EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA THREAT LANDSCAPE 2022

(July 2021 to July 2022)

OCTOBER 2022

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, Rossen Svetozarov Naydenov, Cosmin Ciobanu, Apostolos Malatras, Marianthi Theocharidou – European Union Agency for Cybersecurity

CONTRIBUTORS

Claudio Ardagna, Stephen Corbiaux, Koen Van Impe, Andreas Sfakianakis

ACKNOWLEDGEMENTS

We would like to thank the Members and Observers of the ENISA ad hoc Working Group on Cyber Threat Landscapes (https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-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.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN: 978-92-9204-588-3, DOI: 10.2824/764318

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This is the tenth edition of the ENISA Threat Landscape (ETL) report, an annual report on the status of the cybersecurity threat landscape. It identifies the top threats, major trends observed with respect to threats, threat actors and attack techniques, as well as impact and motivation analysis. It also describes relevant mitigation measures. This year's work has again been supported by ENISA's ad hoc Working Group on Cybersecurity Threat Landscapes (CTL).

During the reporting period of the ETL 2022, the prime threats identified include:

1. **Ransomware**
2. **Malware**
3. **Social Engineering threats**
4. **Threats against data**
5. **Threats against availability: Denial of Service**
6. **Threats against availability: Internet threats**
7. **Disinformation – misinformation**
8. **Supply-chain attacks**

For each of the identified threats, attack techniques, notable incidents and trends are proposed alongside with mitigation measures. When it comes to trends during the reporting period, we must emphasise the following.

- **Impact of geopolitics on the cybersecurity threat landscape**
  - The **conflict between Russia-Ukraine reshaped the threat landscape** during the reporting period. Some of the interesting changes were significant increases in hacktivist activity, cyber actors conducting operations in concert with kinetic military action, the mobilisation of hacktivists, cybercrime, and aid by nation-state groups during this conflict.
  - **Geopolitics continue to have stronger impact on cyber operations.**
  - **Destructive attacks are a prominent component of the operations of state actors.** During the Russia-Ukraine conflict, cyber actors were observed conducting operations in concert with kinetic military action[1].
  - **A new wave of hacktivism[2] has been observed** especially since the Russia-Ukraine crisis began.
  - **Disinformation is a tool in cyberwarfare.** It was used even before the 'physical' war started as a preparatory activity for Russia's invasion of Ukraine.
- **Threat actors increasing their capabilities**
  - **Resourceful threat actors have utilised 0-day exploits** to achieve their operational and strategic goals. The more organisations increase the maturity of their defences and cybersecurity programmes, the more they increase the cost for adversaries, driving them to develop and/or buy 0-day exploits, since defence in depth strategies reduce the availability of exploitable vulnerabilities.
  - **Continuous 'retirements' and the rebranding of ransomware groups** is being used to avoid law enforcement and sanctions.
  - **Hacker-as-a-service business model** gaining traction, growing since 2021.
  - **Threat groups have an increased interest and exhibit an increasing capability in supply chain attacks and attacks against Managed Services Providers (MSPs).**

[1] Microsoft – Special Report: Ukraine – An overview of Russia's cyberattack activity in Ukraine - https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
[2] Republic of Estonia – Information System Authority - Trends and Challenges in Cyber Security – Q1 2022 - https://www.ria.ee/en/news/trends-and-challenges-cyber-security-q1-2022.html

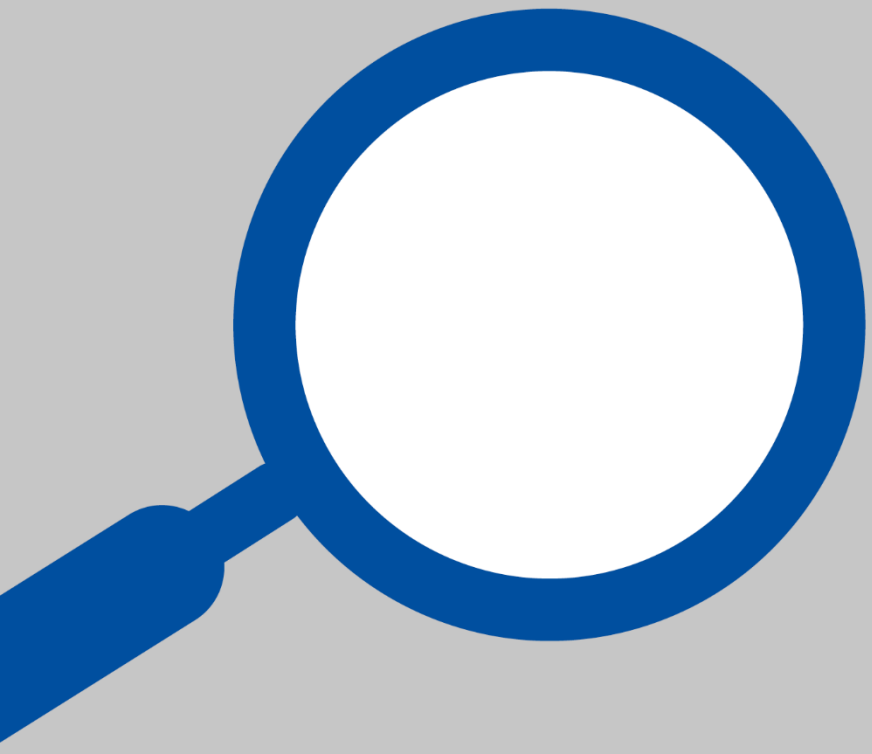
- **Ransomware and attacks against availability rank the highest during the reporting period**
    - **Significant rise on attacks against availability, particularly DDoS**, with the ongoing war being the main reason behind such attacks.
    - **Phishing is once again the most common vector** for initial access. Advances in sophistication of phishing, user fatigue and targeted, context-based phishing have led to this rise. New lures in social engineering threats are focusing on the Ukraine-Russia conflict in a similar manner to what happened during the COVID situation
    - **Malware is on the rise again** after the decrease that was noticed and linked to the COVID-19 pandemic[3].
    - **Extortion techniques are further evolving** with the popular use of leak sites.
    - **DDoS are getting larger and more complex, are moving towards mobile networks and IoT and are being used in the context of cyberwarfare.**
- **Novel, hybrid and emerging threats are marking the threat landscape with high impact**
    - **The Pegasus case triggered media coverage and governmental actions,** which also then was reflected in other cases concerning **surveillance and the targeting of civil society.**
    - **Consent phishing** attackers use consent phishing to send users links that, if clicked, will grant the attacker access and permissions to applications and services.
    - **Data compromise is increasing year on year.** The central role of data in our society produced a sharp increase in the amount of data collected and in the importance of proper data analysis. The price we pay for such importance is a continuous and unstoppable increase in data compromises.
    - **Machine Learning (ML) models** are at the core of modern distributed systems and are increasingly **becoming the target of attacks**.
    - **AI-enabled disinformation and deepfakes.** The proliferation of bots modelling personas can easily disrupt the 'notice-and-comment' rulemaking process, as well as the interaction of the community, by flooding government agencies with fake comments.

Moreover, understanding the trends related to threat actors, their motivations and their targets greatly assists in planning cybersecurity defences and mitigation strategies. Therefore, for the purposes of the ETL 2022, the following four categories of cybersecurity threat actors are considered again:

- **State-sponsored actors**
- **Cybercrime actors**
- **Hacker-for-hire actors**
- **Hacktivists.**

Through continuous analysis, ENISA derived trends, patterns and insights for each of the major threats presented in the ETL 2022. 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.

[3] ENISA Threat Landscape 2021



1. THREAT LANDSCAPE OVERVIEW

In its tenth edition, the ENISA Threat Landscape (ETL) report provides a general overview of the cybersecurity threat landscape. Over the years, the ETL has been used as key instrument in understanding the current status of cybersecurity across the EU and provide insight in terms of trends and patterns, leading to relevant decisions, prioritisation of actions and recommendations. The ETL report is partly strategic and partly technical, with information relevant to both technical and non-technical readers. The ETL 2022 report has been validated and supported by the ENISA ad hoc Working Group on Cybersecurity Threat Landscapes (CTL)[4] and ENISA National Liaison Officers (NLO) Network.

Cybersecurity attacks continued to increase during the second half of 2021 and 2022, not only in terms of vectors and numbers but also in terms of their impact. The Russia-Ukraine crisis has defined a new era for cyberwarfare and hacktivism, its role, and its impact on conflicts. States and other cyber operations will very likely adapt to this new state of affairs and take advantage of the novelties and challenges brought about by this war[5]. However, this new paradigm brought by the war has implications for international norms in cyberspace and, more specifically, for state sponsorship of cyberattacks and against targeting critical civilian infrastructure[5]. Due to the volatile international situation, we expect to observe more cyber operations being driven by geopolitics in the near to mid-term future. The geopolitical situation might trigger cyber operations and potentially damaging cyberattacks[6]. Consequently, a destabilized situation and continued threshold exceedance in terms of malicious cyber activity may also lead to more resulting damage.

It is worth noting that in this iteration of the ETL, additional focus was concentrated on the different kinds of impact cyber threats have in various sectors, including the sectors listed in the Network and Information Security Directive (NISD) and its agreed revision NIS2. 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. The criticality of different sectors is also reflected in relevant policy initiatives, with the recently agreed NISD 2 significantly expanding the list of important sectors in the EU. ENISA is working in parallel on developing sectorial threat landscapes, diving deeper into the elements of each sector and providing targeted insight.

The ETL 2022, building on the foundational elements of the ETL 2021, is based on a variety of open-source information and sources of cyber threat intelligence. It identifies major threats, trends and findings, and provides relevant high-level strategies for mitigation. The ETL 2022 has been developed using the officially established ENISA's Cyber Security Threat Landscape Methodology that was published earlier this year[7]. The ENISA CTL Methodology aims to provide a baseline for the transparent and systematic delivery of horizontal, thematic and sectorial cybersecurity threat landscapes based on a systematic and transparent process for data collection and analysis.

In this edition of the ETL, a novel element includes the analysis of the vulnerability landscape in tandem with the cybersecurity threat landscape analysis. Moreover, for the first time an impact analysis of the threats across different sectors and dedicated analysis of threat actors' motivations give an additional glimpse into the threat landscape. As always, findings are based on analysis of events and incidents, cross-validated with relevant cyber threat intelligence sources.

1.1 PRIME THREATS

A series of cyber threats emerged and materialised in the course of 2021 and 2022. Based on the analysis presented in this report, the ENISA Threat Landscape 2022 identifies and focuses on the following eight prime threat groups

[4] https://www.enisa.europa.eu/topics/threat-risk-management/threats-and-trends/ad-hoc-working-group-cyber-threat-landscapes
[5] Council on Foreign Relations - Cyber Proxies in the Ukraine Conflict: Implications for International Norms - https://www.cfr.org/blog/cyber-proxies-ukraine-conflict-implications-international-norms
[6] QuoIntelligence - Ransomware is here to stay and other cybersecurity predictions for 2022 - https://quointelligence.eu/2022/01/ransomware-and-other-cybersecurity-predictions-for-2022/
[7] https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology

(See Figure 1). These eight threat groups are highlighted because of their prominence during the reporting period, their popularity and the impact that was due to the materialisation of these threats.

- **Ransomware**
  According to ENISA's Threat Landscape for Ransomware Attacks[8] 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 more, 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[9], 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. Traditionally, examples of malicious code types include viruses, worms, trojan horses or other code-based entities that infect a host. Spyware and some forms of adware are also examples of malicious code[10]. During this reporting period, we again observed a large number of incidents involving malware. The incidents analysed are mainly focused on EU countries.

- **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[11]. It uses various forms of manipulation to trick victims into making mistakes or handing over sensitive or secret information. In cybersecurity, social engineering lures users into opening documents, files or e-mails, visiting websites or granting unauthorised persons access to systems or services. And although these tricks can abuse technology they always rely on a human element to be successful. This threat canvas consists mainly of the following vectors: phishing, spear-phishing, whaling, smishing, vishing, business e-mail compromise (BEC), fraud, impersonation and counterfeit, which are analysed in the relevant chapter.

- **Threats against data**
  Threats against data form a collection of threats that target sources of data with the aim of gaining unauthorised access and disclosure, as well as manipulating data to interfere with the behaviour of systems. These threats are also the basis of many other threats, also discussed in this report. For instance, ransomware, RDoS (Ransomware Denial of Service), DDoS (Distributed Denial of Service) aim to deny access to data and possibly collect a payment to restore this access. Technically speaking, threats against data can be mainly classified as data breach and data leak. Data breach is an intentional attack brought by a cybercriminal with the goal of gaining unauthorised access and the release of sensitive, confidential or protected data. Data leak is an event that can cause the unintentional release of sensitive, confidential or protected data due to, for example, misconfigurations, vulnerabilities or human errors.

- **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 has a significant role in the cybersecurity threat landscape[12] [13]. 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[14]. During the reporting period, threats against availability and ransomware rank the highest among the prime threats, which signals a change from ETL 2021 where ransomware was clearly at the top.

- **Threats against availability: Internet threats**

[8] ENISA Threat Landscape for Ransomware Attacks https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks
[9] https://csrc.nist.gov/glossary/term/malware
[10] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
[11] https://www.imperva.com/learn/application-security/social-engineering-attack/
[12] Federal Office for Information Security (BSI), The State of IT Sec in Germany, September 2020
[13] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020
[14] CISA, Understanding Denial-of-Service Attacks, November 2019. https://www.uscert.gov/ncas/tips/ST04-015

Internet use and the free flow of information impacts the lives of everyone. For many people, access to the internet has become a basic necessity to work, study, and to exercise freedom of expression, political freedom, and to interact socially. This group covers the threats that have an impact on the availability of the internet, such as BGP (Border Gateway Protocol) highjacking. Denial of Service (DoS) is covered in a separate section due to its individual impact in the threat landscape.

- **Disinformation – misinformation**
  Disinformation and misinformation campaigns are still on the rise, spurred by the increased use of social media platforms and online media. Digital platforms are nowadays the norm for news and media. Social sites, news and media outlets, even search engines, are now sources of information for many people. Due to the nature of how these sites operate, which is by attracting people and generating traffic to their sites, the information that generates more viewers is usually the one promoted, sometimes without it being validated. The war between Russia and Ukraine has shown new ways to use this threat, targeting people's perception of the status of the war and the responsibilities of the parties involved. Various motives underlie the differences between wrong and purposely falsified information. This is where the definitions of misinformation[15] and disinformation[16] come into play.

- **Supply Chain Attacks**
  A supply chain attack targets the relationship between organisations and their suppliers[17]. For this ETL report we use the definition as stated in the ENISA Threat Landscape for Supply Chain[18] where 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 revelation of this kind of attack and showed the potential impact of supply chain attacks. It seems that threat actors are continuing[19] to feed on this source to conduct their operations and gain a foothold within organisations, in an attempt to benefit from the widespread impact and potential victim base of such attacks.

[15] Misinformation is an unintentional attack, where sharing of information is done inadvertently. The inaccuracy carried by the information is unintentional and could happen for example when a journalist reports wrong information in good faith or reports information by mistake. ENISA ETL 2020
[16] Disinformation is an intentional attack that consists of the creation or sharing of false or misleading information. ENISA ETL 2020
[17] https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
[18] ENISA Threat Landscape for Supply Chain Attacks https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
[19] Accenture Cyber Threat Intelligence Report https://www.accenture.com/ae-en/insights/security/cyber-threat-intelligence

Figure 1: ENISA Threat Landscape 2022 - Prime threats

It should be noted that the aforementioned threats involve categories and refer to collection of different 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 of this report, which elaborates on its particularities and provides more specific information, findings, trends, attack techniques and mitigation vectors.

