Network Segmentation M1032: Multi-factor Authentication M1026: Privileged Account Management M1042: Disable or Remove Feature or Program M1035: Limit Access to Resource Over Network
TA0004: Privilege Escalation	T1134: Access Token Manipulation T1068: Exploitation for Privilege Escalation T1055: Process Injection	M1018: User Account Management M1026: Privileged Account Management M1048: Application Isolation and Sandboxing

[945] Ransomware techniques in ATT&CK, https://healthcyber.mitre.org/blog/resources/attack-navigator/

		M1050: Exploit Protection M1051: Update Software M1038: Execution Prevention M1019: Threat Intelligence Program M1040: Behaviour Prevention on Endpoint
TA0005: Defence Evasion	T1134: Access Token Manipulation T1197: BITS Jobs T1140: Deobfuscate/Decode Files or Information T1480: Execution Guardrails T1036: Masquerading T1112: Modify Registry T1027: Obfuscated Files or Information T1055: Process Injection T1620: Reflective Code Loading T1497: Virtualisation/Sandbox Evasion	M1018: User Account Management M1026: Privileged Account Management M1037: Filter Network Traffic M1028: Operating System Configuration M1055: Do Not Mitigate M1049: Antivirus/Antimalware M1040: Behaviour Prevention on Endpoint M1045: Code Signing M1038: Execution Prevention M1022: Restrict File and Directory Permissions M1024: Restrict Registry Permissions M1047: Audit
TA0006: Credential Access	T1555: Credentials from Password Stores T1539: Steal Web Session Cookie	M1027: Password Policies M1032: Multi-factor Authentication M1054: Software Configuration M1017: User Training
TA0007: Discovery	T1087: Account Discovery T1217: Browser Bookmark Discovery T1135: Network Share Discovery T1069: Permission Groups Discovery T1057: Process Discovery T1012: Query Registry T1518: Software Discovery T1614: System Location Discovery T1033: System Owner/User Discovery T1124: System Time Discovery T1497: Virtualisation/Sandbox Evasion	M1028: Operating System Configuration
TA0008: Lateral Movement	T1210: Exploitation of Remote Services T1080: Taint Shared Content	M1050: Exploit Protection M1030: Network Segmentation M1026: Privileged Account Management M1016: Vulnerability Scanning M1042: Disable or Remove Feature or Program M1048: Application Isolation and Sandboxing M1051: Update Software M1019: Threat Intelligence Program M1038: Execution Prevention M1022: Restrict File and Directory Permissions
TA0009: Collection	T1560: Archive Collected Data T1530: Data from Cloud Storage Object T1213: Data from Information Repositories T1039: Data from Network Shared Drive T1113: Screen Capture	M1047: Audit M1018: User Account Management M1037: Filter Network Traffic M1022: Restrict File and Directory Permissions M1032: Multi-factor Authentication M1041: Encrypt Sensitive Information M1017: User Training

TA0011: Command and Control	T1568: Dynamic Resolution T1095: Non-Application Layer Protocol T1071: Non-Standard Port T1072: Protocol Tunnelling T1090: Proxy T1102: Web Service	M1031: Network Intrusion Prevention M1021: Restrict Web-Based Content M1030: Network Segmentation M1037: Filter Network Traffic M1015: Active Directory Configuration M1032: Multi-factor Authentication M1027: Password Policies M1026: Privileged Account Management M1029: Remote Data Storage M1051: Update Software M1018: User Account Management M1017: User Training M1020: SSL/TLS Inspection
TA0010: Exfiltration	T1041: Exfiltration Over C2 Channel	M1031: Network Intrusion Prevention M1057: Data Loss Prevention
TA0040: Impact	T1485: Data Destruction T1499: Endpoint Denial of Service T1489: Service Stop	M1053: Data Backup M1037: Filter Network Traffic M1030: Network Segmentation M1022: Restrict File and Directory Permissions M1024: Restrict Registry Permissions M1018: User Account Management

MALWARE (PEGASUS FOR ANDROID)

The current table highlights the techniques in the MITRE ATT&CK® Framework (Mobile) associated with the Pegasus spyware. The Pegasus[946] for Android is the Android version of malware that has reportedly been linked to the NSO Group (Update August 2022).

Tactic	Technique	Mitigation
TA0035: Collection	T1429: Audio Capture	M1006: Use Recent OS Version M1011: User Guidance
TA0028: Persistence	T1645: Compromise Client Software Binary	M1002: Attestation M1003: Lock Bootloader M1001: Security Updates M1004: System Partition Integrity
TA0028: Persistence	T1624.001: Event Triggered Execution: Broadcast Receivers	M1006: Use Recent OS Version
TA0029: Privilege Escalation	T1404: Exploitation for Privilege Escalation	M1002: Attestation M1010: Deploy Compromised Device Detection Method M1001: Security Updates
TA0037: Command and Control	T1644: Out of Band Data	M1011: User Guidance

[946] https://attack.mitre.org/techniques/T1587/001/

TA0035: Collection	T1636.001: Protected User Data: Calendar Entries	M1011: User Guidance
TA0035: Collection	T1636.002: Protected User Data: Call Log	M1011: User Guidance
TA0035: Collection	T1636.003: Protected User Data: Contact List	M1011: User Guidance
TA0032: Discovery	T1418: Software Discovery	M1006: Use Recent OS Version M1011: User Guidance
TA0035: Collection	T1409: Stored Application Data	M1006: Use Recent OS Version
TA0032: Discovery	T1422: System Network Configuration Discovery	M1006: Use Recent OS Version
TA0035: Collection	T1512: Video Capture	M1006: Use Recent OS Version

SOCIAL ENGINEERING

The current table highlights the techniques in the MITRE ATT&CK® Framework associated with social engineering. Note that this is a dynamic representation based on actual observations. These can change over time as groups evolve and use new techniques. Every threat actor uses its own specific tools and attack patterns. This overview groups all common techniques relevant to social engineering. We do not include the techniques commonly used for follow-up activity (including for example the methods showing how malicious documents can be executed.

Tactic	Technique	Mitigation
TA0043: Reconnaissance	T1595: Active Scanning T1592: Gather Victim Host Information T1589: Gather Victim Identity Information T1590: Gather Victim Network Information T1591: Gather Victim Org Information T1598: Phishing for Information T1597: Search Closed Sources T1596: Search Open Technical Databases T1593: Search Open Websites/Domains T1594: Search Victim-Owned Websites	M1056: Pre-compromise M1054: Software Configuration M1017: User Training M1013: Application Developer Guidance M1047: Audit
TA0042: Resource Development	T1583: Acquire Infrastructure T1586: Compromise Accounts T1584: Compromise Infrastructure T1587: Develop Capabilities T1585: Establish Accounts T1588: Obtain Capabilities T1608: Stage Capabilities	M1056: Pre-compromise
TA0001: Initial Access	T1133: External Remote Services T1566: Phishing T1199: Trusted Relationship T1078: Valid Accounts	M1035: Limit Access to Resource Over Network M1032: Multi-factor Authentication M1030: Network Segmentation M1042: Disable or Remove Feature or Program M1031: Network Intrusion Prevention M1021: Restrict Web-Based Content M1054: Software Configuration

		M1049: Antivirus/Antimalware M1017: User Training M1018: User Account Management M1036: Account Use Policies M1015: Active Directory Configuration M1013: Application Developer Guidance M1027: Password Policies M1026: Privileged Account Management
TA0002: Execution	T1204: User Execution	M1040: Behaviour Prevention on Endpoint M1038: Execution Prevention M1031: Network Intrusion Prevention M1021: Restrict Web-Based Content M1017: User Training

THREATS AGAINST DATA

The anatomy of data exfiltration is depicted in the following table, which includes the techniques that may be used in each kill chain phase and lead to data exfiltration or data breach or identity theft. The construction of the table is based on the MITRE ATT&CK®947 knowledge base. MITRE ATT&CK® provides information regarding the behaviour of cyber adversaries and a taxonomy of adversarial actions. The techniques leading to data exfiltration were selected using the MITRE ATT&CK® part for Enterprise, which covers behaviours against enterprise IT networks and the cloud.

DATA EXFILTRATION

Tactic	Technique	Mitigation
TA0003: Persistence	T1197: BITS Jobs	M1018: User Account Management M1028: Operating System Configuration M1037: Filter Network Traffic
TA0005: Defence Evasion	T1197: BITS Jobs T1599: Network Boundary Bridging	M1018: User Account Management M1028: Operating System Configuration M1037: Filter Network Traffic M1026: Privileged Account Management M1032: Multi-factor Authentication M1027: Password Policies M1037: Filter Network Traffic M1043: Credential Access Protection
TA0009: Collection	T1560: Archive Collected Data T1005: Data from Local System T1039: Data from Network Shared Drive T1025: Data from Removable Media T1074: Data Staged	M1047: Audit M1057: Data Loss Prevention
TA0010: Exfiltration	T1020: Automated Exfiltration T1048: Exfiltration Over Alternative Protocol T1041: Exfiltration Over C2 Channel	M1030: Network Segmentation M1018: User Account Management M1031: Network Intrusion Prevention M1037: Filter Network Traffic M1057: Data Loss Prevention

947 MITRE ATT&CK®, https://attack.mitre.org/

	T1011: Exfiltration Over Other Network Medium T1052: Exfiltration Over Physical Medium T1567: Exfiltration Over Web Service T1029: Scheduled Transfer T1537: Transfer Data to Cloud Account	M1022: Restrict File and Directory Permissions M1028: Operating System Configuration M1042: Disable or Remove Feature or Program M1034: Limit Hardware Installation M1021: Restrict Web-Based Content M1027: Password Policies

THREATS AGAINST AVAILABILITY (DDOS)

The anatomy of Denial of Services attacks and web attacks are depicted in the following figures, which includes the techniques that may be used in each kill chain phase. The table is constructed based on the MITRE ATT&CK®[948] knowledge base. MITRE ATT&CK® provides information regarding the behaviour of cyber adversaries and a taxonomy of adversarial actions. The techniques are selected using the MITRE ATT&CK® part for Enterprise, which covers behaviours against enterprise IT networks and the cloud.

Tactic	Technique	Mitigation
TA0042: Resource Development	T1583: Acquire Infrastructure T1584: Compromise Infrastructure	M1056: Pre-compromise
TA0005: Defence Evasion	T1553: Subvert Trust Controls	M1038: Execution Prevention M1028: Operating System Configuration M1024: Restrict Registry Permissions M1054: Software Configuration
TA0040: Impact	T1485: Data Destruction T1489: Service Stop T1499: Endpoint Denial of Service T1498: Network Denial of Service	M1053: Data Backup M1030: Network Segmentation M1022: Restrict File and Directory Permissions M1024: Restrict Registry Permissions M1018: User Account Management M1037: Filter Network Traffic

THREATS AGAINST AVAILABILITY- INTERNET THREATS

The current table highlights the techniques in the MITRE ATT&CK® Framework associated with ransomware software, ransomware groups or both according to the legend[949]. Note that this is a dynamic representation based on actual observations. These can change over time as groups evolve and use new techniques. Every threat actor uses its own specific tools and attack patterns. This overview groups all common techniques.

Tactic	Technique	Mitigation
TA0001: Initial Access	T1189: Drive-by Compromise	M1048: Application Isolation and Sandboxing M1050: Exploit Protection M1021: Restrict Web-Based Content M1051: Update Software

[948] MITRE ATT&CK®, https://attack.mitre.org/
[949] Ransomware techniques in ATT&CK, https://healthcyber.mitre.org/blog/resources/attack-navigator/

TA0007: Discovery	T1046: Network Service Scanning	M1042: Disable or Remove Feature or Program M1031: Network Intrusion Prevention M1030: Network Segmentation
TA0009: Collection	T1557: Adversary-in-the-Middle	M1042: Disable or Remove Feature or Program M1041: Encrypt Sensitive Information M1037: Filter Network Traffic M1035: Limit Access to Resource Over Network M1031: Network Intrusion Prevention M1030: Network Segmentation M1017: User Training
TA0040: Impact	T1498: Network Denial of Service	M1037: Filter Network Traffic

INFORMATION MANIPULATION AND INTERFERENCE

It is important to note that disinformation and misinformation attacks are among the preparatory activities at the basis of other attacks (e.g. phishing, social engineering, malware infection). The MITRE ATT&CK® graph below can give an idea of the link between disinformation/misinformation and connected attacks.

Tactic	Technique	Mitigation
TA0043: Reconnaissance	T1592: Gather Victim Host Information T1589: Gather Victim Identity Information T1590: Gather Victim Network Information T1591: Gather Victim Org Information T1598: Phishing for Information T1597: Search Closed Sources T1596: Search Open Technical Databases T1593: Search Open Websites/Domains T1594: Search Victim-Owned Websites	M1056: Pre-compromise M1054: Software Configuration M1017: User Training M1013: Application Developer Guidance M1047: Audit
TA0042: Resource Development	T1586: Compromise Accounts T1585: Establish Accounts	M1056: Pre-compromise
TA0001: Initial Access	T1566: Phishing	M1049: Antivirus/Antimalware M1031: Network Intrusion Prevention M1021: Restrict Web-Based Content M1054: Software Configuration M1017: User Training
TA0002: Execution	T1203: Exploitation for Client Execution T1204: User Execution	M1048: Application Isolation and Sandboxing M1050: Exploit Protection M1040: Behaviour Prevention on Endpoint M1038: Execution Prevention M1031: Network Intrusion Prevention M1021: Restrict Web-Based Content M1017: User Training
TA0005: Defense Evasion	T1036: Masquerading	M1049: Antivirus/Antimalware M1040: Behaviour Prevention on Endpoint M1045: Code Signing

		M1038: Execution Prevention M1022: Restrict File and Directory Permissions
TA0040: Impact	T1565: Data Manipulation T1491: Defacement	M1041: Encrypt Sensitive Information M1030: Network Segmentation M1029: Remote Data Storage M1022: Restrict File and Directory Permissions M1053: Data Backup

SUPPLY CHAIN ATTACKS

The current table highlights the techniques in the MITRE ATT&CK® Framework associated with supply chain attacks. Note that this is a dynamic representation based on actual observations. These can change over time as groups evolve and use new techniques. Every threat actor uses its own specific tools and attack patterns. This overview groups all common techniques. In addition, we only list those techniques relevant for supply chain attacks, and do not include the techniques commonly used for follow-up activity.

In addition to the MITRE ATT&CK Framework, it is useful to note that MITRE revealed its 'System of Trust Framework' [950] in June 2022. This framework builds a basis for trust by identifying the three main trust aspects of supply chain security, suppliers, supplies and services, and then identifying and addressing 14 top-level risk areas that require evaluation. The framework offers a comprehensive, consistent and repeatable methodology for evaluating suppliers, supplies and service providers.

Tactic	Technique	Mitigation
TA0043: Reconnaissance	T1595: Active Scanning T1592: Gather Victim Host Information T1589: Gather Victim Identity Information T1590: Gather Victim Network Information T1591: Gather Victim Org Information T1598: Phishing for Information T1597: Search Closed Sources T1596: Search Open Technical Databases T1593: Search Open Websites/Domains T1594: Search Victim-Owned Websites	M1056: Pre-compromise M1054: Software Configuration M1017: User Training M1013: Application Developer Guidance M1047: Audit
TA0042: Resource Development	T1583: Acquire Infrastructure T1586: Compromise Accounts T1584: Compromise Infrastructure T1587: Develop Capabilities T1585: Establish Accounts T1588: Obtain Capabilities T1608: Stage Capabilities	M1056: Pre-compromise
TA0001: Initial Access	T1195: Supply Chain Compromise T1200: Hardware Additions T1199: Trusted Relationship	M1051: Update Software M1016: Vulnerability Scanning M1035: Limit Access to Resource Over Network M1034: Limit Hardware Installation M1030: Network Segmentation M1018: User Account Management M1032: Multi-factor Authentication

[950] MITRE SoT: https://sot.mitre.org/

B ANNEX: RECOMMENDATIONS

Our recommendations are mapped[951] to the security measures that are part of international standards i.e. ISO/IEC 27001:2013[952], NIST Cybersecurity Framework (CSF), used by operators in the business sectors, as documented[953] by ENISA.