1.1 KEY TRENDS

The list below summarises the main trends observed in the cyber threat landscape during the reporting period. These are also reviewed in detail throughout the various chapters that comprise the ENISA threat landscape of 2022.

- **Ransomware and threats against availability rank at the top during the reporting period.**
- **Resourceful threat actors have utilised 0-day exploits** to achieve their operational and strategic goals. The more organisations increase the maturity of their defences and cybersecurity programmes, the more they increase the cost for adversaries, driving them to develop and/or buy 0-day exploits, since defence in depth strategies reduce the availability of exploitable vulnerabilities.
- **Geopolitics continue to have strong impact on cyber operations.**
- **Destructive attacks are a prominent component of the operations of state actors.** During the Russia-Ukraine conflict, cyber actors were observed conducting operations in concert with kinetic military action[20].
- **Continuous 'retirements' and the rebranding of ransomware groups** is being used to avoid law enforcement and sanctions.
- **Hacker-as-a-service business model** gaining traction, growing since 2021.
- **Significant rise on attacks against availability, particularly DDoS**, with the ongoing war being the main reason behind such attacks.
- **The Pegasus case triggered media coverage and governmental actions,** which also then was reflected in other cases concerning **surveillance and the targeting of civil society.**
- **A new wave of hacktivism[21] has been observed** especially since the Russia-Ukraine crisis began.

[20] Microsoft – Special Report: Ukraine – An overview of Russia's cyberattack activity in Ukraine - https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
[21] Republic of Estonia – Information System Authority - Trends and Challenges in Cyber Security – Q1 2022 - https://www.ria.ee/en/news/trends-and-challenges-cyber-security-q1-2022.html
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

- **Phishing is once again the most common vector** for initial access. Advances in sophistication of phishing, user fatigue and targeted, context-based phishing have led to this rise.
- **Extortion techniques are further evolving** with the popular use of leak sites.
- **Malware is on the rise again** after the decrease that was noticed and linked to the COVID-19 pandemic[22].
- **Consent phishing** attackers use consent phishing to send users links that, if clicked, will grant the attacker access and permissions to applications and services.
- **Data compromise is increasing year on year.** The central role of data in our society produced a sharp increase in the amount of data collected and in the importance of proper data analysis. The price we pay for such importance is a continuous and unstoppable increase in data compromises.
- **Machine Learning (ML) models** are at the core of modern distributed systems and are increasingly **becoming the target of attacks**.
- **DDoS are getting larger and more complex, are moving towards mobile networks and IoT and are being used in the context of cyberwarfare.**
- **State-owned Certificate Authorities (CA)** makes it easy to perform HTTPS traffic interception and man-in-the-middle attacks on its citizens thus putting internet security and privacy at risk.
- **Disinformation is a tool in cyberwarfare.** It was used even before the 'physical' war started as a preparatory activity for Russia's invasion of Ukraine.
- **AI-enabled disinformation and deepfakes.** The proliferation of bots modelling personas can easily disrupt the 'notice-and-comment' rulemaking process, as well as the interaction of the community, by flooding government agencies with fake comments.
- **Threat groups have an increased interest and exhibit an increasing capability in supply chain attacks and attacks against Managed Services Providers (MSPs).**

1.2 EU PROXIMITY OF PRIME THREATS

An important aspect to consider in the context of the ENISA Threat Landscape involves the proximity of a cyber threat with respect to the European Union (EU). This is particularly important to assist analysts in assessing the significance of cyber threats, to correlate them with potential threat actors and vectors and even to guide the selection of appropriately targeted mitigation vectors. In line with the proposed classification for the EU Common Security and Defence Policy (CSDP)[23], we classify cyber threats into four categories as illustrated in Table 1.

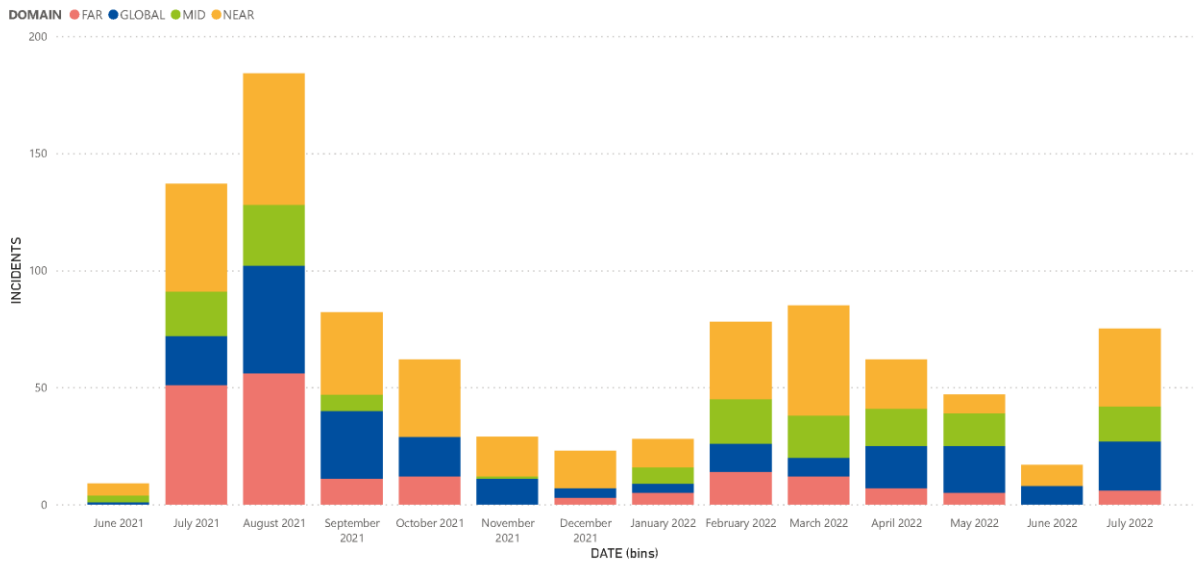
Table 1 Classification of proximity of cyber threats

Proximity	Concerns
NEAR	Affected networks, systems, controlled and assured within EU borders. Affected population within the borders of the EU.
MID	Networks and systems considered vital for operational objectives within the scope of the EU digital single market and the NISD sectors, but their control and assurance relies on non-EU institutional or public or private authorities in Member States (MSs). Affected population in geographical areas close to EU borders.
FAR	Networks and systems that, if influenced, will have a critical impact on operational objectives within the scope of the EU single digital market and the NISD sectors. Control and assurance of those networks and systems lie beyond EU institutional authorities or public or private authorities in MSs. Affected population is in geographical areas far from the EU.
GLOBAL	All the aforementioned areas

[22] ENISA Threat Landscape 2021
[23] https://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Figure 2 illustrates a time series of incidents related to the categories of prime threats reported in the ETL 2022. It should be noted that the information in the graph is based on OSINT (Open Source Intelligence) and is a result of work by ENISA in the area of Situational Awareness[24].

Figure 2: Observed incidents related to major ETL threats (OSINT-based situational awareness) in terms of their proximity **F**



As evidenced by the above figure, 2022 has seen a reduced number of incidents overall compared to 2021. This is partly due to the fact that incident handling and analysis is ongoing and reporting follows, as well as the open source nature of information collection in the ETL, which might inadvertently introduce bias in the results. In particular though, the category NEAR has a steady high number of observed incidents related to prime threats, which implies their significance in the context of the EU. This comes as no surprise considering the geopolitical situation in which the EU is involved. Unsurprisingly, the monthly trends (not shown in the figure for brevity) are quite similar among the different classifications since cybersecurity knows no border and in most cases threats materialise at all levels of proximity.

1.3 PRIME THREATS BY SECTOR

Cyber threats are usually not restricted to any particular sector and in most cases affect more than one. This is indeed true since in many cases the threats manifest themselves by exploiting vulnerabilities in underlying ICT systems that are being used in a variety of sectors. However, targeted attacks as well as attacks exploiting the differences in cybersecurity maturity across sectors and the popularity or prominence of certain sectors are all factors that need to be considered, particularly when it comes to prioritising targeted mitigating actions. These factors contribute to threats manifesting themselves as incidents in specific sectors and this is why it is important to look deeply into the sectorial aspects of observed incidents and threats.

Figure 3 and Figure 4 highlight the affected sectors concerning the incidents observed based on OSINT (Open Source Intelligence) and are a result of work by ENISA in the area of Situational Awareness[25]. They refer to incidents related to the prime threats of ETL 2022. The sectors have been aligned to the sectors listed in the Network and Information Security Directive[26] (NISD) and the agreed text[27] for its review (NISD 2.0).

[24] In accordance with the EU cybersecurity act Art.7, Para.6 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN
[25] In accordance with the EU cybersecurity act Art.7, Para.6 (https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN)
[26] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016L1148&from=EN
[27] https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985

Figure 3: Observed incidents related to prime ETL threats in terms of the affected sector

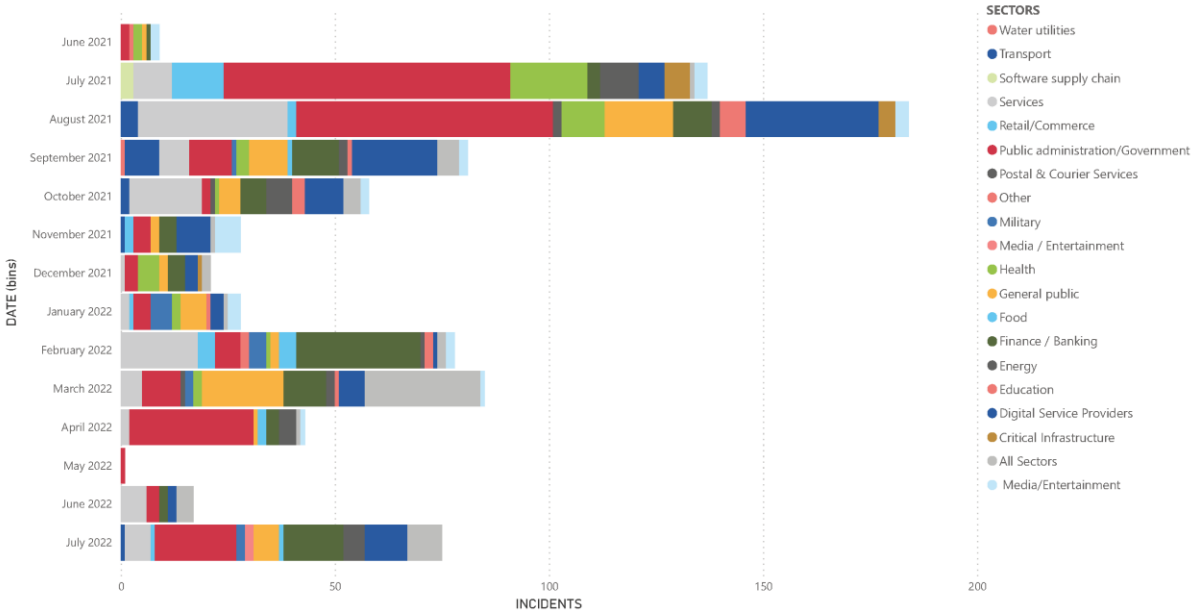
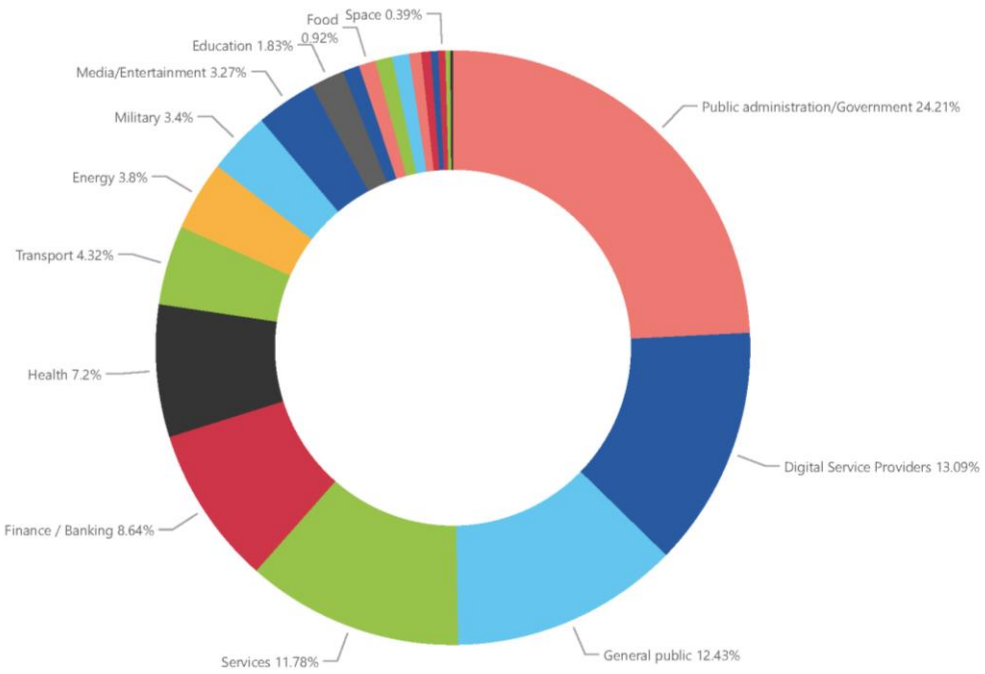


Figure 4: Targeted sectors per number of incidents (July 2021-June 2022)



During this reporting period, we again observed a large number of incidents targeting public administration and government and digital service providers. The latter is to be expected given the horizontal provisioning of services for this sector and thus its impact on many other sectors. We also observed a significant number of incidents targeting end users and not necessarily a particular sector. Interestingly, the finance sector faced a consistent number of incidents throughout the reporting period with the health sector following it close behind.

1.4 IMPACT ASSESSMENT BY SECTOR

In this iteration of ENISA's threat landscape we have included an assessment of the impacts of the incidents that were observed during the reporting period. With this qualitative process of impact analysis ENISA seeks to identify the consequences of a disruptive cyber incident by defining five types of potential impact and assigning respective levels or degrees of impact i.e. high, medium, low or unknown. Due to the fact that information related to the impact of a cybersecurity attack is often not available or made public for obvious reasons, 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 NIS 2 Directive and an area where ENISA will continue its efforts in the coming years.