RANSOMWARE 	
Implement a secure and redundant backup strategy. Ensure you maintain offline, encrypted data backups that are regularly tested, following your backup procedures.	
ISO/IEC 27001:2013 A.12.3 Backup A.17.1 Information security continuity A.18.1.3 Protection of records	**NIST Cybersecurity Framework (CSF)** PR. IP-4: Backups of information are conducted, maintained, and tested
Create, maintain, and exercise an incident response plan that is regularly tested. Document the communication flows, including response and notification procedures during an incident. The ransomware Response Checklist from CISA can help you prepare.	
ISO/IEC 27001:2013 A.16.1.1 Responsibilities and procedures A.16.1.5 Response to information security incidents A.17.1 Information security continuity	**NIST Cybersecurity Framework (CSF)** PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed PR.IP-10: Response and recovery plans are tested RS.RP-1: Response plan is executed during or after an incident Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
Ensure your internet-facing infrastructure is secure. Perform regular vulnerability scanning to identify and address vulnerabilities. Install (security) updates and patches regularly, per your patch policy.	
ISO/IEC 27001:2013 A.12.6.1 Management of technical vulnerabilities	**NIST Cybersecurity Framework (CSF)** PR.IP-12: A vulnerability management plan is developed and implemented DE.CM-8: Vulnerability scans are performed
Ensure remote access technology or other exposed services are configured security, and MFA and strong password policies are actively managed, audited, and enforced on the user accounts. Apply the principles of least privilege and separation of duties.	
ISO/IEC 27001:2013 A.6.1.2 Segregation of duties A.6.2.1 Mobile device policy A.6.2.2 Teleworking A.9.1 Business requirements of access control A.9.2 User access management A.9.3 User responsibilities	**NIST Cybersecurity Framework (CSF)** Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorised users, processes, and devices, and is managed consistent with the assessed risk of unauthorised access to authorised activities and transactions.

[951] Note that when a measure is applied to a given recommendation, we include all measures as documented by ENISA. For example, for the first recommendation, all measures for an 'Information system security incident response' were taken into consideration.
[952] https://www.iso.org/standard/27001
[953] Minimum Security Measures for Operators of Essentials Services https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services

A.9.4 System and application access control A.11.2.4 Equipment maintenance A.11.2.6 Security of Equipment and Assets Off-Premises A.13.1.1 Network Controls A.13.2.1 Information Transfer Policies & Procedures A.15.1.1 Information Security Policy for Supplier Relationships A.15.2.1 Monitoring and review of supplier services	PR.MA-2: Remote maintenance of organisational assets is approved, logged, and performed in a manner that prevents unauthorised access
Periodic security awareness and training are critical, as ransomware often relies on social engineering to lure users into clicking a link.	
ISO/IEC 27001:2013 A.7.2.2 Information Security Awareness, Education and Training A.12.2.1 Documented Operating Procedures	**NIST Cybersecurity Framework (CSF)** Awareness and Training (PR.AT): The organisation's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements.
Collaborate with peers and national CERTs. Use the tools available for sharing malware information and -mitigation (e.g., MISP).	
ISO/IEC 27001:2013 7.4 Communication A.6.1.3 Contact with authorities A.6.1.4 Contact with special interest groups A.16.1.2 Reporting Information Security Events	**NIST Cybersecurity Framework (CSF)** Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies). E.DP-4: Event detection information is communicated
Monitor and centralise logs using a security incident and event management (SIEM) solution. Develop relevant use-cases to improve the effectiveness of detections and reduce log alert fatigue and achievable continuous monitoring.	
ISO/IEC 27001:2013 A.12.2.1 Documented Operating Procedures A.12.4.1 Event Logging A.16.1.7 Collection of evidence	**NIST Cybersecurity Framework (CSF)** Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood. Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Ensure your assets are inventoried, managed, and under control.	
ISO/IEC 27001:2013 A.8.1.1 Inventory of assets A.8.1.2 Ownership of Assets A.11.2.6 Security of Equipment and Assets Off-Premises, A.13.2.1 Information Transfer Policies & Procedures A.13.2.2 Agreements on information transfer	**NIST Cybersecurity Framework (CSF)** Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organisation to achieve business purposes are identified and managed consistent with their relative importance to organisational objectives and the organisation's risk strategy.
Deploy EDR/XDR and ensure the signatures are up to date. **Use application directory allow-listing, blocking any unauthorized software execution.** **Monitor process execution to detect anomalies** **Employ e-mail filtering for malicious e-mails and remove executable attachments.**	
ISO/IEC 27001:2013 A.12.4.1 Event Logging A.14.2.7 Outsourced Development A.15.2.1 Monitoring and review of supplier services	**NIST Cybersecurity Framework (CSF)** Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood. Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

MALWARE

Create, maintain, and exercise an incident response plan that is regularly tested. Document the communication flows, including response and notification procedures during an incident.

ISO/IEC 27001:2013	NIST Cybersecurity Framework (CSF)
A.16.1.1 Responsibilities and procedures A.16.1.5 Response to information security incidents A.17.1 Information security continuity	ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed PR.IP-10: Response and recovery plans are tested RS.RP-1: Response plan is executed during or after an incident Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).

Ensure your internet-facing infrastructure is secure.

Perform regular vulnerability scanning to identify and address vulnerabilities. Install (security) updates and patches regularly, per your patch policy.

ISO/IEC 27001:2013	NIST Cybersecurity Framework (CSF)
A.12.6.1 Management of technical vulnerabilities	DE.CM-8: Vulnerability scans are performed PR.IP-12: A vulnerability management plan is developed and implemented RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks ID.RA-1: Asset vulnerabilities are identified and documented

Ensure remote access technology or other exposed services are configured security, and MFA and strong password policies are actively managed, audited, and enforced on the user accounts.

Apply the principles of least privilege and separation of duties.

ISO/IEC 27001:2013	NIST Cybersecurity Framework (CSF)
A.6.1.2 Segregation of Duties A.6.2.1 Mobile device policy A.6.2.2 Teleworking A.9.1 Business requirements of access control A.9.2 User access management A.9.3 User responsibilities A.9.4 System and application access control A.11.2.4 Equipment maintenance A.11.2.6 Security of Equipment and Assets Off-Premises, A.13.1.1 Network Controls, A.13.2.1 Information Transfer Policies & Procedures A.15.1.1, Information Security Policy for Supplier Relationships A.15.2.1 Monitoring and review of supplier services	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorised users, processes, and devices, and is managed consistent with the assessed risk of unauthorised access to authorised activities and transactions. PR.MA-2: Remote maintenance of organisational assets is approved, logged, and performed in a manner that prevents unauthorised access

Periodic security awareness and training are critical, as ransomware often relies on social engineering to lure users into clicking a link.

ISO/IEC 27001:2013	NIST Cybersecurity Framework (CSF)

A.7.2.2 Information Security Awareness, Education and Training, A.12.2.1 Documented Operating Procedures	Awareness and Training (PR.AT): The organisation's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity related duties and responsibilities consistent with related policies, procedures, and agreements.
Collaborate with peers and national CERTs. Use the tools available for sharing malware information and -mitigation (e.g., MISP).	
ISO/IEC 27001:2013 7.4 Communication A.6.1.3 Contact with authorities A.6.1.4 Contact with special interest groups A.16.1.2 Reporting Information Security Events	**NIST Cybersecurity Framework (CSF)** Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies). DE.DP-4: Event detection information is communicated
Monitor and centralise logs using a security incident and event management (SIEM) solution. Develop relevant use-cases to improve the effectiveness of detections and reduce log alert fatigue and achievable continuous monitoring.	
ISO/IEC 27001:2013 A.12.2.1 Documented Operating Procedures A.12.4.1 Event Logging A.16.1.7 Collection of evidence	**NIST Cybersecurity Framework (CSF)** Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood. Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.
Ensure your assets are inventoried, managed, and under control.	
ISO/IEC 27001:2013 A.8.1.1 Inventory of assets A.8.1.2 Ownership of Assets A.11.2.6 Security of Equipment and Assets Off-Premises, A.13.2.1 Information Transfer Policies & Procedures A.13.2.2 Agreements on information transfer	**NIST Cybersecurity Framework (CSF)** Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organisation to achieve business purposes are identified and managed consistent with their relative importance to organisational objectives and the organisation's risk strategy.
Deploy EDR/XDR and ensure the signatures are up to date. **Use application directory allow-listing, blocking any unauthorised software execution.** **Monitor process execution to detect anomalies.** **Employ E-mail filtering for malicious e-mails and remove executable attachments.** **Implement malware detection for all inbound/outbound channels, including e-mail, network, web, and application systems on all applicable platforms (i.e., servers, network infrastructure, personal computers, and mobile devices).** **Inspect the SSL/TLS traffic allowing the firewall to decrypt what is being transmitted to and from websites, e-mail communications, and mobile applications.**	
ISO/IEC 27001:2013 A.12.4.1 Event Logging A.14.2.7 Outsourced Development A.15.2.1 Monitoring and review of supplier services	**NIST Cybersecurity Framework (CSF)** Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood. Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures.

SOCIAL ENGINEERING

Review and update the incident response plans to adapt to the latest trends identified for social engineering attacks.