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

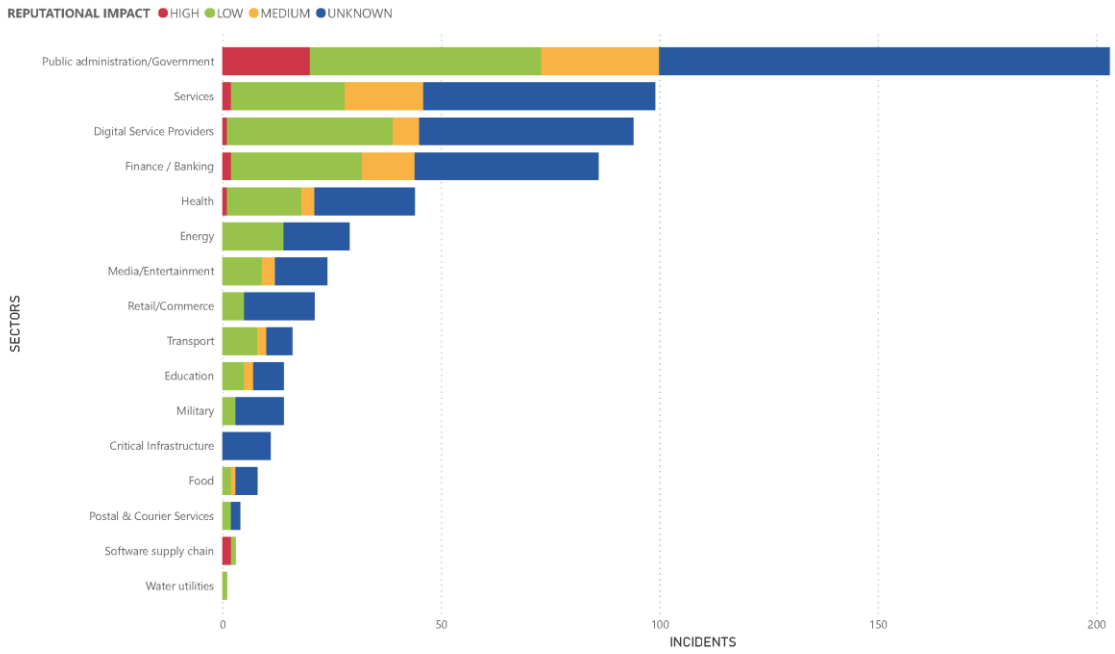
- **Reputational impact** refers to the potential for negative publicity or an adverse public perception of the entity that has been the victim of a cyber incident.
- **Digital impact** refers to damaged or unavailable systems, corrupted data files or exfiltration of data.
- **Economic impact** refers 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 requested.
- **Physical impact** refers to any kind of injury or harm to employees, customers or patients.
- **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).

The incidents collected were classified according to these five types of impact by applying internal ENISA experience and expertise. One of the highlights that emerged from the analysis is that in most of the incidents or cases the impact remained 'unknown' either because the victims were not clear about the level or type of impact that affected

their organisations or because they were not willing to disclose this kind of information due to a worry about the cascading impact that this could have to their reputation. This lack of reliable data from the targeted organisations makes it very hard to fully understand the situation. Once again, the significance of incident reporting and sharing of information concerning cybersecurity incidents emerges. The accurate understanding of the cybersecurity threat landscape and situational awareness in general, rely on timely and reliable incident reporting information.

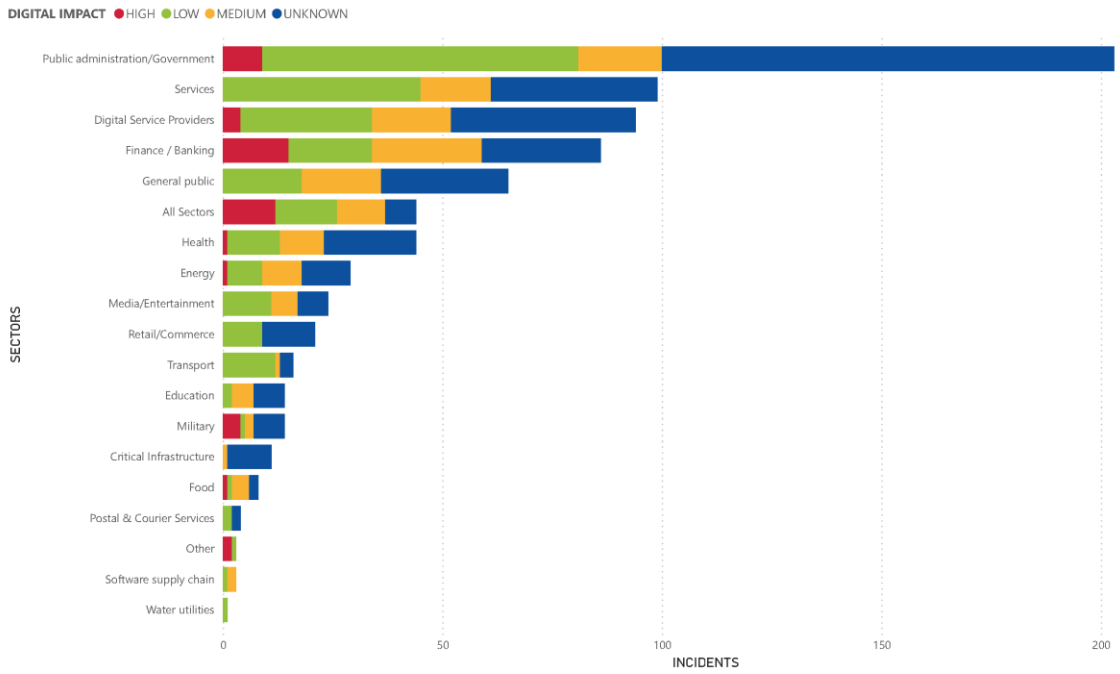
In Figure 5 it can be observed, according to the analysis, that the Public Administration sector was impacted the most when it was the target of a cyberattack. This is probably due to a loss of trust in the targeted entity. The second sector that was most hit by incidents with a high impact on its reputation was the Finance sector.

Figure 5 Reputational impact by sector



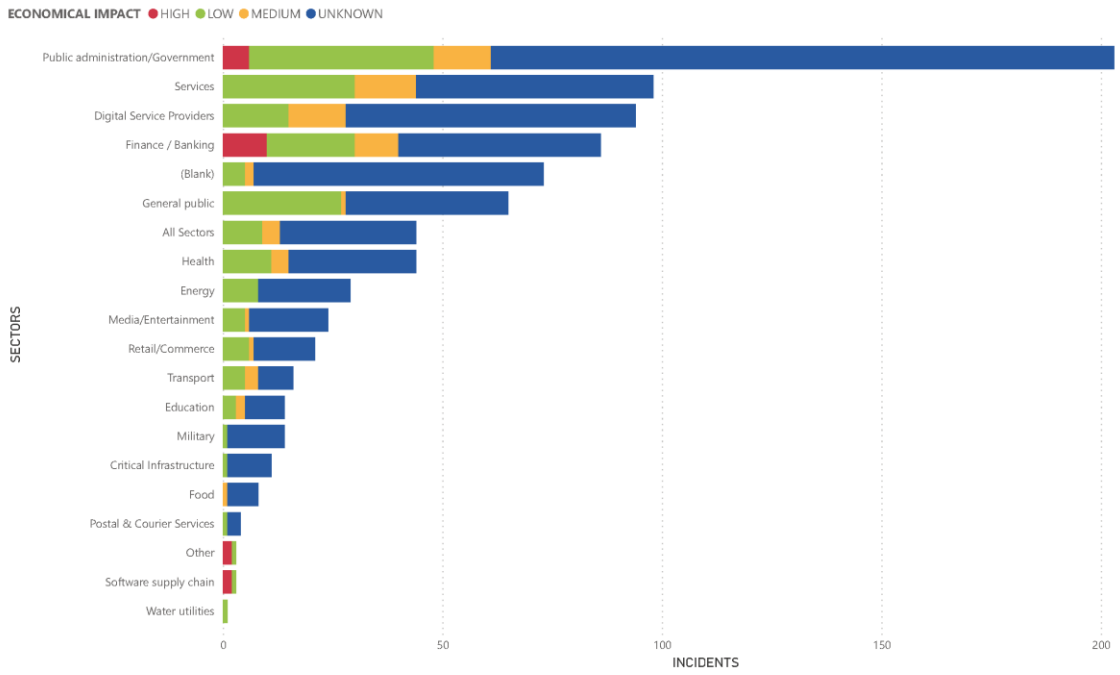
Digital impact (Figure 6) was in most sectors set to medium to low with the exception of the Public administration, Finance and Digital Service Providers which showed incidents with high impacts. The cause for this was usually a ransomware incident.

Figure 6 Digital impact by sector



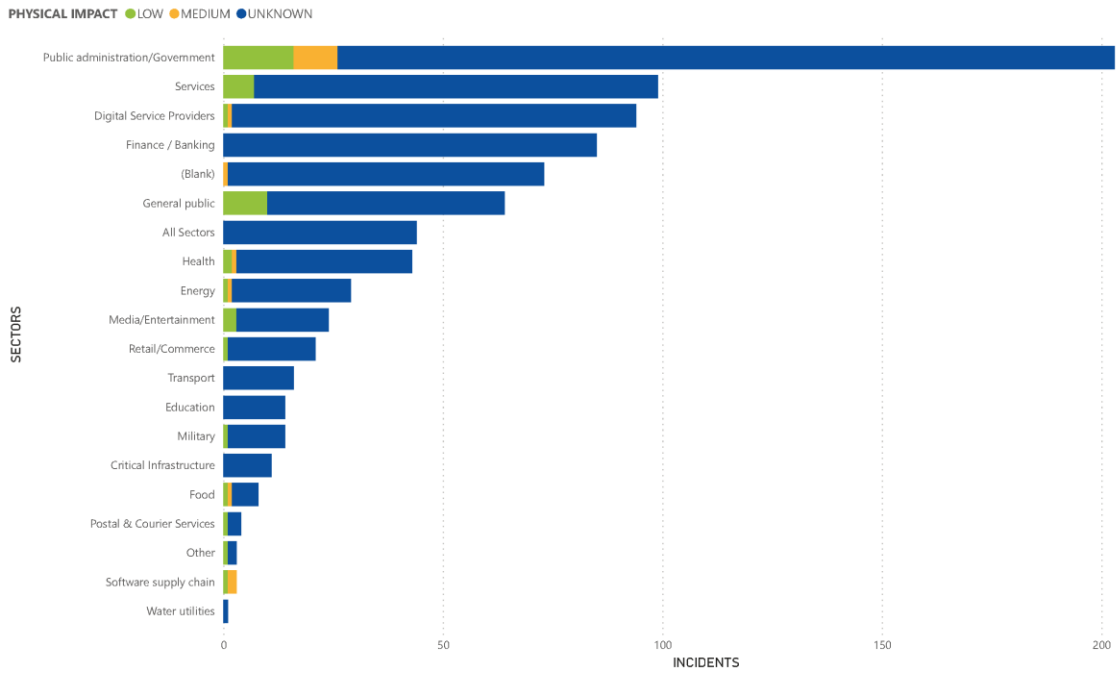
When talking about economic losses (Figure 7), it was observed that the Public Administration and Finance sectors had some of the highest impacts. This can be tied to many breaches related to stealing banking data or details and many breaches regarding personal data, in conjunction with the public sector also being the primary target of ransomware attacks this year.

Figure 7 Economic impact by sector



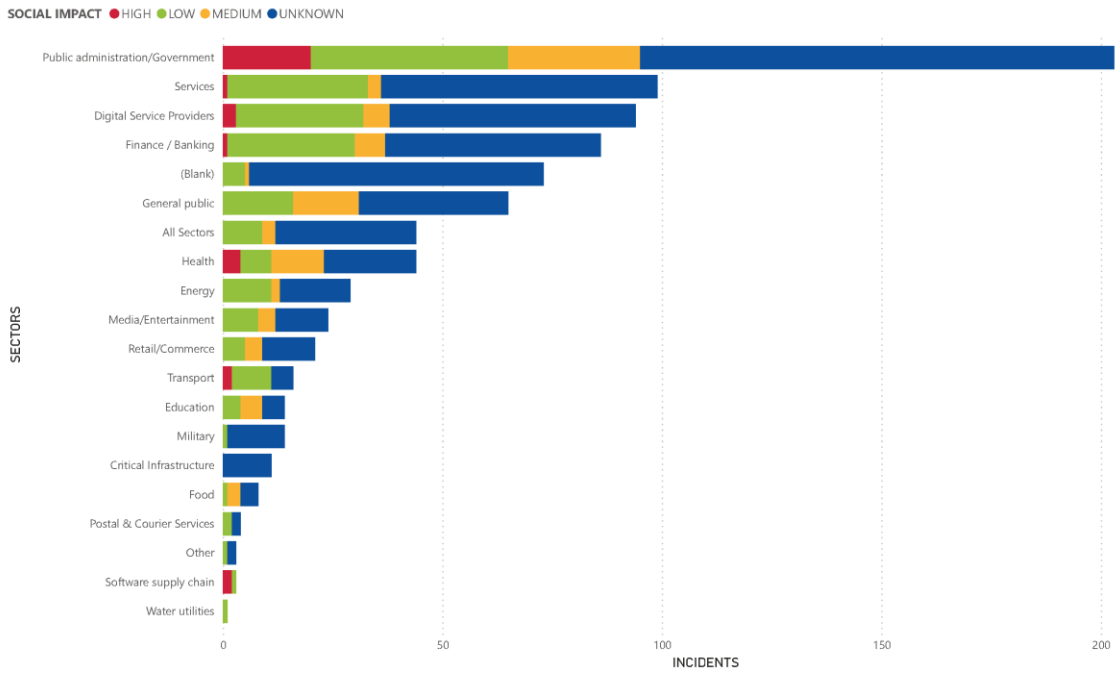
Physical impact (Figure 8) remains the most unknown impact due to the lack of published information or available reliable data.

Figure 8 Physical impact by sector



The Public Administration sector was the one with the highest number of incidents with regards to social impact, which in most cases concerned either the disruption of services or breaches of personal data. In addition, it was observed that the Health sector also had a large number of 'high' impact incidents, due to cases of either sensitive data being breached or Health services such as the appointment of bookings being unavailable.

Figure 9 Social Impact by sector



1.5 PRIME THREATS BY MOTIVATION

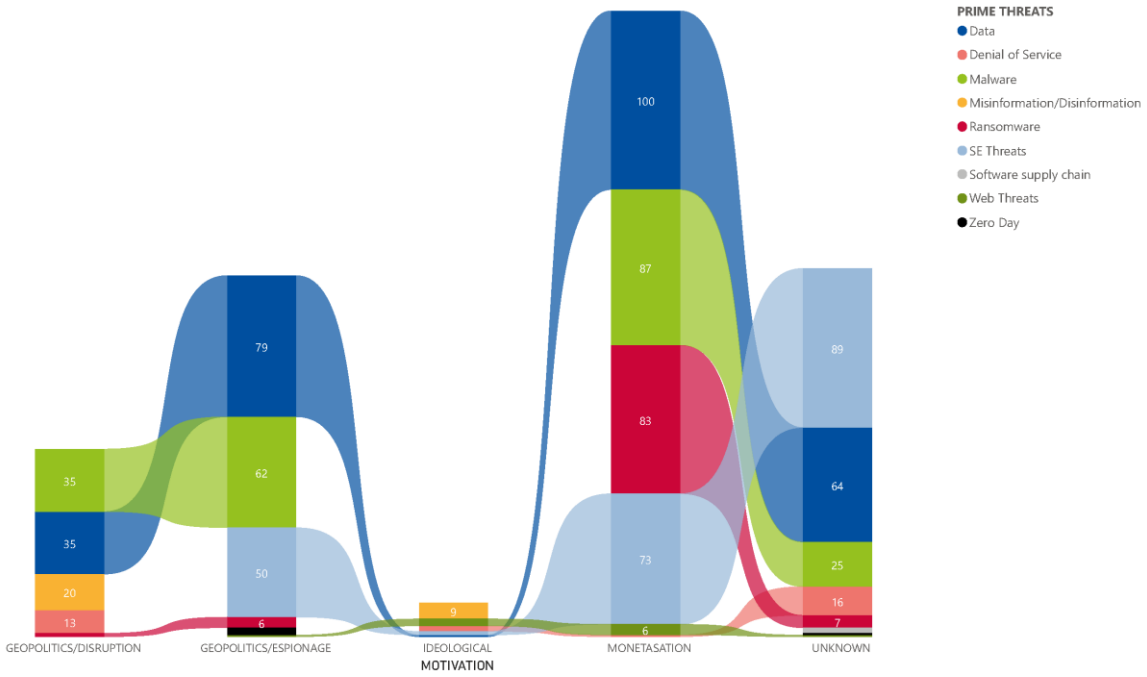
Understanding the enemy and the motivation behind a cybersecurity incident or targeted attack is important because it can determine what an adversary is after. Knowing the motives can help organisations determine and prioritise what to protect and how to protect it. It also provides an idea of the attackers'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

For all the above reasons, ETL 2022 has been expanded to include an assessment of the motivation behind the incidents observed during the reporting period. For this purpose, four different kinds of motivation have been defined that can be linked to threat actors:

- Monetisation: any financially related action (carried out by cybercrime groups);
- Geopolitics/Espionage: gaining information on IP (Intellectual Property), sensitive data, classified data (mostly executed by state sponsored groups);
- Geopolitics/Disruption: any disruptive action done in the name of geopolitics (mostly carried out by state sponsored groups);
- Ideological: any action backed up with an ideology behind it (such as hactivism).