ISO/IEC 27001:2013	NIST Cybersecurity Framework (CSF)
A16.1 Management of information security incidents & improvements	Risk Assessment (ID.RA) PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed RS.AN-2: The impact of the incident is understood RS.AN-5: Processes are established to receive, analyse and respond to vulnerabilities disclosed to the organisation from internal and external sources (e.g. internal testing, security bulletins, or security researchers) RC.RP-1: Recovery plan is executed during or after a cybersecurity incident

Maintain an overview of the digital footprint of your organisation and update this information on a frequent basis. Ideally this updating is done automatically and changes in the digital footprint trigger an alert for follow-up investigations.

Appoint a role within your organisation to do regular OSINT research on your organisation (taking on the role of an "outsider").

Preventively register domains that resemble your organisation's name, including alternative TLDs. Regularly review the organisations 'domain settings to support anti-spoofing and authentication mechanisms to filter e-mail.

ISO/IEC 27001:2013	NIST Cybersecurity Framework (CSF)
4.1 Understanding the organisation and its context 4.2 Understanding the needs and expectations of interested parties 4.3 Determining the scope of the information security management system 8.1 Operational planning and control 9.3 Management review A.8.1.1 Inventory of assets A.12.6.1 Management of technical vulnerabilities A.18.2.1 Independent review of information security	ID.GV-4: Governance and risk management processes address cybersecurity risks ID.RA (see above) Risk Management Strategy (ID.RM Asset Management (ID.AM) ID.BE-4: Dependencies and critical functions for delivery of critical services are established PR.IP-12: A vulnerability management plan is developed and implemented RS.AN-5: Processes are established to receive, analyse and respond to vulnerabilities disclosed to the organisation from internal and external sources (e.g. internal testing, security bulletins, or security researchers)

Adjust the awareness trainings to take into account the new social engineering trends. Consider tailored trainings that focus on the HR, sales and finance departments. Also consider specific trainings for IT and security staff.

ISO/IEC 27001:2013	NIST Cybersecurity Framework (CSF)
5.3 Organisational roles, responsibilities, and authorities 6.2 Information security objectives and planning to achieve them 7 Support 9.1 Monitoring, measurement, analysis and evaluation A.6.1.1 Information security roles and responsibilities A.6.1.2 Segregation of duties A.7 Human resource security A.9.3 User responsibilities	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) Awareness and Training (PR.AT) DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability RS.CO-1: Personnel know their roles and order of operations when a response is needed

Ensure that the infrastructure of your organisation where social engineering attacks can be detected is "forensic ready", meaning the relevant logs are collected with sufficient details to support incident response investigations. Logs should be complete, reliable, accurate and consistent.

Expand the monitoring use cases to go beyond your perimeter and to include domain and certificate monitoring that resemble the organisations 'assets. Additionally, include in these monitoring use cases detections for signs of data breaches relevant for your organisation. **Employ threat intelligence relevant to detect social engineering operations and automatically apply this information for network intrusion prevention, web access and e-mail filtering.** **Subscribe to a feed of issued certificates (certificate transparency feed) and alert on names resembling your organisation's name or assets. Monitor newly issued domains for names resembling your organisation's name or assets. Subscribe to alerts from data breach monitoring sites. Subscribe to alerts of the organisation assets being published on criminal forums. Consider the use of the AIL framework954.** **Deploy detection rules that alert on the presence (or opening) of disk image files on systems where these file types are not commonly present.**	
ISO/IEC 27001:2013 9.3 Management review A.12.4 Logging and monitoring A.12.6.1 Management of technical vulnerabilities A.14.1.2 Securing application services on public networks A.15.2.1 Monitoring and review of supplier services A.18.1.3 Protection of records	**NIST Cybersecurity Framework (CSF)** ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organisational stakeholders PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures. PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events. RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks RS.AN-1: Notifications from detection systems are investigated
Block the use of disk images exchanged via e-mail.	
ISO/IEC 27001:2013 8.1 Operational planning and control A.13.1 Network security management	**NIST Cybersecurity Framework (CSF)** PR.PT-4: Communications and control networks are protected PR.DS-2: Data-in-transit is protected
Enforce user-consent settings so users cannot consent to allow third-party application access. Only allow applications from verified publishers or for specific low-risk permissions. **Routinely review mail server configurations, employee mail settings and connection logs. Focus efforts on identifying employee mail-forwarding rules and identifying abnormal connections to mail servers.** **Utilise e-mail security features that notify a user when an e-mail is being sent from a user they have not interacted with before.**	
ISO/IEC 27001:2013 A.6.2.1 Mobile device policy A.8.3.1 Management of removable media A.12.5 Control of operational software A.12.6.2 Restrictions on software installation A.14.1 Security requirements of information systems A.14.2. Security in development and support processes	**NIST Cybersecurity Framework (CSF)** PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed
Review consented permissions for external applications on a regular basis.	
ISO/IEC 27001:2013	**NIST Cybersecurity Framework (CSF)**

954 AIL Framework https://github.com/CIRCL/AIL-framework

9.3 Management review A.5.1.2 Review of the policies for information security	ID.RM-1: Risk management processes are established, managed, and agreed to by organisational stakeholders ID.GV-1: Organisational cybersecurity policy is established and communicated

THREATS AGAINST DATA

Build a team of specialists: Having a team of specialists with skill and knowledge to respond to data breaches is critically important to maintain data availability, confidentiality, and integrity.

Asset discovery, risk assessment, mitigation plan: A proper mitigation strategy starts from the knowledge of the assets that can be target of an attack, as well as a proper risk assessment are at the basis of a proper data security posture.

ISO/IEC 27001:2013	**NIST Cybersecurity Framework (CSF)**
5.3 Organisational roles, responsibilities and authorities 7.5.3 Control of documented information 8.1 Operational planning and control A.6.1.1 Information security roles and responsibilities A.16.1.5 Response to information security incidents A.16.1.6 Learning from information security incidents	ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organisational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident. RS.RP-1: Response plan is executed during or after an incident RC.RP-1: Recovery plan is executed during or after a cybersecurity incident ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)

Proper security budgeting and spending: Data breaches and leaks are increasing risks that are plaguing current enterprises and corresponding systems. Proper planning and budgeting for data management risks is key and requires alignment in understanding security impacts between management and practitioners.955

ISO/IEC 27001:2013	**NIST Cybersecurity Framework (CSF)**
A.11.2.4 Equipment maintenance A.12.1.2 Change management A.15.2.2 Managing changes to supplier services and control	Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organisation to achieve business purposes are identified and managed consistent with their relative importance to organisational objectives and the organisation's risk strategy. PR.MA-1: Maintenance and repair of organisational assets are performed and logged, with approved and controlled tools ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.

Support for compliance and certification:956

ISO/IEC 27001:2013	**NIST Cybersecurity Framework (CSF)**
A.5.1.1 Policies for information security A.12.7.1 Information systems audit controls	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organisation's regulatory, legal, risk,

955 2022 Thales Data Threat Report
956 https://artificialintelligenceact.eu/

A.18.1.1 Identification of applicable legislation and contractual requirements A.18.1.2 Intellectual property rights A.18.2.2 Compliance with security policies and standards	environmental, and operational requirements are understood and inform the management of cybersecurity risk. PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy DE.DP-2: Detection activities comply with all applicable requirements
Authorisation Management: Human errors and misconfigurations are at the basis of many data breaches. A proper authorisation management that reviews access privileges according to changing rights of the users, users leaving an organisation is key to reduce possible insider threat attacks. 957 **Zero trust architectures: Zero trust architectures can increase the security posture of a system by implementing "never trust, always verify" paradigm. 958 This paradigm could be particularly important when accessing sensitive information.** **Unique and strong passwords: A proper password management approach is important to reduce the risk of an attack to a system. 959 Unique passwords avoid multiple system compromise with a single password breach. Strong passwords can increase the robustness of the system against attacks. A password manager can simplify users' activities.** **Enforcing password hygiene: Having unique and strong passwords contributes to the protection of sensitive data. Unfortunately, the current norm tells of users adopting weak password that are easily guessable and can be broken with brute force attacks. Multi-factor authentication (T1) can be used to strengthen the authentication process using token or fingerprints. Enforcement of longer passwords or enterprise password management systems come with additional burden on users and organisations. 960** **User awareness training and education: Insufficient level of cybersecurity expertise and inadequate education of employees can lead to database breaches. Non-technical employees can put the entire system and its data at risk. Both IT security personnel and end users should be professionally trained and know the most recent cybersecurity trends. The first should increase their knowledge to implement security controls and professionally manage data; the latter should undergo basic training in database security. 961 The need of a security awareness programme stands out when social attacks are executed and result in malware installation and stolen credentials. 962**	
ISO/IEC 27001:2013 A.6.1.2 Segregation of duties A.7 Human resource security A.9.1 Business requirements of access control A.9.2 User access management A.9.3 User responsibilities A.9.4 System and application access control A.12.4.3 Administrator and operator logs	**NIST Cybersecurity Framework (CSF)** ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed RS.CO-1: Personnel know their roles and order of operations when a response is needed, PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)DE.DP-1 Awareness and Training (PR.AT): The organisation's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements. Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorised users, processes, and devices, and is managed consistent with the assessed risk of unauthorised access to authorised activities and transactions. PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
Data security auditing: The support of security auditing is key to identify organisational gaps and vulnerabilities, as well as data misuse. 963 Security audits can be performed either by security experts or by a third party (e.g. penetration testing model), evaluating the risk of data breaches. 964	
ISO/IEC 27001:2013 A.12.7.1 Information systems audit controls	**NIST Cybersecurity Framework (CSF)**