We can observe that in most cases the prime threats fall under one or more motivations quite evenly. Ransomware though is done purely for financial gain.

Figure 10 Motivation of threat actors per threat category



1.6 METHODOLOGY

The ENISA Cybersecurity Threat Landscape (CTL) methodology[28] was used to produce the ETL 2022 report. The methodology was published in July 2022. By establishing the ENISA Cybersecurity Threat Landscape (CTL) methodology, the Agency sets a baseline for the transparent and systematic delivery of horizontal, thematic, and sectorial cybersecurity threat landscapes.

The ENISA Threat Landscape (ETL) 2022 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 2022 report is July 2021 to June 2022 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 report on the basis of a January to December year, contrary to the ETL 2022 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.

[28] ENISA Cybersecurity Threat Landscape (CTL) methodology, July 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

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**[29].

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[30] commonly used in the industry.

1.7 STRUCTURE OF THE REPORT

The ENISA Threat Landscape (ETL) 2022 has maintained the core structure of previous ETL reports for highlighting the prime cybersecurity threats in 2022. Readers of past iterations will notice that the threat categories have been consolidated in line with a move towards a new cybersecurity threat taxonomy to be used in the future.

This report is structured as follows.

Chapter 2 explores the trends related to threat actors (i.e. state-sponsored actors, cybercrime actors, hacker-for-hire actors and hacktivists).
Chapter 3 discusses major findings, incidents and trends regarding ransomware.
Chapter 4 presents major findings, incidents and trends regarding malware.
Chapter 5 describes major findings, incidents and trends regarding social engineering.
Chapter 6 highlights major findings, incidents and trends regarding threats against data (data breach, data leak).
Chapter 7 discusses major findings, incidents and trends regarding threats against availability (denial of service).
Chapter 8 presents major findings, incidents and trends regarding threats against availability (internet threats).
Chapter 9 underlines the importance of hybrid threats and describes major findings, incidents and trends regarding disinformation and misinformation.
Chapter 10 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 includes notable incidents per threat, as observed during the reporting period.
Annex C includes a CVE landscape, as observed during the reporting period.
Annex D presents recommendations and security controls that might add to the mitigation of the threats**.**

[29] MISP estimative language https://www.misp-project.org/taxonomies.html#_estimative_language
[30] 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. They are entities aiming to carry out a malicious act by taking advantage of existing vulnerabilities with the intent to harm their victims. Understanding how threat actors think and act and their motivations and goals are essential for a more robust cyber threat management and incident response. 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 threat assessment since it allows security controls to be prioritised and a dedicated strategy based on potential impact and the likelihood that threats will materialise. 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.

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 2022, we consider once more the following four categories of cybersecurity threat actors:

- **State-sponsored actors**
- **Cybercrime actors**
- **Hacker-for-hire actors**
- **Hacktivists.**

The list of potential threat actors is extensive and encompasses other categories, such as insider actors. The focus on the above four categories does not imply that other categories of threat actors are deemed of lesser significance. The focus on the four selected categories of threat actors is based on their relative prominence during the ETL 2022 reporting period.

2.1 STATE-SPONSORED ACTOR TRENDS

Increased exploitation of 0-day and other critical vulnerabilities. According to public reporting, exploitation of vulnerabilities was the most frequently identified vector[31] of intrusions while, during 2021, the number of disclosed 0-day exploits reached an all-time high of sixty six (66)[32].

[31] Mandiant – M-Trends 2022 - https://www.mandiant.com/resources/m-trends-2022
[32] Trend Micro Security Prediction for 2022 - https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2022
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

During the reporting period, state-sponsored actors exploited many critical vulnerabilities[31] in the wild, some of which were against Microsoft[33] [34] [35] [36], Pulse Secure VPN appliances[37], Atlassian Confluence[38], F5 Big-IP devices[39], Fortinet appliances[33] [44], and Apache's Log4j utility[40] [41] [42]. Moreover, we have observed state-sponsored threat actors targeting small office or home office routers worldwide and using this compromised infrastructure for their cyber operations while hindering defenders' efforts [43] [44]. We have also observed the replacement of Sandworm's VPNFilter malware with Cyclops Blink for targeting WatchGuard firewall devices and ASUS routers[45] [46].

Although the topic of 0-day vulnerabilities is not new, we would like to highlight the significant increase in 0-day disclosures during the reporting period. The factors that contributed to the increased number of disclosed 0-day vulnerabilities include the following. [47] [48] [51]

- The growing need for more software solutions provides a bigger surface and more opportunities for researching and exploiting vulnerabilities.
- It is likely that nation-state actors have to use 0-day exploits to accomplish their goals due to the maturing security posture of their targets and the security technologies they use.[51]
- Nation-state threat actors increasingly dedicate resources to 0-day research and the development of exploits. We have observed that sometimes these efforts can also lead to policy decisions, e.g. a new law in China requires vendors to report 0-day vulnerabilities to the government[49] [50].
- Another possibility is the increased focus on the supply chain by nation-state actors, which likely encourages research into the vulnerability of widely used software technologies. Thus, by exploiting one 0-day vulnerability, the threat actors can get initial access to multiple targets. Google, Microsoft, Apple, and Adobe products are indicatively some of the prime targets for such 0-day vulnerabilities[51].
- The Access-as-a-Service market has matured and been professionalised, offering services such as vulnerability research, exploitation, and malware payload development (among others)[52].
- Threat hunting and vulnerability research programmes are maturing and developing more capabilities to detect 0-day exploitation in the wild.
- Through security bulletins, more vendors have started to disclose the 0-day vulnerabilities of their software that were exploited in-the-wild. The same happens for security researchers that publicly disclosed 0-day vulnerabilities before the vendors' patches (especially if there was exploitation in-the-wild and no vendor patch).

[33] CISA - Iranian Government-Sponsored APT Cyber Actors Exploiting Microsoft Exchange and Fortinet Vulnerabilities in Furtherance of Malicious Activities - https://www.cisa.gov/uscert/ncas/alerts/aa21-321a
[34] CISA-FBI - Joint Advisory on Compromise of Microsoft Exchange Server - https://www.cisa.gov/uscert/ncas/current-activity/2021/03/10/fbi-cisa-joint-advisory-compromise-microsoft-exchange-server
[35] CISA - Russian State-Sponsored Cyber Actors Gain Network Access by Exploiting Default Multifactor Authentication Protocols and 'PrintNightmare' Vulnerability - https://www.cisa.gov/uscert/ncas/alerts/aa22-074a
[36] Security Affairs - Another nation-state actor exploits Microsoft Follina to attack European and US entities - https://securityaffairs.co/wordpress/131992/apt/nation-state-actors-follina-exploits.html
[37] CISA - Exploitation of Pulse Connect Secure Vulnerabilities - https://www.cisa.gov/uscert/ncas/alerts/aa21-110a
[38] The Record - Microsoft: Ransomware groups, nation-states exploiting Atlassian Confluence vulnerability - https://therecord.media/microsoft-ransomware-groups-nation-states-exploiting-atlassian-confluence-vulnerability/
[39] CISA - Threat Actors Exploiting F5 BIG-IP CVE-2022-1388 - https://www.cisa.gov/uscert/ncas/alerts/aa22-138a
[40] Bleeping Computer - Log4j vulnerability now used by state-backed hackers, access brokers - https://www.bleepingcomputer.com/news/security/log4j-vulnerability-now-used-by-state-backed-hackers-access-brokers/
[41] CERT-EU - Threat Landscape Report 2021 Q4 - Executive Summary - https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-2021Q4-Threat_Landscape_Report-Executive-Summary-v1.0.pdf
[42] CrowdStrike – 2022 Global Threat Report - https://www.crowdstrike.com/resources/reports/global-threat-report/
[43] Microsoft – Digital Defense Report - https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report
[44] CISA - People's Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices - https://www.cisa.gov/uscert/ncas/alerts/aa22-158a
[45] CISA - New Sandworm Malware Cyclops Blink Replaces VPNFilter - https://www.cisa.gov/uscert/ncas/alerts/aa22-054a
[46] US Department of Justice - Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU) - https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation
[47] PwC Cyber Threats 2021: A Year in Retrospect - https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect.html
[48] esentire - The State of Zero-Day Attacks in 2021 - https://www.esentire.com/resources/library/the-state-of-zero-day-attacks-in-2021
[49] The Hacker News - China's New Law Requires Vendors to Report Zero-Day Bugs to Government - https://thehackernews.com/2021/07/chinas-new-law-requires-researchers-to.html
[50] CERT-EU - Threat Landscape Report 2021 Q3 - Executive Summary - https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-2021Q3-Threat_Landscape_Report-Executive-Summary-v1.0.pdf
[51] Google TAG - How we protect users from 0-day attacks - https://blog.google/threat-analysis-group/how-we-protect-users-0-day-attacks/
[52] Atlantic Council - Countering cyber proliferation: Zeroing in on Access-as-a-Service - https://www.atlanticcouncil.org/in-depth-research-reports/report/countering-cyber-proliferation-zeroing-in-on-access-as-a-service/
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

- Vulnerability developers have more opportunities to get financial rewards for their 0-day exploitation work. One can make money from 0-day exploits usually by hacking contests, e.g. Tianfu Cup and Pwn2Own, or the underground marketplaces.

Heightened risk for Operational Technology networks. In ETL 2021, our assessment was that the interest of state actors in targeting critical infrastructure and Operational Technology (OT) networks would certainly grow in the near future. Throughout the reporting period, our assessment held valid as cyber operations targeting such infrastructure primarily for the collection of intelligence, deployment of newly observed ICS-targeting malware, and disruption were all observed.

According to public reports, three new activity groups (out of 18 in total) have been identified as showing intent or capability to target OT networks[53], namely KOSTOVITE, PETROVITE, and ERYTHRITE. In general, adversaries are willing to dedicate time and resources in compromising their targets to harvest information on the OT networks for future purposes. Currently, most adversaries in this space prioritise pre-positioning and information gathering over disruption as strategic objectives[53] .

We also observed two new additions to the short list of ICS-capable malware: Industroyer2[54] and INCONTROLLER[55] [56] (also known as PIPEDREAM[57]). ICS-specific malware is rare, and Industroyer2 and INCONTROLLER are the sixth and seventh known ICS malware, respectively, following Stuxnet[58], Havex[59], BlackEnergy2[60], CrashOverride[61] or Industroyer[62], and Trisis or Triton[63] [64] [65] [53]. Industroyer2 was detected while analysing an attack against a Ukrainian energy company with the intent to cut power in a Ukrainian region during the Russia Ukraine crisis. The perpetrator of this attack is assessed to be the state-sponsored threat group Sandworm[54]. INCONTROLLER is very likely a state-sponsored malware (based on the resources needed for development and research) focused on disruption, sabotage, and potential destruction.

In our assessment, state-backed threat actors will step up their reconnaissance against OT networks[160] develop capabilities and increasingly target them for the foreseeable future, especially during times of crisis and armed conflict. We assess that state-backed actors interested in targeting OT networks will continue dedicating resources and developing extensible ICS malware frameworks because of their modularity and capability in targeting multiple victims and equipment used across multiple industries[66].

Destructive attacks as a prominent component of state actors' operations. During the Russia-Ukraine conflict, it was observed that cyber actors conducting operations in concert with kinetic military action[67]. Part of these operations included widespread use of wiper attacks[68] to destroy and disrupt networks of governmental agencies and critical infrastructure entities. The intentions of the threat actors in using wiper malware are predominantly to degrade the functioning of the targeted entities but also to undermine public trust in the country's leadership, spread FUD (fear, uncertainty, and doubt), and facilitate disinformation operations.

[53] Dragos – 2021 ICS/OT Cybersecurity Year in Review - https://www.dragos.com/year-in-review/
[54] ESET - Industroyer2: Industroyer reloaded - https://www.welivesecurity.com/2022/04/12/industroyer2-industroyer-reloaded/
[55] CISA - APT Cyber Tools Targeting ICS/SCADA Devices - https://www.cisa.gov/uscert/ncas/alerts/aa22-103a
[56] Mandiant - INCONTROLLER: New State-Sponsored Cyber Attack Tools Target Multiple Industrial Control Systems - https://www.mandiant.com/resources/incontroller-state-sponsored-ics-tool
[57] Dragos - CHERNOVITE's PIPEDREAM Malware Targeting Industrial Control Systems (ICS) - https://www.dragos.com/blog/industry-news/chernovite-pipedream-malware-targeting-industrial-control-systems/
[58] Wired - An Unprecedented Look at Stuxnet, the World's First Digital Weapon - https://www.wired.com/2014/11/countdown-to-zero-day-stuxnet/
[59] Palo Alto Unit 42 - Why Havex Is a Game-Changing Threat to Industrial Control Systems - https://unit42.paloaltonetworks.c
[60] Dragos - The Evolution of Cyber Attacks on Electric Operations - https://www.dragos.com/blog/industry-news/the-evolution-of-cyber-attacks-on-electric-operations/
[61] Dragos - CRASHOVERRIDE Analysis of the Threat to Electric Grid Operations - https://www.dragos.com/wp-content/uploads/CrashOverride-01.pdf
[62] ESET - Industroyer: Biggest malware threat to critical infrastructure since Stuxnet - https://www.eset.com/int/industroyer/
[63] Dragos - TRISIS Malware Analysis of Safety System Targeted Malware - https://www.dragos.com/wp-content/uploads/TRISIS-01.pdf
[64] Mandiant - Attackers Deploy New ICS Attack Framework 'TRITON' and Cause Operational Disruption to Critical Infrastructure - https://www.mandiant.com/resources/attackers-deploy-new-ics-attack-framework-triton
[65] Dragos - PIPEDREAM: CHERNOVITE'S EMERGING MALWARE TARGETING INDUSTRIAL CONTROL SYSTEMS - https://hub.dragos.com/hubfs/116-Whitepapers/Dragos_ChernoviteWP_v2b.pdf?hsLang=en
[66] Mandiant - INDUSTROYER.V2: Old Malware Learns New Tricks - https://www.mandiant.com/resources/industroyer-v2-old-malware-new-tricks
[67] Microsoft – Special Report: Ukraine – An overview of Russia's cyberattack activity in Ukraine - https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE4Vwwd
[68] Max Smeets – Wipers - https://docs.google.com/spreadsheets/d/1qpVZVaSmxNELB2DaGEDzp6QNG236KcC3wPmGUtMQ-zQ/edit#gid=0
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

As of the time of writing, state-sponsored threat actors have deployed nine wiper malware families: WhisperGate[69] or WhisperKill, Hermetic Wiper[70], CaddyWiper[71], DesertBlade[72], AcidRain[73], Industroyer2[54], IsaacWiper[74], and DoubleZero[75]. Apart from the sheer number of distinct wiper malware families observed, the tempo of these operations was also relatively high. From 23 February 2022 to 8 April 2022, Microsoft reported that they saw 40 discrete destructive attacks targeting hundreds of systems in dozens of Ukrainian organisations [67]

An interesting observation was the targeting of satellite communications in which the AcidRain wiper malware was used. The EU[76], US[77], and the UK[78] (among others[79]) formally pointed at Russia for hacking Viasat (a commercial satellite communication company) before the Ukraine invasion. The impact of this attack was particularly observed in Ukraine as Viasat satellite modems were not functioning. There was also spill-over across central Europe as wind farms were disrupted[80] and satellite internet connectivity was impacted.

It is our assessment that destructive or disruptive operations by state-backed actors will certainly continue as the conflict goes on. Within Ukraine, the prime targets include the government and military networks and the energy and communications sectors from the perspective of critical infrastructure. Further disruptive operations could potentionally spill-over to other countries.

Furthermore, it is our assessment that Western or NATO allies (especially critical infrastructure entities[81]) will likely be targeted as part of retaliatory actions in response to the sanctions imposed on Russia and the support provided to Ukraine[82]. There is a possibility that some pro-Russia cybercrime ransomware groups will be coordinated to conduct destructive operations against western organisations. Finally, state-sponsored groups may leverage existing ransomware variants to disguise their operations in order to generate plausible deniability of their activities [83].[189]

Public attribution and legal actions continue. Last year in ETL 2021, we highlighted the trend of governments 'stepping up their game' to disrupt, 'name and shame', and take legal action against state-sponsored threat actors.[22]

During the reporting period, many significant events took place involving state-sponsored actors.

- A Venezuelan was charged for using and selling ransomware associated with Iran[84]. This indictment provides an indication of the interest of state-backed actors in leveraging ransomware (and buying this capability) to achieve their strategic goals[85], although this aspect needs to be further examined.

[69] CISA - Update: Destructive Malware Targeting Organizations in Ukraine - https://www.cisa.gov/uscert/ncas/alerts/aa22-057a
[70] Sentinel LABS - HermeticWiper | New Destructive Malware Used In Cyber Attacks on Ukraine - https://www.sentinelone.com/labs/hermetic-wiper-ukraine-under-attack/
[71] ESET - CaddyWiper: New wiper malware discovered in Ukraine - https://www.welivesecurity.com/2022/03/15/caddywiper-new-wiper-malware-discovered-ukraine/
[72] Microsoft - Cyber threat activity in Ukraine: analysis and resources - https://msrc-blog.microsoft.com/2022/02/28/analysis-resources-cyber-threat-activity-ukraine/
[73] Sentinel LABS - AcidRain | A Modem Wiper Rains Down on Europe - https://www.sentinelone.com/labs/acidrain-a-modem-wiper-rains-down-on-europe/
[74] ESET - IsaacWiper and HermeticWizard: New wiper and worm targeting Ukraine - https://www.welivesecurity.com/2022/03/01/isaacwiper-hermeticwizard-wiper-worm-targeting-ukraine/
[75] Security Affairs - Ukrainian enterprises hit with the DoubleZero wiper - https://securityaffairs.co/wordpress/129417/malware/doublezero-wiper-hit-ukraine.html
[76] European Council - Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union - https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/
[77] U.S. Department of State - Attribution of Russia's Malicious Cyber Activity Against Ukraine - https://www.state.gov/attribution-of-russias-malicious-cyber-activity-against-ukraine/
[78] GOV.UK - Russia behind cyber-attack with Europe-wide impact an hour before Ukraine invasion - https://www.gov.uk/government/news/russia-behind-cyber-attack-with-europe-wide-impact-an-hour-before-ukraine-invasion
[79] Washington Post - U.S. allies blame Russia for a cyberattack early in its Ukraine invasion - https://www.washingtonpost.com/politics/2022/05/11/us-allies-blame-russia-cyberattack-early-its-ukraine-invasion/
[80] Reuters - Satellite outage knocks out thousands of Enercon's wind turbines - https://www.reuters.com/business/energy/satellite-outage-knocks-out-control-enercon-wind-turbines-2022-02-28/
[81] CISA - Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure - https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
[82] IT World Canada - Canadian, US, UK sanctions may spark retaliatory cyberattacks on Western critical infrastructure - https://www.itworldcanada.com/article/us-uk-sanctions-may-spark-retaliatory-cyber-attacks-on-western-critical-infrastructure/474071
[83] The Hacker News - State-Backed Hackers Using Ransomware as a Decoy for Cyber Espionage Attacks - https://thehackernews.com/2022/06/state-backed-hackers-using-ransomware.html
[84] U.S. Department of Justice - Hacker and Ransomware Designer Charged for Use and Sale of Ransomware, and Profit Sharing Arrangements with Cybercriminals - https://www.justice.gov/usao-edny/pr/hacker-and-ransomware-designer-charged-use-and-sale-ransomware-and-profit-sharing
[85] The Institute for National Security Studies - Iranian Cyber Influence Operations against Israel Disguised as Ransomware Attacks - https://www.inss.org.il/publication/cyber-iran/

Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

- The USA charged four operators of state-sponsored threat group APT40[86].
- Ukraine's Security Service (SBU) indicted three operators of the group Gamaredon[87].
- Two Iranian were charged with carrying out cyber campaigns and influence operations related to the 2020 US Presidential election[88].
- The US Department of Treasury sanctioned Blender cryptocurrency mixer service after laundering crypto for the state-sponsored Lazarus threat group[89].
- Four Russians were charged with participating in the Triton and Dragonfly cyber operations against critical infrastructure[90].
- UC Berkeley's Human Rights Centre sent a formal request to the Office of the Prosecutor for the International Criminal Court in the Hague to prosecute the Sandworm threat group on charges of war crimes for its involvement in shutting off power in Ukraine during 2015 and 2016[91].
- The FBI shut down a botnet named Cyclops Blink, controlled by Russia's military intelligence service (GRU)[92].
- The EU and US allies formally attributed the cyberattack against commercial satellite company Viasat to Russia[93] [94].
- The EU and Member States have strongly condemned the cyberattacks against Ukraine[95] and the Distributed Denial of Service (DDoS) attacks against several Member States of the EU[96].
- The Attorney General has issued an arrest warrant for a hacker of the state-sponsored APT28 group[97]. The adversary conducted cyber espionage against a NATO think tank in 2017.

In our view, as cyber operations have become a priority for governments, we will certainly observe increased efforts by them in the public attribution of cyber campaigns, the disruption of the infrastructure of adversaries, and indictments to 'name and shame' operators[6]. It is also our assessment that more states will likely continue to take legal actions against threat actors in this area in the near to mid-term future.

On the other hand, it is still unclear how these activities will deter highly sophisticated and determined state-backed threat actors in the long term. A good example is the state-sponsored threat group APT41 which had seven of its operators indicted by the US Department of Justice and part of its infrastructure seized on 7 September 2020[98]. However, the group set up a new infrastructure and continued its operations from late 2021 until mid-2022[47] . Another example is the threat group APT40 which kept advertising for new recruits despite its indictment by the FBI[99]. These

[86] U.S. Department of Justice - Four Chinese Nationals Working with the Ministry of State Security Charged with Global Computer Intrusion Campaign Targeting Intellectual Property and Confidential Business Information, Including Infectious Disease Research - https://www.justice.gov/opa/pr/four-chinese-nationals-working-ministry-state-security-charged-global-computer-intrusion
[87] Kyiv Post - SBU unveils names of Russian hackers attacking Ukraine since 2014 - https://www.kyivpost.com/technology/sbu-unveils-names-of-russian-hackers-attacking-ukraine-since-2014.html
[88] U.S. Department of Justice - Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election - https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed
[89] U.S. Department of Treasury - Cyber-related Designation; North Korea Designation Update - https://home.treasury.gov/policy-issues/financial-sanctions/recent-actions/20220506
[90] U.S. Department of Justice - Four Russian Government Employees Charged in Two Historical Hacking Campaigns Targeting Critical Infrastructure Worldwide - https://www.justice.gov/opa/pr/four-russian-government-employees-charged-two-historical-hacking-campaigns-targeting-critical
[91] Wired - The Case for War Crimes Charges Against Russia's Sandworm Hackers - https://www.wired.com/story/cyber-war-crimes-sandworm-russia-ukraine/
[92] U.S. Department of Justice - Justice Department Announces Court-Authorized Disruption of Botnet Controlled by the Russian Federation's Main Intelligence Directorate (GRU) - https://www.justice.gov/opa/pr/justice-department-announces-court-authorized-disruption-botnet-controlled-russian-federation
[93] Council of the EU - Russian cyber operations against Ukraine: Declaration by the High Representative on behalf of the European Union - https://www.consilium.europa.eu/en/press/press-releases/2022/05/10/russian-cyber-operations-against-ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union/
[94] Washington Post - U.S. allies blame Russia for a cyberattack early in its Ukraine invasion - https://www.washingtonpost.com/politics/2022/05/11/us-allies-blame-russia-cyberattack-early-its-ukraine-invasion/
[95] Council of the EU - Ukraine: Declaration by the High Representative on behalf of the European Union on the cyberattack against Ukraine - https://www.consilium.europa.eu/en/press/press-releases/2022/01/14/ukraine-declaration-by-the-high-representative-on-behalf-of-the-european-union-on-the-cyberattack-against-ukraine/
[96] Council of the EU - 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 - 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/
[97] Security Affairs - Russian APT28 hacker accused of the NATO think tank hack in Germany - https://securityaffairs.co/wordpress/132452/hacking/apt28-hacked-nato-think-tank.html
[98] U.S. Department of Justice - Seven International Cyber Defendants, Including 'Apt41' Actors, Charged In Connection With Computer Intrusion Campaigns Against More Than 100 Victims Globally - https://www.justice.gov/opa/pr/seven-international-cyber-defendants-including-apt41-actors-charged-connection-computer
[99] Financial Times - Chinese hackers kept up hiring drive despite FBI indictment - https://www.ft.com/content/341d7b60-228d-497e-bbb3-14ac0537f96a

Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

examples indicate that sometimes the indictments of the operators of a threat group may not have a significant impact on the (cyber) operations of that threat group[139] and further coordinated actions are encouraged.

State-backed threat actors increasingly focus on supply chain compromises. Supply chain compromises accounted for 17% (or up to 62% according to other sources[100]) of the intrusions in 2021 compared to less than 1% during 2020[31].Since the revelation of the SolarWinds supply chain campaign in December 2020, state-backed threat actors have realised the potential and have increasingly targeted third parties to expand their cyber operations downstream to their clients.

Cloud Service Providers (CSPs), Managed Services Providers (MSPs), and IT services organisations are prime targets for threat actors to exploit their trust relationships to conduct nefarious operations[101]. The NOBELIUM activity group consistently targeted service providers and their downstream customers. At the same time, threat actors targeted over 40 IT services companies (primarily based in India) to access their clients' networks[102].

In our assessment state-backed threat actors will certainly further develop their toolsets to target and compromise supply chains[103] as indirect vectors to achieve their objectives. Software supply chain attacks (e.g. open-source software development libraries, popular software packages, software platform compromises, etc.) will very likely be leveraged by well-funded state-backed groups to get a foothold in the networks of hundreds of victims [143]

Geopolitics continue to influence cyber operations. As mentioned in ETL 2021, geopolitics is one of the key driver for collecting intelligence through cyber operations. It was observed that targeting increases consistently with increasing geopolitical tensions [47].

According to public reports, several cyber operations have been observed against Ukrainian entities by state-backed groups due to the ongoing armed conflict[43]. These threat groups focused on initial access operations and collection of intelligence that would give military forces any tactical or strategic advantage. State-sponsored threat actors have also targeted 128 governmental organisations in 42 countries that support Ukraine (The USA, The EU, Poland, countries bordering Russia, and NATO members were prioritised)[104].

Security researchers believe there is a direct link between a county's 5-Year Plan[105] and the targets of state-sponsored threat groups[31]. These threat groups are reportedly tasked with collecting intelligence on investments, negotiations, and influence related to the Belt and Road Initiative[43]. During the reporting period, state-sponsored threat actors have been observed targeting entities from countries in Southeast Asia, Japan[106], Australia[107] and Taiwan[108]. Due to increased tensions between specific countries in the Asian Region, an interesting observation is that state-sponsored threat actors have targeted countries (including Member States of the EU) that had established closer ties with Taiwan[109]. Another interesting development is that some threat actors targeted Ukrainian[110] and Russian[111] entities during the early days of the conflict, likely for the collection of intelligence.

[100] Verizon – 2022 DBIR - https://www.verizon.com/business/resources/reports/dbir/2022/master-guide/
[101] CISA, NSA, FBI - CISA, NSA, FBI AND INTERNATIONAL CYBER AUTHORITIES ISSUE CYBERSECURITY ADVISORY TO PROTECT MANAGED SERVICE PROVIDERS (MSP) AND CUSTOMERS - https://www.cisa.gov/news/2022/05/11/joint-cybersecurity-advisory-protect-msp-providers-and-customers
[102] Microsoft - Iranian targeting of IT sector on the rise - https://www.microsoft.com/security/blog/2021/11/18/iranian-targeting-of-it-sector-on-the-rise/
[103] Microsoft - NOBELIUM targeting delegated administrative privileges to facilitate broader attacks - https://www.microsoft.com/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/
[104] Microsoft - Defending Ukraine: Early Lessons from the Cyber War - https://blogs.microsoft.com/on-the-issues/2022/06/22/defending-ukraine-early-lessons-from-the-cyber-war/
[105] DIGICHINA - Translation: 14th Five-Year Plan for National Informatization – Dec. 2021 - https://digichina.stanford.edu/work/translation-14th-five-year-plan-for-national-informatization-dec-2021/
[106] Ministry of Foreign Affairs of Japan - Cases of cyberattacks including those by a group known as APT40 which the Chinese government is behind (Statement by Press Secretary YOSHIDA Tomoyuki) - https://www.mofa.go.jp/press/danwa/press6e_000312.html
[107] The Hacker News - A Decade-Long Chinese Espionage Campaign Targets Southeast Asia and Australia - https://thehackernews.com/2022/06/a-decade-long-chinese-espionage.html
[108] The Record - Chinese hackers linked to months-long attack on Taiwanese financial sector - https://therecord.media/chinese-hackers-linked-to-months-long-attack-on-taiwanese-financial-sector/
[109] State Security department of the Republic of Lithuania - NATIONAL THREAT ASSESSMENT 2022 - https://www.vsd.lt/wp-content/uploads/2022/04/ANGL-el-_.pdf
[110] BBC - Mystery of alleged Chinese hack on eve of Ukraine invasion - https://www.bbc.com/news/technology-60983346
[111] CheckPoint - Twisted Panda: Chinese APT espionage operation against Russian's state-owned defense institutes - https://research.checkpoint.com/2022/twisted-panda-chinese-apt-espionage-operation-against-russians-state-owned-defense-institutes/
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Additionally, threat actors have reportedly targeted entities in the Middle Eastern area as tensions have escalated between various countries. These actors widely adopted ransomware and[43] 'lock-and-leak'[47] information operations, and they mainly targeted organisations in Israel and the USA, and in the Middle East and North African regions. The cyber operations between these countries in the Middle Eastern area had reached such a scale that they also affected civilians[112].