957 EU H2020 CONCORDIA, D4.3
958 https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf
959 https://blog.f-secure.com/data-breach-and-data-leak-whats-the-difference/
960 EU H2020 CONCORDIA, D4.3
961 EU H2020 CONCORDIA, D4.3
962 https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf
963 EU H2020 CONCORDIA, D4.3
964 EU H2020 CONCORDIA, D4.3

A.18.2 Information security reviews	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy ID.RA-1: Asset vulnerabilities are identified and documented PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality) DE.AE-3: Event data are collected and correlated from multiple sources and sensors
Data sanitisation: Data sanitisation enables end-users to protect their data by decreasing the quality of data according to different techniques including anonymisation, generalisation, encryption, masking, filtering. Manipulated data can then be used for testing, training, processing. 965 966 **Countermeasures against data poisoning: Countermeasures against data poisoning are important to increase the robustness of the model by using datasets of higher quality. The dataset is evaluated to filter out poisoned data points, including poisoned data points removal,967 replacement and healing.968 Countermeasures should also aim to increase the strength of the model itself, for instance, by using an ensemble of models to reduce the impact of a poisoning attack. 969 970** **Adversarial training: Adversarial training is important to protect a ML model against inference-time attacks. It builds on training set augmentation (adversarial training),971 where adversarial data points are added to the training set to increase the resilience of the model against malicious data points.**	
ISO/IEC 27001:2013 A.6.2.1 Mobile device policy A.8.3.1 Management of removable media A.10.1 Cryptographic controls A.12.1 Operational procedures and responsibilities A.12.5 Control of operational software A.12.6.2 Restrictions on software installation A.13.1.2 Security of network services A.14.1 Security requirements of information systems A.14.2.1 Secure development policy A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development environment A.18.1.5 Regulation of cryptographic controls	**NIST Cybersecurity Framework (CSF)** PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality) PR.IP-3: Configuration change control processes are in place DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed PR.DS-1: Data-at-rest is protected PR.DS-2: Data-in-transit is protected PR.DS-5: Protections against data leaks are implemented PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity PR.PT-4: Communications and control networks are protected
Data Loss Prevention solutions: Inspecting and controlling file management and transfer is key to avoid sensitive and personal data or intellectual property does not exit the corporate network or to a user without access.	
ISO/IEC 27001:2013 A.13.2.2 Agreements on information transfer	**NIST Cybersecurity Framework (CSF)** ID.AM-3: Organisational communication and data flows are mapped

965 EU H2020 CONCORDIA, D4.3
966 Marco Anisetti, Claudio A. Ardagna, Chiara Braghin, Ernesto Damiani, Antongiacomo Polimeno, and Alessandro Balestrucci. 2021. Dynamic and Scalable Enforcement of Access Control Policies for Big Data. Proceedings of the 13th International Conference on Management of Digital EcoSystems.
967 N. Peri, N. Gupta, W. R. Huang, L. Fowl, C. Zhu, S. Feizi, T. Goldstein, and J. P. Dickerson, 'Deep k-NN Defence Against Clean-Label Data Poisoning Attacks,' in Proc. of ECCV 2020, August 2020.
968 E. Rosenfeld, E. Winston, P. Ravikumar, and Z. Kolter, 'Certified Robustness to Label-Flipping Attacks via Randomised Smoothing,' in Proc. of ICML 2020, Virtual, June 2020.
969 J. Jia, X. Cao, and N. Z. Gong, 'Intrinsic Certified Robustness of Bagging against Data Poisoning Attacks,' in Proc. of AAAI 2021, Virtual, February 2021.
970 W. Wang, A. Levine, and S. Feizi, 'Improved Certified Defences against Data Poisoning with (Deterministic) Finite Aggregation,' arXiv preprint arXiv:2202.02628, 2022.
971 A. Kurakin, D. Boneh, F. Tramèr, I. Goodfellow, N. Papernot, and P. McDaniel, 'Ensemble Adversarial Training: Attacks and Defences,' in Proc. of ICLR 2018, Vancouver, BC, Canada, April, May 2018.

Data backups: Data backups are fundamental to support prompt recovery from attacks. 972 Backup sites must be geographically distributed and separated to avoid being tampered by the same attack. Geographical redundancy can also help in preventing damages originating from natural disasters and sudden power outages.	
ISO/IEC 27001:2013 A.17.2 Redundancies	**NIST Cybersecurity Framework (CSF)** PR.DS-4: Adequate capacity to ensure availability is maintained PR.DS-5: Protections against data leaks are implemented

THREATS AGAINST AVAILABILITY

Build a team of specialists: having a team of specialists with the skills and knowledge to respond to DDoS attacks is critically important to maintain system availability and operation.	
ISO/IEC 27001:2013 5.3 Organisational roles, responsibilities and authorities 7.5.3 Control of documented information 8.1 Operational planning and control 10.1 Nonconformity and corrective action A.6.1.1 Information security roles and responsibilities A.11.2.4 Equipment maintenance A.12.1.2 Change management A.12.6.1 Management of technical vulnerabilities A.14.1.1 Information security requirements analysis and specification A 14.2 Security in development and support processes A.15.2.2 Managing changes to supplier services A.16.1.1 Responsibilities and procedures A.16.1.4 Assessment of and decisions on information security events A.16.1.5 Response to information security incidents A.16.1.6 Learning from information security incidents A.16.1.7 Collection of evidence A.17.1 Information security continuity	**NIST Cybersecurity Framework (CSF)** Risk Assessment (ID.RA): The organisation understands the cybersecurity risk to organisational operations (including mission, functions, image, or reputation), organisational assets, and individuals. PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition PR.DS-4: Adequate capacity to ensure availability is maintained Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organisational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities. Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident. Improvements (RS.IM): Organisational response activities are improved by incorporating lessons learned from current and previous detection/response activities. Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centres, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors). Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents. ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations)
Knowledge on third-party agreements: a response to a DDoS attack with third parties. Validating third-party agreements and contact information is key.	
ISO/IEC 27001:2013 6.2 Information security objectives and planning to achieve them 7.1 Resources 7.2 Competence 9 Performance evaluation 9.1 Monitoring, measurement, analysis and evaluation 9.3 Management review A.12.1.3 Capacity Management	**NIST Cybersecurity Framework (CSF)** ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritised based on their classification, criticality, and business value Risk Management Strategy (ID.RM): The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. PR.IP-7: Protection processes are improved PR.IP-8: Effectiveness of protection technologies is shared PR.DS-4: Adequate capacity to ensure availability is maintained

[972] EU H2020 CONCORDIA, D4.3

A.16.1.4 Assessment of and decisions on information security events A.16.1.7 Collection of evidence	ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations) ID.RA-4: Potential business impacts and likelihoods are identified ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood. Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events. RS.AN-1: Notifications from detection systems are investigated RS.AN-5: Processes are established to receive, analyse and respond to vulnerabilities disclosed to the organisation from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
Service restore: a plan B should exist in order to quickly restore business-critical services and reduce the mean time to recovery.	
ISO/IEC 27001:2013 9.3 Management review 10.2 Continual improvement A.5.1.2 Review of the policies for information security A.11.2.4 Equipment maintenance A.17.1 Information security continuity A.17.2 Redundancies	**NIST Cybersecurity Framework (CSF)** Risk Management Strategy (ID.RM): The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organisational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. RS.MI-2: Incidents are mitigated Improvements (RS.IM): Organisational response activities are improved by incorporating lessons learned from current and previous detection/response activities. Recovery Planning (RC.RP): Recovery processes and procedures are executed and maintained to ensure restoration of systems or assets affected by cybersecurity incidents. Communications (RC.CO): Restoration activities are coordinated with internal and external parties (e.g. coordinating centres, Internet Service Providers, owners of attacking systems, victims, other CSIRTs, and vendors). PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations PR.DS-4: Adequate capacity to ensure availability is maintained ID.BE-5: Resilience requirements to support delivery of critical services are established for all operating states (e.g. under duress/attack, during recovery, normal operations) ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers
Asset discovery, risk assessment and mitigation plan: a proper mitigation strategy starts from knowledge of the assets that can be the target of an attack as well as a proper assessment of risk[973]. All critical elements (e.g. servers, services and applications) should be protected and included in recurrent tests of a DDoS mitigation plan[974].	
ISO/IEC 27001:2013 6 Planning 7.5.3 Control of documented information 8 Operation 8.1 Operational planning and control 9.3 Management review 10 Improvement	**NIST Cybersecurity Framework (CSF)** ID.GV-4: Governance and risk management processes address cybersecurity risks Risk Assessment (ID.RA): The organisation understands the cybersecurity risk to organisational operations (including mission, functions, image, or reputation), organisational assets, and individuals.