Cyber operations reportedly targeted South Korean, US, European, and Japanese entities[43]. The threat actors strongly focused on collecting diplomatic and geopolitical intelligence, likely driven by its requirements related to the sanctions imposed on their state[43]. In this particular case, another main driver for its cyber operations is the acquisition of financial resources, primarily through crypto heists[113].

Due to the volatile international situation, we expect to observe more cyber operations being driven by geopolitics in the near to mid-term. The geopolitical situation in areas like the Middle East, Eastern Mediterranean, Artic Region, Baltics, Afghanistan, Yemen, Syria, and Libya might trigger cyber operations and potentially damaging cyber-attacks.[181] It needs to be nonetheless clarified, that the cyber operation triggered by the geopolitical situation in Ukraine have a bigger potential, relevance and connection to the EU.

Finally, during the reporting period, we also observed cyber campaigns from threat groups that reportedly had connections with an increasing number of states such as Vietnam, Turkey, Pakistan, India, Ukraine, Belarus, and others[114]. We expect to see more and more states deploying their cyber capabilities for the collection of intelligence, especially in times of increased tensions or conflict.

Armies of cyber volunteers?

The armed conflict in Ukraine mobilised many hacktivists, cybercrime, and nation-state groups[115]. The case of the IT Army of Ukraine[116] is a unique case that is difficult to categorise; it could be considered a hacktivist group of volunteers, or a state-backed group or a hybrid one. As of the time of writing, the cyber security community has not reached a consensus. The IT Army of Ukraine will definitely feed future scholars in cyber warfare studies, and it might highlight a trend in future conflicts.

On 26 February 2022, Ukraine's deputy prime minister and minister for digital transformation announced the creation of Ukraine's IT Army[117]. The announcement was a call for volunteers whose actions on the cyber front were coordinated through a Telegram channel (the channel had 300.000 subscribers)[118]. Ukraine's IT Army managed to target various entities and conducted mostly coordinated Distributed Denial of Services (DDoS) attacks but was not limited to such attacks[119] [293].

At the time of the Russian invasion, Ukraine had no military cyber command unit[120]. Based on the model of Estonia's Cyber Defence League[121], as well as out of necessity, Ukraine managed to create a hybrid entity that is quite difficult to categorise as it is comprised of Ukrainian and international civilians, private companies, as well as Ukrainian defence and military personnel. It is not a civilian, military, public, private, local or international entity[122]. Moreover, it

[112] The New York Times - Israel and Iran Broaden Cyberwar to Attack Civilian Targets - https://www.nytimes.com/2021/11/27/world/middleeast/iran-israel-cyber-hack.html
[113] Mandiant - Not So Lazarus: Mapping DPRK Cyber Threat Groups to Government Organizations - https://www.mandiant.com/resources/mapping-dprk-groups-to-government
[114] Mandiant - UNC1151 Assessed with High Confidence to have Links to Belarus, Ghostwriter Campaign Aligned with Belarusian Government Interests - https://www.mandiant.com/resources/unc1151-linked-to-belarus-government
[115] Cyberknow - Update 15. 2022 Russia-Ukraine war — Cyber group tracker. June 13. - https://cyberknow.medium.com/update-15-2022-russia-ukraine-war-cyber-group-tracker-june-13-35289e4bfdb7
[116] CFR - Ukrainian IT Army - https://www.cfr.org/cyber-operations/ukrainian-it-army
[117] Twitter – Mykhailo Fedorov - https://twitter.com/FedorovMykhailo/status/1497642156076511233
[118] Telegram – itarmyofukraine2022 - https://t.me/itarmyofukraine2022
[119] CrowdStrike - Compromised Docker Honeypots Used for Pro-Ukrainian DoS Attack - https://www.crowdstrike.com/blog/compromised-docker-honeypots-used-for-pro-ukrainian-dos-attack/
[120] Foreign Policy - Don't Underestimate Ukraine's Volunteer Hackers - https://foreignpolicy.com/2022/04/11/russia-cyberwarfare-us-ukraine-volunteer-hackers-it-army/
[121] KAITSELIIT - Estonian Defence League's Cyber Unit - https://www.kaitseliit.ee/en/cyber-unit
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

raises topics for discussion related to international laws in cyberspace, state cyber norms, the targeting of civilian infrastructure, and the ethics of private companies[122].

It is our assessment that state actors will likely adopt the structure and setup of the IT Army of Ukraine as a blueprint for non-state participation in future conflicts[122] [132] (especially for states that lack an organised military cyber command unit). It is also likely that these crowdsourced cyber armies will incorporate a non-public side which will further complicate their structure, operational conduct, and analysis by the cyber community, scholars, and cyber warfare analysts.

Tech companies' increasing defensive role in cyber operations during conflicts.

During the Russian invasion of Ukraine, it was observed for the first time that some big technology companies were taking sides and supporting Ukraine in the cyber war front [132] [123]. The most prominent example is Microsoft which provided support to Ukrainian cybersecurity officials to tackle FoxBlade malware[124] as well as awareness and intelligence reports on Russian cyber operations[125] [126]. Microsoft and AWS have been awarded the 'Peace Prize' by the President of Ukraine, Volodymyr Zelenskyy[127].

We would like to emphasise that this trend is interesting but also challenging to assess. Currently, the long-term consequences of such a strong alignment with one side of the conflict are not well understood [132]. Moreover, discussions are being raised about the role and responsibilities of private companies in future cyber operations during conflicts (e.g. should tech companies take on the burden of defence?[132]).

Increasing sophistication and scope of disinformation[43].

Several state-backed actors have built the capability to use social media platforms, search engines and messaging services to disseminate disinformation. Their approach differs from the traditional disinformation campaigns since these services provide out-of-the-box tools to test and optimise their content and monitor the outreach and impact of disinformation campaigns[43]. Moreover, developments in Machine Learning (ML), Artificial Intelligence (AI), deep fakes, and voice biometrics have provided threat actors with powerful tools to create misleading content for their campaigns[43].

Some of the significant information developments that were observed during the reporting include the following.

- Influence operations that were either financially motivated or linked to a state [128] [129] [130] (e.g. Turkey, Iraq, China, Russia, Latin America, Philippines, Iran, Sudan, Uganda, China, Nicaragua, etc.) were active.
- Chinese threat groups too were active on social media to amplify pro-Chinese messages[50] and information operations in Europe originating from China and Russia[41].
- There were coordinated information operations related to the Russia-Ukraine crisis (and linked to Russian threat actors)[130]. Some information operations coincided with disruptive or destructive and other cyber threat activity, while others contained fabricated content and promoted Russian favoured narratives via various platforms[131]. Moreover, some leaks and dumps of information from pro-Russia and pro-Ukraine actors had psychological effects on the ground[132].

[122] ETH Zurich CSS – Stefan Soesanto - The IT Army of Ukraine Structure, Tasking, and Ecosystem - https://css.ethz.ch/content/dam/ethz/special-interest/gess/cis/center-for-securities-studies/pdfs/Cyber-Reports-2022-06-IT-Army-of-Ukraine.pdf
[123] Miko Hypponen - Mikko Hypponen 'Ctrl-Z' at #SPHERE22 - https://www.youtube.com/watch?v=Yjogm9ejcPQ
[124] New York Times - As Tanks Rolled Into Ukraine, So Did Malware. Then Microsoft Entered the War. - https://www.nytimes.com/2022/02/28/us/politics/ukraine-russia-microsoft.html
[125] Microsoft - Disrupting cyberattacks targeting Ukraine - https://blogs.microsoft.com/on-the-issues/2022/04/07/cyberattacks-ukraine-strontium-russia/
[126] Microsoft - The hybrid war in Ukraine - https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/
[127] TechRadar - Microsoft and AWS awarded Ukrainian peace prize for cloud efforts - https://www.techradar.com/news/microsoft-and-aws-awarded-ukrainian-peace-prize-for-cloud-efforts
[128] Google Threat Analysis Group - TAG Bulletin: Q4 2021 - https://blog.google/threat-analysis-group/tag-bulletin-q4-2021/
[129] Google Threat Analysis Group - TAG Bulletin: Q3 2021 - https://blog.google/threat-analysis-group/tag-bulletin-q3-2021/
[130] Google Threat Analysis Group - TAG Bulletin: Q1 2022 - https://blog.google/threat-analysis-group/tag-bulletin-q1-2022/
[131] Mandiant - The IO Offensive: Information Operations Surrounding the Russian Invasion of Ukraine - https://www.mandiant.com/resources/information-operations-surrounding-ukraine
[132] ECCRI - Cyber Operations during the 2022 Russian invasion of Ukraine: Lessons Learned (so far) - https://eccri.eu/wp-content/uploads/2022/07/ECCRI_WorkshopReport_Version-Online.pdf
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

- Actors conducting pro-China and pro-Iran information operations took opportunistic advantage of the Russian invasion to further progress their strategic objectives[134].
- According to a public report[133], there has indeed been a '*Russification*' of Chinese influence operations since about 2017. The report mentions that China 'draws inspiration from Russia' and that there is a certain degree of cooperation.
- One of the major groups conducting cyber-enabled information attacks in Europe is Ghostwriter, linked to Belarusian interests [134135109].
- Two Iranian nationals were charged with conducting cyber-enabled disinformation to influence the 2020 US Presidential Election[136].
- Several threat actors (such as Moses Staff[137] and Black Shadow[138]) have conducted a number of hack and leak operations, mostly against targets within Israel. These operations have also included a disruptive element.

It is our assessment that nation-backed threat actors will certainly be conducting information operations for the foreseeable future. As the Russia-Ukraine conflict progresses, we expect information operations related to the conflict to expand in scope and outside Eastern Europe, in addition to being leveraged to serve the strategic objectives of various states[131]. Finally, we would like to emphasise to governments and media organisations the heightened risk of cyber operations (compromise, disruption, and information operations) during high-profile physical or geopolitical events.

2.2 CYBERCRIME ACTOR TRENDS

Cybercriminals exhibit increasing capability and interest in supply chain attacks. While supply chain attacks are primarily associated with state-backed actors[139], cybercriminals became more interested and proficient in the supply chain as an attack vector to conduct their operations during the reporting period. During the reporting period, supply chain attacks have become increasingly interconnected with ransomware campaigns[140] [141] [142], allowing the threat actors to increase the scale of their operations with a single initial compromise[150]. Such supply chain attacks usually lead to ransomware deployment, coin mining, stealing cryptocurrency, or stealing credentials that will enable cybercriminals to facilitate their malicious activities further.

Public reports say supply chain attacks are related to poisoned developer libraries and software platform compromises[143]. Software supply chain attacks (e.g. via widely deployed software) can have a high impact and [143]disrupt critical services or even services not directly affected. Indicative examples of such attacks include the Node Package Manager (NPM) package compromises[144] [145] [143] exploitation of the Log4j Java logging library vulnerability[144], malicious python library manager PyPi packages [146] [147], and malicious RubyGems packages[148]. Major

[133] French Institute for Strategic Research - CHINESE INFLUENCE OPERATIONS - https://www.irsem.fr/report.html
[134] Mandiant - UNC1151 Assessed with High Confidence to have Links to Belarus, Ghostwriter Campaign Aligned with Belarusian Government Interests - https://www.mandiant.com/resources/unc1151-linked-to-belarus-government
[135] Mandiant – M-Trends 2022 - https://www.mandiant.com/resources/m-trends-2022
[136] U.S. Department of Justice - Two Iranian Nationals Charged for Cyber-Enabled Disinformation and Threat Campaign Designed to Influence the 2020 U.S. Presidential Election - https://www.justice.gov/opa/pr/two-iranian-nationals-charged-cyber-enabled-disinformation-and-threat-campaign-designed
[137] Bleeping Computer - Moses Staff hackers wreak havoc on Israeli orgs with ransomless encryptions - https://www.bleepingcomputer.com/news/security/moses-staff-hackers-wreak-havoc-on-israeli-orgs-with-ransomless-encryptions/
[138] Cyber Scoop - Hack-and-leak group Black Shadow keeps targeting Israeli victims - https://www.cyberscoop.com/hack-and-leak-group-black-shadow-keeps-targeting-israeli-victims/
[139] PwC Cyber Threats 2021: A Year in Retrospect - https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect.html
[140] Trend Micro Security Prediction for 2022 - https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2022
[141] Europol - Internet Organised Crime Threat Assessment (IOCTA) - https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021
[142] Tenable – 2021 Threat Landscape Retrospective - https://www.tenable.com/cyber-exposure/2021-threat-landscape-retrospective
[143] Accenture – Cyber Threat Intelligence Report – Volume 2- 2021 - https://www.accenture.com/_acnmedia/PDF-173/Accenture-Cyber-Threat-Intelligence-Report-Vol-2.pdf
[144] Red Canary 2022 Threat Detection Report - https://resource.redcanary.com/rs/003-YRU-314/images/2022_ThreatDetectionReport_RedCanary.pdf
[145] CISA – Malware Discovered in Popular NPM package, ua-parser-js - https://www.cisa.gov/uscert/ncas/current-activity/2021/10/22/malware-discovered-popular-npm-package-ua-parser-js
[146] JFrog - Python Malware Imitates Signed PyPI Traffic in Novel Exfiltration Technique - https://jfrog.com/blog/python-malware-imitates-signed-pypi-traffic-in-novel-exfiltration-technique/
[147] JFrog - JFrog Detects Malicious PyPI Packages Stealing Credit Cards and Injecting Code - https://jfrog.com/blog/malicious-pypi-packages-stealing-credit-cards-injecting-code/#products
[148] Bleeping Computer - Malicious RubyGems packages used in cryptocurrency supply chain attack - https://www.bleepingcomputer.com/news/security/malicious-rubygems-packages-used-in-cryptocurrency-supply-chain-attack/
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

obstacles to detecting and defending against such attacks are the large number of interdependencies of various open-source packages and the fact that most organisations do not audit, manage or inspect the third-party packages imported into supply chains and trusted environments[149].

Managed Service Providers (MSPs) have also been increasingly targeted by ransomware threat groups[150] (as well as state-sponsored groups) due to their trusted network connectivity and privileged access to their customers. In May 2022, the cybersecurity authorities of the United Kingdom, Australia, Canada, New Zealand and the United States released an alert informing organisations about the cyber threats to MSPs and their customers[151].

We expect cybercriminals to continue targeting the software supply chain and MSPs for the foreseeable future. Cybercrime threat actors will certainly be further enabled by the increased focus on Access-as-a-Service (AaaS) brokers in supply chain targeting. Cybercriminals are also likely to target the management tools used by MSPs such as professional services automation software (PSA) or remote monitoring and management (RMM) tools[152]. Finally, we expect the continued exploitation of critical vulnerabilities in the remote execution of code affecting the software supply chain (e.g. Log4j) in upcoming months[145]. Organisations are advised to include such supply chain attacks in their threat modelling process and evolve their strategies by applying the zero-trust approach in their security practices[140]. Moreover, the third-party risk teams of organisations should work with their critical suppliers and partners on enhancing their security processes and should define contractual commitments on the basis of acceptable risk levels[151].

Widespread cloud adoption provides attack opportunities for cybercriminals. COVID-19 has accelerated the adoption of cloud-based services supporting the business processes of organisations. Since cybercriminals follow trends in technology, it comes as no surprise that cybercriminals are targeting cloud environments.

Cybercriminals target cloud services mostly in the following ways.

- Exploiting cloud vulnerabilities: virtualisation infrastructure has been increasingly targeted (e.g. VMWare vSphere and ESXi platforms[160]) by cybercriminals and especially by ransomware groups[153].
- Using cloud services for hosting their infrastructure: cybercriminals take advantage of the highly scalable and reliable cloud infrastructure [143]and use legitimate cloud services to bypass security controls by blending into normal network traffic[154].
- Targeting cloud credentials: cybercriminals use social engineering attacks to harvest credentials for cloud services (e.g. Microsoft Office 365, Okta, etc.)[154].
- Exploiting misconfigured image containers [154]cybercriminals increasingly target poorly configured Docker containers[155] and Kubernetes clusters[156].
- Targeting cloud instances for cryptomining[157] (e.g. TeamTNT group): security researchers have identified a cloud-focused toolset from the TeamTNT group[158].
- Targeting cloud infrastructure (e.g. Azure AD), cloud application programming interfaces (APIs), and cloud-hosted backups by ransomware groups [150]to infiltrate cloud environments [154]and increase impact[143].

It is our assessment that cybercriminals will certainly continue to compromise and abuse cloud environments as cloud adoption grows[159][140]. We expect more malware families to shift their targeting from generic Linux systems to container platforms used in cloud solutions (e.g. Docker)[160]. At the same time, ransomware groups will continue

[149] Palo Alto Networks – Unit 42 Cloud Threat Report 2H 2021 - https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research-2h21
[150] CISA - 2021 Trends Show Increased Globalized Threat of Ransomware - https://www.cisa.gov/uscert/ncas/alerts/aa22-040a
[151] CISA - Protecting Against Cyber Threats to Managed Service Providers and their Customers - https://www.cisa.gov/uscert/ncas/alerts/aa22-131a
[152] Acronis Cyberthreats Report 2022 - https://www.acronis.com/en-us/blog/posts/acronis-cyberthreats-report-2022-unveils-cyberthreat-predictions/
[153] Mandiant – M-Trends 2022 - https://www.mandiant.com/resources/m-trends-2022
[154] CrowdStrike – 2022 Global Threat Report - https://www.crowdstrike.com/resources/reports/global-threat-report/
[155] CrowdStrike - LemonDuck Targets Docker for Cryptomining Operations - https://www.crowdstrike.com/blog/lemonduck-botnet-targets-docker-for-cryptomining-operations/
[156] Bleepeng Computer - Attackers deploy cryptominers on Kubernetes clusters via Argo Workflows - https://www.bleepingcomputer.com/news/security/attackers-deploy-cryptominers-on-kubernetes-clusters-via-argo-workflows/
[157] Google Cloud – Threat Horizons – Cloud Threat Intelligence November 2021 - https://services.google.com/fh/files/misc/gcat_threathorizons_full_nov2021.pdf
[158] VX Underground – Twitter - https://twitter.com/vxunderground/status/1453627390387802117
[159] Mandiant – Security Predictions 2022 - https://www.mandiant.com/resources/security-predictions-2022-report
[160] IBX X-Force Threat Intelligence Index 2022 - https://www.ibm.com/downloads/cas/ADLMYLAZ
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

developing custom tools for cloud targeting[143]. Finally, cybercriminals will increasingly target cloud APIs to disrupt cloud automated processes, thus causing severe impacts on businesses[161].

Imposing cost on ransomware threat actors. Several governments prioritised ransomware as a national security threat during the reporting period. A combination of (mostly) legal and regulatory responses tried to alter the cost-benefit calculations of cybercriminals while some anti-ransomware initiatives popped up[162] [163] [164] [165].

Law enforcement actions against ransomware groups forced some to leave the stage, some even releasing decryption keys[166]. Moreover, law enforcement agencies have offered millions in rewards for arresting members of ransomware groups[167]. Through international cooperation, law enforcement operations arrested cybercriminals associated with ransomware threat groups such as REvil, Cl0p, NetWalker, and LockerGoga or MegaCortex [168] [169] [170] [171] [172] [173] [174].

Military and intelligence services came into play against ransomware. According to public reports, the US military has acted against ransomware groups[175]. An interesting development was the arrest by the Russian Federal Security Service (FSB) of the members of the REvil ransomware group[176]. This action could be attributed to Russia's pursuit of its strategic geopolitical objectives[177] or the potential targeting of Russian entities by the REvil group[139].

The White House organised a meeting coordinating an international response against ransomware (to which Russia was not invited)[178]. From the regulatory perspective, The Ransom Disclosure Act made it mandatory for ransomware victims to inform the US government within 48 hours of the ransom payment[179]. Finally, the government of the Netherlands indicated that it would use its intelligence and/or armed forces to respond to ransomware attacks[180].

It is our assessment that the efforts of law enforcement to disrupt ransomware groups will continue for the foreseeable future[181]. Law enforcement attention will certainly have an impact on the modus operandi of several ransomware groups (e.g. increased operational security, rebranding, internal conflicts, targeting of small companies[181] etc.) and underground forums (e.g. banning any promotion of ransomware affiliate programmes[182]) for the short-term. However, it is not clear how law enforcement actions will affect the ransomware threat landscape

[161] Acronis – Cyberthreats Report 2022 - https://www.acronis.com/en-us/blog/posts/acronis-cyberthreats-report-2022-unveils-cyberthreat-predictions/
[162] Ransomware Task Force - https://securityandtechnology.org/ransomwaretaskforce/
[163] StopRansomware - https://www.cisa.gov/stopransomware
[164] WEF – Partnership against Cybercrime - https://www.weforum.org/projects/partnership-against-cybercime
[165] U.S. Department of State – Update on the International Counter-Ransomware Initiative - https://www.state.gov/briefings-foreign-press-centers/update-on-the-international-counter-ransomware-initiative
[166] ESET Threat Report T3 2021 - https://www.welivesecurity.com/2022/02/09/eset-threat-report-t32021/
[167] Bleeping Computer - US targets DarkSide ransomware and its rebrands with $10 million reward - https://www.bleepingcomputer.com/news/security/us-targets-darkside-ransomware-and-its-rebrands-with-10-million-reward/
[168] Europol – Five affiliates to REvil unplugged - https://www.europol.europa.eu/media-press/newsroom/news/five-affiliates-to-sodinokibi/revil-unplugged
[169] Interpol – Ransomware gang arrested in Ukraine - https://www.interpol.int/en/News-and-Events/News/2021/Ransomware-gang-arrested-in-Ukraine
[170] Interpol – Major gang members in handcuffs, assets seized - https://www.interpol.int/News-and-Events/News/2021/INTERPOL-led-operation-takes-down-prolific-cybercrime-ring
[171] Europol - 12 targeted for involvement in ransomware attacks against critical infrastructure - https://www.europol.europa.eu/media-press/newsroom/news/12-targeted-for-involvement-in-ransomware-attacks-against-critical-infrastructure
[172] Krebs On Security - Estonian Tied to 13 Ransomware Attacks Gets 66 Months in Prison - https://krebsonsecurity.com/2022/03/estonian-tied-to-13-ransomware-attacks-gets-66-months-in-prison/
[173] Bleeping Computer - NetWalker ransomware affiliate sentenced to 80 months in prison - https://www.bleepingcomputer.com/news/security/netwalker-ransomware-affiliate-sentenced-to-80-months-in-prison/
[174] US Department of Justice - Former Canadian Government Employee Extradited to the United States to Face Charges for Dozens of Ransomware Attacks Resulting in the Payment of Tens of Millions of Dollars in Ransoms - https://www.justice.gov/opa/pr/former-canadian-government-employee-extradited-united-states-face-charges-dozens-ransomware
[175] NY Times - U.S. Military Has Acted Against Ransomware Groups, General Acknowledges - https://www.nytimes.com/2021/12/05/us/politics/us-military-ransomware-cyber-command.html
[176] Bleeping Computer - Russia arrests REvil ransomware gang members, seize $6.6 million - https://www.bleepingcomputer.com/news/security/russia-arrests-revil-ransomware-gang-members-seize-66-million/
[177] Intel471 - What can we expect from the REvil arrests? - https://intel471.com/blog/revil-ransomware-arrests-cybercrime-underground
[178] ZDNet - The White House is having a big meeting about fighting ransomware. It didn't invite Russia - https://www.zdnet.com/article/the-white-house-is-having-a-big-meeting-about-fighting-ransomware-it-didnt-invite-russia/
[179] ZDNet - Ransomware law would require victims to disclose ransom payments within 48 hours - https://www.zdnet.com/article/ransomware-law-would-require-victims-to-disclose-ransom-payments-within-48-hours/
[180] The Record - Netherlands can use intelligence or armed forces to respond to ransomware attacks - https://therecord.media/netherlands-can-use-intelligence-or-armed-forces-to-respond-to-ransomware-attacks/?s=01
[181] QuoIntelligence - Ransomware is here to stay and other cybersecurity predictions for 2022 - https://quointelligence.eu/2022/01/ransomware-and-other-cybersecurity-predictions-for-2022/
[182] Flashpoint - After Ransomware Ads Are Banned On Cybercrime Forums, Alternative Platforms Being Used to Advertise and Recruit - https://flashpoint.io/blog/avoslocker-ransomware-advertise-and-recruit/

Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

(new groups appearing and new business methods)[181] and further increase the risks for ransomware actors [183][159]. Furthermore, we expect to see increased volumes of activity from groups operating outside the USA[159], while Russia-based cybercriminals are unlikely to be deterred due to the arrest of REvil members by the FSB[184][177]. Finally, we expect that governments will increasingly allocate resources to combat ransomware threats by tasking their military and intelligence services to disrupt the operations of cybercriminals, collect intelligence about members of these groups and recover ransom payments[185] [186] [187].

Cybercriminals continue to disrupt the industrial sector. Last year we estimated that cybercrime attacks against Operational Technology (OT) systems would very likely become more disruptive[188]. This assessment still holds true and, during the reporting period, ransomware was the major cause of compromises in the industrial sector, with the manufacturing industry being the most targeted sector by far[189] [190] . Disruptive attacks have had significant impacts on other sectors: food and beverages, healthcare, transportation and energy.

Cybercriminal operations can disrupt OT operations using[196]:

- malware that has an OT-specific module for OT systems[191];
- limited network segmentation allowing ransomware to spread from IT to OT network[192];
- the shutdown of OT infrastructure by operators to prevent the spreading of ransomware to the OT network[193] [194][150];
- exfiltration of sensitive information about the OT environment that can facilitate further cyber-physical attacks by other threat actors (cybercrime as well as state-sponsored groups)[195].

It is our assessment that ransomware groups will likely continue to target and disrupt OT operations for the foreseeable future[196] [197]. Contributing factors to this assessment are:

- the ongoing digital transformation in the industrial sector and the increased connectivity between IT and OT networks; [189]
- an increased urgency to pay ransom to avoid any critical business and social impact; [159]
- the ongoing rebranding of ransomware groups which increases the chances of malware blending and the development of capabilities to target and disrupt OT networks; [189]
- the Russia-Ukraine crisis as ransomware groups (e.g. Conti[198]) are taking sides and are likely to conduct retaliatory attacks against critical Western infrastructure;
- the massive increase in the number of newly identified vulnerabilities in OT environments.[159]

[183] Coveware - Ransomware attackers down shift to 'Mid-Game' hunting in Q3 2021 - https://www.coveware.com/blog/2021/10/20/ransomware-attacks-continue-as-pressure-mounts
[184] Recorded Future - Dark Covenant: Connections Between the Russian State and Criminal Actors - https://www.recordedfuture.com/russian-state-connections-criminal-actors
[185] SonicWall – 2022 Cyber Threat Report - https://www.sonicwall.com/medialibrary/en/white-paper/2022-sonicwall-cyber-threat-report.pdf
[186] Security Intelligence - Recovering Ransom Payments: Is This the End of Ransomware? - https://securityintelligence.com/articles/recovering-ransomware-payment/
[187] AP News - US recovers most of ransom paid after Colonial Pipeline hack - https://apnews.com/article/technology-business-government-and-politics-8e7f5b297012333480d5e9153f40bd52
[188] ENISA Threat Landscape 2021 - https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
[189] Dragos – 2021 ICS/OT Cybersecurity Year in Review - https://www.dragos.com/year-in-review/
[190] Intel471 - Manufacturers should focus on protecting their supply chains - https://intel471.com/blog/manufacturing-cybersecurity-threats-supply-chain
[191] MITRE ATT&CK – EKANS Software - https://attack.mitre.org/software/S0605/
[192] CISA - Rising Ransomware Threat To Operational Technology Assets - https://www.cisa.gov/sites/default/files/publications/CISA_Fact_Sheet-Rising_Ransomware_Threat_to_OT_Assets_508C.pdf
[193] NY Times - Cyberattack Forces a Shutdown of a Top U.S. Pipeline - https://www.nytimes.com/2021/05/08/us/politics/cyberattack-colonial-pipeline.html
[194] NCSC-UK – What is OT malware? - https://www.ncsc.gov.uk/blog-post/what-is-ot-malware
[195] SecurityWeek - OT Data Stolen by Ransomware Gangs Can Facilitate Cyber-Physical Attacks - https://www.securityweek.com/ot-data-stolen-ransomware-gangs-can-facilitate-cyber-physical-attacks
[196] Dragos - ICS/OT Ransomware Analysis: Q1 2022 - https://www.dragos.com/blog/industry-news/dragos-industrial-ransomware-analysis-q1-2022/
[197] Dragos - ICS/OT Ransomware Analysis: Q4 2021 - https://www.dragos.com/blog/industry-news/dragos-ics-ot-ransomware-analysis-q4-2021/
[198] CyberScoop - Conti ransomware group announces support of Russia, threatens retaliatory attacks - https://www.cyberscoop.com/conti-ransomware-russia-ukraine-critical-infrastructure/
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Organisations are recommended to plan and remediate the most common issues causing security incidents within OT environments[189]: limited OT visibility, poor network segmentation between IT and OT networks, external remote access to OT network, and shared and reused credentials.

Continuous 'retirements' and rebranding to avoid law enforcement and sanctions. As described above, the sheer volume of ransomware operations and some highly critical incidents (e.g. Colonial Pipeline[199]) resulted in increased efforts by law enforcement and governments worldwide. Thus, ransomware groups resorted to 'retiring' and rebranding, [139] [143]taking an average time of 17 months before they do so[160].

Cybercriminals behave this way potentially due to a need to:

a) reboot their operations in case their tools, TTPs or infrastructure were critically compromised (e.g. security researchers develop a decryptor);

b) avoid law enforcement, media, and political attention[200];

c) hinder and delay efforts to attribute an attack so that victims can pay the ransom to a non-sanctioned entity[201] [202];

d) resolve internal disputes[203].

During the reporting period, some ransomware families left the scene, such as Egregor, REvil, BlackMatter, and Doppelpaymer[144]. On the other hand, some of the new families that appeared had similarities to those that disappeared. Some indicative examples of the rebranding of ransomware groups include the following.