[973] Neustar, Pay Or Else: DDoS Ransom Attacks
[974] https://www.netscout.com/blog/asert/ddos-attack-campaign-targeting-multiple-organizations-ukraine

10.1 Nonconformity and corrective action A.8.1.1 Inventory of assets A.12.6.1 Management of technical vulnerabilities A.11.2.4 Equipment maintenance A.12.1.2 Change management A.14.1.1 Information security requirements, analysis and specification A 14.2 Security in development and support processes A.15.2.2 Managing changes to supplier services A.18.2.1 Independent review of information security	Risk Management Strategy (ID.RM): The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. Improvements (RS.IM): Organisational response activities are improved by incorporating lessons learned from current and previous detection/response activities. Supply Chain Risk Management (ID.SC): The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organisation has established and implemented the processes to identify, assess and manage supply chain risks. Improvements (RS.IM): Organisational response activities are improved by incorporating lessons learned from current and previous detection/response activities. Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organisation to achieve business purposes are identified and managed consistent with their relative importance to organisational objectives and the organisation's risk strategy. DE.CM-8: Vulnerability scans are performed RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks RS.AN-5: Processes are established to receive, analyse and respond to vulnerabilities disclosed to the organisation from internal and external sources (e.g. internal testing, security bulletins, or security researchers) Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures. Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organisational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition PR.DS-4: Adequate capacity to ensure availability is maintained
Guarantee Best Current Practices (BCPs): organisations at risks should support relevant network infrastructure, architectural and operational best current practices (BCPs), for instance, proper network access policies and traffic filtering[975]. **Update and patch your system: the basic rules of updating and patching all systems should become a mantra, especially in scenarios involving IoT and smart devices[976]. For instance, Mozi botnet continues to rely on the same set of older vulnerabilities, even those that are eight years old[977].**	
ISO/IEC 27001:2013	**NIST Cybersecurity Framework (CSF)**
4.3 Determining the scope of the information security management system 8.1 Operational planning and control A.6.2.1 Mobile device policy A.8.3.1 Management of removable media A.12.1 Operational procedures and responsibilities A.12.5 Control of operational software A.12.6.2 Restrictions on software installation A.13.1 Network security management A.13.1.2 Security of network services A.13.2.1 Information transfer policies and procedures A.13.2.2 Agreements on information transfer A.14.1 Security requirements of information systems A.14.2.1 Secure development policy	PR.IP-1: A baseline configuration of information technology/industrial control systems is created and maintained incorporating security principles (e.g. concept of least functionality) PR.IP-2: A System Development Life Cycle to manage systems is implemented PR.IP-3: Configuration change control processes are in place DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities PR.PT-4: Communications and control networks are protected PR.AC-3: Remote access is managed PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation) PR.DS-2: Data-in-transit is protected

[975] https://www.netscout.com/blog/asert/ddos-attack-campaign-targeting-multiple-organizations-ukraine
[976] https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-ddos-attack-trends
[977] eset_threat_report_t22021

A.14.2.2 System change control procedures A.14.2.3 Technical review of applications after operating platform changes A.14.2.4 Restrictions on changes to software packages A.14.2.5 Secure system engineering principles A.14.2.6 Secure development environment	DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events DE.CM-7: Monitoring for unauthorised personnel, connections, devices, and software is performed
Deploy sufficient resources to increase the cost of an attack: DDoS attacks can be counteracted by deploying as much resources as possible or moving the target system to a powerful infrastructure (e.g. cloud infrastructure)[978]. For instance, the higher the bandwidth of a system or service, the more difficult or expensive a successful attack will be for a cybercriminal[979].	
ISO/IEC 27001:2013 7.5.3 Control of documented information 8.1 Operational planning and control 10.1 Nonconformity and corrective action A.11.2.4 Equipment maintenance A.12.1.2 Change management A.12.6.1 Management of technical vulnerabilities A.14.1.1 Information security requirements analysis and specification A 14.2 Security in development and support processes A.15.2.2 Managing changes to supplier services	**NIST Cybersecurity Framework (CSF)** Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures. Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organisational entities), processes, and procedures are maintained and used to manage protection of information systems and assets. PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition PR.DS-4: Adequate capacity to ensure availability is maintained ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations.
Model traffic trends and profiles: knowledge of the traffic trends and tendencies in the network is paramount to creating a baseline to simplify the detection of anomalies in the network activities that can be an indicator of a DDoS attack. Network and application monitoring tools can be used for this, further restricting the volume of incoming traffic[980] [981].	
ISO/IEC 27001:2013 9.1 Monitoring, measurement, analysis and evaluation A.12.2 Protection from malware A.12.4 Logging and monitoring A.12.6.1 Management of technical vulnerabilities A.14.1.2 Securing application services on public networks A.15.2.1 Monitoring and review of supplier services A.18.1.3 Protection of records	**NIST Cybersecurity Framework (CSF)** PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood. Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events. PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy ID.RA-1: Asset vulnerabilities are identified and documented ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organisational stakeholders Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures. RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks

[978] Neustar, Pay Or Else: DDoS Ransom Attacks
[979] https://hacked.com/will-2022-be-the-year-of-the-ddos-attack/
[980] David Warburton, F5Labs, DDoS Attack Trends for 2020, May 2021, https://www.f5.com/labs/articles/threat-intelligence/ddos-attack-trends-for-2020
[981] Neustar Security, Cyber Threats & Trends: Securing Your Network Pandemic-Style, 2020
https://www.cdn.neustar/resources/whitepapers/security/neustar-cyber-threats-trends-2020-report.pdf

Cybersecurity training and education: DDoS attacks are often built on a strong set of activities in preparation that range from botnet building to attack coordination and orchestration[982]. The remediations for these threats depend on correct and complete training and education in cybersecurity[983].	
ISO/IEC 27001:2013 4.1 Understanding the organisation and its context 4.2 Understanding the needs and expectations of interested parties 5.3 Organisational roles, responsibilities, and authorities 6.2 Information security objectives and planning to achieve them 7 Support 9.1 Monitoring, measurement, analysis and evaluation A.6.1.1 Information security roles and responsibilities A.6.1.2 Segregation of duties A.7 Human resource security A.9.3 User responsibilities	**NIST Cybersecurity Framework (CSF)** ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed RS.CO-1: Personnel know their roles and order of operations when a response is needed PR.IP-7: Protection processes are improved PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening) DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability Awareness and Training (PR.AT): The organisation's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

INFORMATION MANIPULATION AND INTERFERENCE

Information manipulation and interference is a complex issue, where cybersecurity is only one of multiple components. Indeed, one problem in addressing information manipulation and interference is "linkage blindness" that occurs when different organisations and governments look at different facets of the same issue, but no one is positioned to take responsibility for adopting a comprehensive approach (see section 2.1.6). A whole-of-society approach, which is an inclusive approach ensuring participation of parties with diverse backgrounds and perspectives can help against linkage blindness.

A number of recommendations are reported below[984]

Strategic level

- **Foster mutual exchanges between the cybersecurity and the community of defenders against information manipulation**. Concepts of cybersecurity can be applied to the detection and analysis of FIMI/disinformation incidents and operations. Existing frameworks, taxonomies, tools, structures and interoperable standards from cybersecurity can be adapted and adopted by the counter FIMI/disinformation community to speed up analytical maturity and interoperability within and beyond the field. For example, the EEAS is supporting the creation of an open source, decentralised and interoperable framework that increases the efficiency of sharing threat insights between the different stakeholders involved in FIMI analysis and disruption[985].
- **Improve the availability and quality of data on information manipulation**. Aggregable, structured, machine-readable and representative data on information manipulation is so far mostly unavailable. While individual data and research exist and stakeholders do share highly relevant insights, the sector is still underdeveloped compared to the diversity, specialisation and quantity of information shared in the cybersecurity sector. In this sense, the

[982] D4.2 concordia
[983] H-ISAC. Distributed Denial of Service (DDoS) Attacks, March 2021 https://www.aha.org/system/files/media/file/2021/03/distributed-denial-of-service-ddos-attacks-march-2021.pdf
[984] These recommendations stem from the 2022 ENISA-EEAS joint report 'Foreign Information Manipulation and Interference (FIMI) and Cybersecurity – Threat Landscape'
[985] https://www.eeas.europa.eu/sites/default/files/documents/2023/EEAS-DataTeam-ThreatReport-2023..pdf

adoption of standard formats to share information, such as such as STIX[986], the Standard Threat Information Expression language, could be a crucial step to move beyond information sharing by written reports.

Policy level

- **Facilitating, including with financial support, institutional/organisational cooperation and capacity building, especially to prevent and handle crisis and surrounding important events such as the upcoming 2024 European Elections.**

Operational level

- **Reporting on information manipulation should consider cybersecurity aspects more systematically and should be supported by structured and seamless incident reporting among different actors.** One of the most relevant limitations in the analysis of information manipulation events has been the quality of the data. Open-source data about information manipulation events might not contain sufficient information about its cybersecurity aspects. For example, in many cases the description of the cyber-component was not sufficiently detailed to identify the cybersecurity techniques utilised. This is particularly relevant also because the role of cybersecurity seems to be particularly important in establishing attribution.
- **Given the role of cyber-attacks at initial stages of an information manipulation campaign, awareness raising is important to limit the development or acquisition of content and the compromise of infrastructure that facilitate dissemination.** In particular, since the more high-level the account compromised is, the more legitimacy it has, it is important that high-profile members of governmental/public and media/audio-visual sectors are aware of this. This aspect might be especially relevant in the context of elections and should therefore be considered to help boost the EU's resilience in view of the 2024 European Parliament election
- **It is important for organisations to strengthen practices for critical information gathering, triaging, and distribution processes also considering the need to verify the authenticity of the information in order to mitigate the impact of polluted data and mischaracterised information**[987]**.** For the time being, guidance on this aspect, as well as how to seamlessly integrate reporting of manipulated information in "traditional" cybersecurity processes, is limited and constitutes an area for further investigation.
- **Social network detection and mitigation are still among the most important technical. Countermeasures can include: suspension of fake accounts (e.g. accounts that post duplicate or redundant information), mechanisms to filter and flag fake news, reductions of automatic activities (e.g. Bots), artificial Intelligence tools and platforms to detect fake news based on online approaches, mobile applications and chatbots powered by factcheckers targeting the general public, web-browser extensions for the general public. In addition, privacy tools that are natively supported by (social) platforms can help to mute, block, and report other users**[988]**.**

SUPPLY CHAIN ATTACKS

Establish a formal C-SCRM (Cyber Supply Chain Risk Management) programme and setup a dedicated third-party risk management office.

ISO/IEC 27001:2013	NIST Cybersecurity Framework (CSF)
4.2 Understanding the needs and expectations of interested parties 5.2 Policy 7.4 Communication 7.5 Documented information 8.1 Operational planning and control 9.3 Management review A.5.1.1 Policies for information Security A.7.1.2 Terms and conditions of employment A.7.2 During employment A.7.3 Termination and change of employment	ID.RM-1: Risk management processes are established, managed, and agreed to by organisational stakeholders ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners Supply Chain Risk Management (ID.SC): The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organisation has established and implemented the processes to identify, assess and manage supply chain risks. Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).

[986] See https://stixproject.github.io/
[987] https://www.ofcom.org.uk/news-centre/2022/one-in-three-internet-users-fail-to-question-misinformation
[988] https://www.apa.org/monitor/2022/06/news-misinformation-attack

A.12.7 Information systems audit considerations A.13.2 Information transfer A.14.2.7 Outsourced development A.15 Supplier relationships A.18.1.1 Identification of applicable legislation and contractual requirements	
Include key suppliers in business continuity and incident response plans and exercises. **Get insight into the functioning and services of the PSIRTs of key vendors, possibly with the help of the FIRST PSIRT Services Framework. It is strongly recommended that vendors start a PSIRT (according to the FIRST PSIRT Services Framework[989]) and coordinate security communications with customers via this PSIRT.**	
ISO/IEC 27001:2013 A.16.1.1 Responsibilities and procedures A.16.1.4 Assessment of and decisions on information security events A.16.1.5 Response to information security incidents A.16.1.6 Learning from information security incidents A.16.1.7 Collection of evidence	**NIST Cybersecurity Framework (CSF)** Risk Assessment (ID.RA): The organisation understands the cybersecurity risk to organisational operations (including mission, functions, image, or reputation), organisational assets, and individuals. ID.SC-5: Response and recovery planning and testing are conducted with suppliers and third-party providers PR.IP-9: Response plans (Incident Response and Business Continuity) and recovery plans (Incident Recovery and Disaster Recovery) are in place and managed PR.IP-10: Response and recovery plans are tested Analysis (RS.AN): Analysis is conducted to ensure effective response and support recovery activities. Mitigation (RS.MI): Activities are performed to prevent expansion of an event, mitigate its effects, and resolve the incident. Improvements (RS.IM): Organisational response activities are improved by incorporating lessons learned from current and previous detection/response activities. Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies). RS.RP-1: Response plan is executed during or after an incident
In awareness campaigns include a warning that users should not re-use passwords at vendors.	
ISO/IEC 27001:2013 A.9.1 Business requirements of access control A.9.3 User responsibilities A.9.4.1 Information access restriction A.9.4.2 Secure log-on procedures A.9.4.3 Password management system	**NIST Cybersecurity Framework (CSF)** Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorised users, processes, and devices, and is managed consistent with the assessed risk of unauthorised access to authorised activities and transactions. PR.DS-5: Protections against data leaks are implemented
Develop your defences based on the principle that your systems will be breached. Start small and log and track asset activity on and between internal networks (user, system and services logs, network data such as DNS queries and NetFlow, etc.).	
ISO/IEC 27001:2013 9.1 Monitoring, measurement, analysis and evaluation 9.3 Management review A.12.4 Logging and monitoring A.12.6.1 Management of technical vulnerabilities A.14.1.2 Securing application services on public networks A.15.2.1 Monitoring and review of supplier services A.16.1.4 Assessment of and decisions on information security events A.16.1.7 Collection of evidence A.18.1.3 Protection of records	**NIST Cybersecurity Framework (CSF)** ID.RA-1: Asset vulnerabilities are identified and documented ID.RA-4: Potential business impacts and likelihoods are identified ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organisational stakeholders PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity

[989] FIRST PSIRT Services Framework https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.1

	Maintenance (PR.MA): Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures. PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy PR.IP-7: Protection processes are improved Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. Anomalies and Events (DE.AE): Anomalous activity is detected and the potential impact of events is understood. Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events. RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks RS.AN-1: Notifications from detection systems are investigated RS.AN-5: Processes are established to receive, analyse and respond to vulnerabilities disclosed to the organisation from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
There should be no gap between physical security and cybersecurity. Ensure that physical access to devices is restricted and authenticated.	
ISO/IEC 27001:2013 A.8.1 Responsibility for assets A.11 Physical and environmental security	**NIST Cybersecurity Framework (CSF)** ID.AM-1: Physical devices and systems within the organisation are inventoried ID.AM-4: External information systems are catalogued PR.IP-5: Policy and regulations regarding the physical operating environment for organisational assets are met PR.IP-6: Data is destroyed according to policy PR.AC-2: Physical access to assets is managed and protected PR.AC-3: Remote access is managed PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition PR.PT-2: Removable media is protected and its use restricted according to policy PR.PT-5: Mechanisms (e.g., failsafe, load balancing, hot swap) are implemented to achieve resilience requirements in normal and adverse situations DE.CM-2: The physical environment is monitored to detect potential cybersecurity events DE.CM-3: Personnel activity is monitored to detect potential cybersecurity events DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events
Establish protocols for vulnerability disclosure and incident notification and establish protocols for communications with external stakeholders during incidents. Apply the FIRST990 guidelines and practices for multi-party vulnerability coordination and disclosure. **Use third-party assessments, site visits and formal certification to assess critical suppliers. Look beyond the software (or hardware) product and examine a suppliers' approach towards cybersecurity. Do not rely solely on vendor supplied documentation or information. Trust, but verify.** **Create an inventory of all the hardware, software and service providers on which you rely and trust. Make sure this inventory is checked automatically. Connections from unknown devices or software or abnormal traffic patterns from service providers should trigger an alert for follow-up investigations.** **A patch management process should be implemented to check unused dependencies, unmaintained and/or previously vulnerable dependencies, unnecessary features, components, files and documentation. Ensure all software is up-to-date.**	
ISO/IEC 27001:2013	**NIST Cybersecurity Framework (CSF)**

[990] FIRST SIG: https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.1

6 Planning 8 Operation 9.3 Management review 10 Improvement A.8.1.1 Inventory of assets A.12.6.1 Management of technical vulnerabilities A.18.2.1 Independent review of information security	ID.GV-4: Governance and risk management processes address cybersecurity risks Risk Assessment (ID.RA): The organisation understands the cybersecurity risk to organisational operations (including mission, functions, image, or reputation), organisational assets, and individuals. Risk Management Strategy (ID.RM): The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. Asset Management (ID.AM): The data, personnel, devices, systems, and facilities that enable the organisation to achieve business purposes are identified and managed consistent with their relative importance to organisational objectives and the organisation's risk strategy. ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organisational stakeholders ID.SC-2: Suppliers and third-party partners of information systems, components, and services are identified, prioritised, and assessed using a cyber supply chain risk assessment process Business Environment (ID.BE): The organisation's mission, objectives, stakeholders, and activities are understood and prioritised; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. PR.IP-12: A vulnerability management plan is developed and implemented DE.CM-8: Vulnerability scans are performed RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks RS.AN-5: Processes are established to receive, analyse and respond to vulnerabilities disclosed to the organisation from internal and external sources (e.g. internal testing, security bulletins, or security researchers) Improvements (RS.IM): Organisational response activities are improved by incorporating lessons learned from current and previous detection/response activities. Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
Document and align responsibilities in SaaS or PaaS managed cloud services. **Have a vulnerability management policy. Ensure vulnerabilities are identified and tracked.** **Apply 'one strike and you're out' policies with respect to vendor products that are either counterfeit or do not match specifications as contractually agreed and/or documented.** **Include security requirements in all RFPs and contracts.** **Ensure boot integrity and require firmware and driver security. Ensure that all firmware and drivers installed on servers or end-user equipment follow the necessary security requirements and have the documentation needed to prove their compliance.**	
ISO/IEC 27001:2013 4.3 Determining the scope of the information security management system 4.4 Information security management system 5.1 Leadership and commitment 5.2 Policy 5.3 Organisational roles, responsibilities and authorities 6.2 Information security objectives and planning to achieve them 9.3 Management review A.5.1.1 Policies for information security A.5.1.2 Review of the policies for information security A.6.1.1 Information security roles and responsibilities A.7.2.1 Management responsibilities A.18.1.1 Identification of applicable legislation and contractual requirements	**NIST Cybersecurity Framework (CSF)** Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organisation's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. Business Environment (ID.BE): The organisation's mission, objectives, stakeholders, and activities are understood and prioritised; this information is used to inform cybersecurity roles, responsibilities, and risk management decisions. ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established Awareness and Training (PR.AT): The organisation's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurity-related duties and responsibilities consistent with related policies, procedures, and agreements.

A.18.1.2 Intellectual property rights A.18.2.2 Compliance with security policies and standards	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability
Implement continuous monitoring of sources of vulnerabilities and the use of tools for automatic and manual reviews of code.	
ISO/IEC 27001:2013 9.1 Monitoring, measurement, analysis and evaluation A.12.2 Protection from malware A.12.4 Logging and monitoring A.12.6.1 Management of technical vulnerabilities A.15.2.1 Monitoring and review of supplier services	**NIST Cybersecurity Framework (CSF)** PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed DE.AE-5: Incident alert thresholds are established Security Continuous Monitoring (DE.CM): The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures. Detection Processes (DE.DP): Detection processes and procedures are maintained and tested to ensure awareness of anomalous events.
Setup tight controls on access by service vendors. Enforce the use of encrypted communications and multi-factor authentication.	
ISO/IEC 27001:2013 A.9.2 User access management A.9.4.4 Use of privileged utility programs A.9.4.5 Access control to program source code	**NIST Cybersecurity Framework (CSF)** ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritised based on their classification, criticality, and business value ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorised users, processes, and devices, and is managed consistent with the assessed risk of unauthorised access to authorised activities and transactions. PR.DS-5: Protections against data leaks are implemented PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities
Setup communication channels with the various PSIRTs of your vendors.	
ISO/IEC 27001:2013 7.4 Communication 7.5 Documented information A.6.1.3 Contact with authorities A.6.1.4 Contact with special interest groups A.8.2.2 Labelling of information	**NIST Cybersecurity Framework (CSF)** DE.DP-4: Event detection information is communicated Communications (RS.CO): Response activities are coordinated with internal and external stakeholders (e.g. external support from law enforcement agencies).
Enable MFA for access to developer accounts[991].	
ISO/IEC 27001:2013 A.9.1 Business requirements of access control A.9.3 User responsibilities A.9.4.1 Information access restriction A.9.4.2 Secure log-on procedures A.9.4.3 Password management system	**NIST Cybersecurity Framework (CSF)** Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorised users, processes, and devices, and is managed consistent with the assessed risk of unauthorised access to authorised activities and transactions. PR.DS-5: Protections against data leaks are implemented
Apply code hashing authentication. **Scan and audit containers before putting them into production.**	

[991] https://github.blog/2022-03-28-how-to-secure-your-end-to-end-supply-chain-on-github/

ISO/IEC 27001:2013	NIST Cybersecurity Framework (CSF)
6 Planning 8 Operation 9.2 Internal audit 9.3 Management review 10 Improvement A.5.1.2 Review of the policies for information security A.12.7.1 Information systems audit controls A.18.2 Information security reviews	Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organisation's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. Risk Assessment (ID.RA): The organisation understands the cybersecurity risk to organisational operations (including mission, functions, image, or reputation), organisational assets, and individuals. Risk Management Strategy (ID.RM): The organisation's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. ID.SC-4: Suppliers and third-party partners are routinely assessed using audits, test results, or other forms of evaluations to confirm they are meeting their contractual obligations. PR.AC-1: Identities and credentials are issued, managed, verified, revoked, and audited for authorised devices, users and processes PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy PR.IP-7: Protection processes are improved PR.IP-12: A vulnerability management plan is developed and implemented DE.CM-8: Vulnerability scans are performed DE.DP-5: Detection processes are continuously improved Improvements (RS.IM): Organisational response activities are improved by incorporating lessons learned from current and previous detection/response activities. Improvements (RC.IM): Recovery planning and processes are improved by incorporating lessons learned into future activities.
Isolate legacy systems and development ('non-production') systems in separate network segments.	
ISO/IEC 27001:2013	**NIST Cybersecurity Framework (CSF)**
A.12.1.4 Separation of development, testing and operational environments A.13.1 Network security management	PR.DS-5: Protections against data leaks are implemented PR.DS-7: The development and testing environment(s) are separate from the production environment PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities PR.PT-4: Communications and control networks are protected PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation) PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions
Use container image signing.	
ISO/IEC 27001:2013	**NIST Cybersecurity Framework (CSF)**
A.10.1 Cryptographic controls A.18.1.5 Regulation of cryptographic controls	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed Data Security (PR.DS): Information and records (data) are managed consistent with the organisation's risk strategy to protect the confidentiality, integrity, and availability of information. PR.PT-4: Communications and control networks are protected

978-92-9204-588-3

ABOUT ENISA

The European Union Agency for Cybersecurity, ENISA, is the Union's agency dedicated to achieving a high common level of cybersecurity across Europe. Established in 2004 and strengthened by the EU Cybersecurity Act, the European Union Agency for Cybersecurity contributes to EU cyber policy, enhances the trustworthiness of ICT products, services and processes with cybersecurity certification schemes, cooperates with Member States and EU bodies, and helps Europe prepare for the cyber challenges of tomorrow. Through knowledge sharing, capacity building and awareness raising, the Agency works together with its key stakeholders to strengthen trust in the connected economy, to boost resilience of the Union's infrastructure and, ultimately, to keep Europe's society and citizens digitally secure. More information about ENISA and its work can be found here: www.enisa.europa.eu.

ENISA
European Union Agency for Cybersecurity

Athens Office
1 Vasilissis Sof as Str
151 24 Marousi, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN 978-92-9204-588-3
DOI: 10.2824/782573