- Grief ransomware displayed similarities to DoppelPaymer[204] [139].
- WastedLocker ransom notes appeared as Hades ransomware or Cryptolocker during Spring 2021, Payloadbin during Summer 2021, and Macaw during Autumn 2021[139].
- Darkside ransomware was rebranded to DarkSide 2.0 after its decryptor was published[205] and then rebranded to BlackMatter[206] after the Colonial Pipeline incident and halted its operations. The BlackMatter gang stopped their operations in November 2021 (due to law enforcement pressure[200]), while in February 2022, the BlackCat ransomware gang confirmed that they are former members of the DarkSide or BlackMatter operation[207].
- GandCrab evolved into REvil[208].

It is our assessment that ransomware groups will continue their 'retirement' and rebranding activities. Thus, over short periods, we expect that the prevalent ransomware groups in the threat landscape will be completely different[209][159][160]. We also estimate that ransomware groups will acquire smaller tier groups, potentially resulting in the overlapping use of different ransomware variants [161].

[199] Forbes - 1 Year Later: Actions Taken, Lessons Learned Since The Colonial Pipeline Cyberattack - https://www.forbes.com/sites/edwardsegal/2022/05/07/1-year-later-actions-taken-lessons-learned-since-the-colonial-pipeline-cyberattack/
[200] TechCrunch - BlackMatter ransomware gang says it's shutting down over law enforcement pressure - https://techcrunch.com/2021/11/03/blackmatter-ransomware-shut-down/
[201] U.S. Department of the Treasury - Treasury Sanctions Evil Corp, the Russia-Based Cybercriminal Group Behind Dridex Malware - https://home.treasury.gov/news/press-releases/sm845
[202] Mandiant - To HADES and Back: UNC2165 Shifts to LOCKBIT to Evade Sanctions - https://www.mandiant.com/resources/unc2165-shifts-to-evade-sanctions
[203] ZDNet - REvil ransomware operators claim group is ending activity again, victim leak blog now offline - https://www.zdnet.com/article/revil-ransomware-operators-claim-group-is-ending-activity-again-happy-blog-now-offline/
[204] Bleeping Computer - DoppelPaymer ransomware gang rebrands as the Grief group - https://www.bleepingcomputer.com/news/security/doppelpaymer-ransomware-gang-rebrands-as-the-grief-group/
[205] Bitdefender - Darkside Ransomware Decryption Tool - https://www.bitdefender.com/blog/labs/darkside-ransomware-decryption-tool/
[206] CISA - BlackMatter Ransomware - https://www.cisa.gov/uscert/ncas/alerts/aa21-291a
[207] Bleeping Computer - BlackCat (ALPHV) ransomware linked to BlackMatter, DarkSide gangs - https://www.bleepingcomputer.com/news/security/blackcat-alphv-ransomware-linked-to-blackmatter-darkside-gangs/
[208] CrowdStrike - The Evolution of PINCHY SPIDER from GandCrab to REvil - https://www.crowdstrike.com/blog/the-evolution-of-revil-ransomware-and-pinchy-spider/
[209] Intel471 - A reset on ransomware: Dominant variants differ from prior years - https://intel471.com/blog/ransomware-attacks-2021-lockbit-hive-conti-clop-revil-blackmatter

Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Russia Ukraine conflict impacted the cybercrime ecosystem. During the Ukraine-Russia conflict, it was observed how a major geopolitical incident could mobilise cybercrime groups, reveal connections between cybercrime and state actors, and provide opportunities for cybercriminals to make financial gains.

According to public reports, several cybercrime groups expressed their support for Russia during the Russia-Ukraine conflict[210]. They threatened to target Western organisations in retaliation for providing support to Ukraine as well as for the sanctions imposed on Russia[211]. Some of these groups directly threatened the critical infrastructure of Russia's enemies[212] [196]. A very interesting data point is the increase in ransomware detections in Russia, especially since Russia and the Commonwealth of Independent States (CIS) were not traditionally targeted by ransomware operations[214]. Finally, the 'Conti leaks' (a leak of the group's internal chats dubbed the Panama Papers of ransomware[213]) were interesting because they revealed connections between the Russian Federal Security Service (FSB) and the Conti ransomware group[214]. Finally, right after the Russian invasion, cybercriminals identified money-making opportunities by trying to socially engineer people trying to support Ukraine via fake charities and fundraisers[214].

While cybercrime, specifically ransomware, is becoming a heated geopolitical issue, we expect the West to continue trying to limit safe havens for cyber criminals [181]. Other countries (e.g. Russia) will be leveraging the cybercrime underground for diplomatic advantage and as proxy actors achieving their strategic objectives[215] [216] (state-ignored and state-encouraged activity regarding state responsibility[217] [218]). We estimate that the association between cybercrime groups and state actors will certainly continue for the foreseeable future with a strong focus on plausible deniability[219]. In the short-term future, we expect several ransomware incidents in the critical infrastructure to cause concerns and grasp media attention as potential cyberwar and retaliatory actions[220].

The sanctions imposed on Russia and the limited financial transactions between the West and Russia will likely incentivise cybercriminals to cash out through payment cards[221] that have already been compromised and cryptocurrencies[222]. Finally, we expect cybercriminals to continue targeting entities in Ukraine (and Russia) as the demand from various actors increases for access credentials, personally identifiable information (PII), or intellectual property[215].

Cybercriminals love CVEs[223]. In 2021, there were 66 disclosures of zero-day vulnerabilities observed[224]. Moreover, the number of disclosed vulnerabilities is growing yearly (implying a similar increase in discovered vulnerabilities), reaching a record high in 2021[160], together with the growing number of proof-of-concept exploits. Cybercriminals jump on the disclosure of vulnerabilities to find additional weaknesses, weaponize them, and exploit them in the wild.

During the reporting period, the exploitation of vulnerabilities was reportedly the most common cause of security incidents[31], which increased by 33% compared to 2020[160]. The most widely exploited vulnerabilities by cybercriminals

[210] CISA - Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure - https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
[211] Bloomberg - Russian Isolation Spells Trouble for Global Cybersecurity - https://www.bloomberg.com/news/newsletters/2022-03-16/russian-isolation-spells-trouble-for-global-cybersecurity
[212] CSO Online - Conti gang says it's ready to hit critical infrastructure in support of Russian government - https://www.csoonline.com/article/3651498/conti-gang-says-its-ready-to-hit-critical-infrastructure-in-support-of-russian-government.html
[213] Trellix – ATR Report April 2022 - https://www.trellix.com/en-us/threat-center/threat-reports/apr-2022.html
[214] ESET – Threat Report T1 2022 - https://www.welivesecurity.com/2022/06/02/eset-threat-report-t12022/
[215] Intel471 - How the Russia-Ukraine conflict is impacting cybercrime - https://intel471.com/blog/russia-ukraine-conflict-cybercrime-underground
[216] QuoIntelligence - Unexpected changes to the Global Threat Landscape from the Ukraine War - https://quointelligence.eu/2022/06/consequences-ukraine-war-on-global-threat-landscape/
[217] Atlantic Council - Beyond Attribution: Seeking National Responsibility in Cyberspace - https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/beyond-attribution-seeking-national-responsibility-in-cyberspace/
[218] QuoIntelligence - Unexpected changes to the Global Threat Landscape from the Ukraine War - https://quointelligence.eu/2022/06/consequences-ukraine-war-on-global-threat-landscape/
[219] Recorded Future - Dark Covenant: Connections Between the Russian State and Criminal Actors - https://www.recordedfuture.com/russian-state-connections-criminal-actors
[220] CERT-EU - Threat Landscape Report 2022 Q1 - Executive Summary - https://media.cert.europa.eu/static/MEMO/2022/TLP-WHITE-2022Q1-Threat_Landscape_Report-Executive-Summary-v1.0.pdf
[221] Recorded Future - Russian Invasion of Ukraine and Sanctions Portend Rise in Card Fraud - https://www.recordedfuture.com/russian-invasion-of-ukraine-and-sanctions-portend-rise-in-card-fraud
[222] FinCEN - FinCEN Provides Financial Institutions with Red Flags on Potential Russian Sanctions Evasion Attempts - https://www.fincen.gov/news/news-releases/fincen-provides-financial-institutions-red-flags-potential-russian-sanctions
[223] Intel471 - Three ways ransomware-as-a-service has become easier than ever to launch - https://intel471.com/blog/ransomware-as-a-service-fivehands-printnightmare-babuk-conti
[224] Trend Micro – Security Predictions for 2022 - https://www.trendmicro.com/vinfo/us/security/research-and-analysis/predictions/2022
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

include ProxyLogon, ProxyShell, PrintNightmare, and Log4Shell [144].[160] ProxyLogon and Log4Shell vulnerabilities have been exploited by cybercriminals (and nation-backed groups) in such a widespread and opportunistic targeting that national security concerns were raised[139]. Finally, high volumes of buying and selling were observed within the underground market for exploits that enable cybercriminals to obtain unauthorised access to corporate networks[143].

In our assessment cybercriminals will certainly weaponize and exploit newly discovered vulnerabilities in a timely way for the foreseeable future. We expect the exploitation of administration tools, Microsoft services[225], and continued Log4j targeting throughout 2022[166]. The evolution of the perimeter will also provide cybercriminals with opportunities to target IoT devices[159], VPN, and cloud infrastructure[226].

Organisations are recommended to enhance their processes around monitoring the exploitation of vulnerabilities (for newly discovered vulnerabilities of the tech stack that are exploited in the wild) and security patching (for legacy vulnerabilities). Cyber security teams should focus on raising capacities and capabilities in people, technology and processes for their risk-based vulnerability management programmes.

Data exfiltration and extortion without the use of ransomware. Last year in the ENISA Threat Landscape 2021 report, we highlighted the trend of multiple extortion methods by ransomware groups [188](aka multi-faceted extortion or triple extortion). While this approach remained the standard [144] during the reporting period, increased data theft was observed and extortion without any data encryption taking place [143] [154] [227]. Cybercriminals realised they could request ransoms without the deployment of ransomware and thus create dedicated marketplaces[228] where they advertise and sell stolen data. We have also observed that ransomware gangs cited victims' cyber insurance policies during the negotiation phase[229]. Prominent groups that conduct such activities are LAPSUS$ (also known as DEV-0537)[230] and Karakurt[231].

In our opinion, this trend will continue to rise for the foreseeable future as this approach is lucrative for cybercriminals while their operations can be quicker and at scale[142] [232]. We also estimate that it is likely that cybercriminals will try to recruit insiders within victim organisations to exfiltrate data or deploy malware[159].

The focus on data theft and the subsequent public shaming and extortion highlights the increased privacy, regulatory, and reputational risks for victim organisations. Organisations must realise that focusing on backup strategies is essential but not enough and that the relevant detection and prevention security controls for the MITRE ATT&CK Exfiltration Tactic (TA0010[233]) should also be prioritised.

The cybercrime ecosystem is still thriving and further evolving. One of the cybercrime trends we reported last year in ETL 2021 was the increased collaboration and professionalisation of the cybercrime ecosystem. During the reporting period, it was observed that this trend was still valid and had evolved further[141].

It seems that intrusions are a 'mix and match' as different affiliates are involved in different phases of the intrusion [144]. Nowadays, one can find in the cybercrime ecosystem a supply chain offering many SaaS variants that set the entry bar relatively low for cybercriminals to conduct such attacks. For example, stolen credentials and phishing kits are cheap, DDoS attacks are affordable for unprotected sites, and ransomware kits enable low-skilled cybercriminals to

[225] Sophos – 2022 Threat Report - https://www.sophos.com/en-us/labs/security-threat-report
[226] Tenable – 2021 Threat Landscape Retrospective - https://www.tenable.com/cyber-exposure/2021-threat-landscape-retrospective
[227] Microsoft - Ransomware-as-a-service: Understanding the cybercrime gig economy and how to protect yourself - https://www.microsoft.com/security/blog/2022/05/09/ransomware-as-a-service-understanding-the-cybercrime-gig-economy-and-how-to-protect-yourself/
[228] Bleeping Computer - New Industrial Spy stolen data market promoted through cracks, adware - https://www.bleepingcomputer.com/news/security/new-industrial-spy-stolen-data-market-promoted-through-cracks-adware/
[229] The Record - Ransomware group demands £500,000 from British schools, citing cyber insurance policy - https://therecord.media/ransomware-group-demands-500000-from-british-schools-citing-cyber-insurance-policy/
[230] Microsoft - DEV-0537 criminal actor targeting organisations for data exfiltration and destruction - https://www.microsoft.com/security/blog/2022/03/22/dev-0537-criminal-actor-targeting-organizations-for-data-exfiltration-and-destruction/
[231] CISA - Karakurt Data Extortion Group - https://www.cisa.gov/uscert/ncas/alerts/aa22-152a
[232] The Register Security - We're now truly in the era of ransomware as pure extortion without the encryption - https://www.theregister.com/2022/06/25/ransomware_gangs_extortion_feature/
[233] MITRE ATT&CK – Exfiltration Tactic - https://attack.mitre.org/tactics/TA0010/
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

conduct sophisticated attacks[234] (very low barriers to entry for participating in the ransomware industry[183]). According to public reports, the number of sites offering such services increased during the reporting period[234].

Affiliate programmes are the vehicles that primarily drive the growth of the cybercrime ecosystem[140]. At the same time, ransomware schemes strengthen their relationships with surrounding entities (e.g. other ransomware groups[235] [150]) and, more specifically, with Access-as-a-Service (AaaS) brokers[181] [139] [143] [236] [237] [238]. Moreover, due to the Conti leaks, we also learned that ransomware groups are set up as if they were legitimate businesses[239] while their development teams mirror legitimate technology firms[240]. We also observed increasing disputes between ransomware affiliates and ransomware group operators[143]. Finally, we saw that (at least) one ransomware gang has launched its own Bug Bounty programme[241].

Our assessment is that the cybercrime ecosystem will continue to evolve and adapt to the cybersecurity ecosystem because of law enforcement efforts[161]. Cybercriminals are expected to use outsourced services and resort to custom and advanced tools mostly in complex targeted attacks[140]. We also expect cybercriminals to increase automation, taking advantage of the services offered in the cybercrime ecosystem to decrease costs and increase their pace and scale[234].

The outsourcing of services will further blur the lines between cybercrime and state-sponsored operations[159]. We are also certain that the use of AaaS brokers will grow in the foreseeable future, while it is expected that AaaS brokers will increasingly target the supply chain. Finally, since many actors are involved in different phases of the attacks and are paid a percentage of the ransom, the chances are even that we will observe conflicts among these actors primarily due to disruptions to payments by law enforcement or victims who do not pay the ransom[159].

2.3 HACKER-FOR-HIRE ACTOR TRENDS

The Access-as-a-Service market continues to enable state actors. The hacker-for-hire threat actor category refers to entities within the 'Access-as-a-Service' (AaaS) market, mainly comprised of companies that offer offensive cyber capabilities. Their clients are usually governments (but also corporations and individuals), and the service categories they offer are usually bundled as a single service[242]: Vulnerability Research and Exploitation, Malware Payload Development, Technical Command and Control, Operational Management, and Training and Support. The CTI community maintains a crowdsourced (and ever-growing) list of publicly known private companies mostly involved in nation-state offensive cyber operations[243].

On 23 May 2022, Interpol's Secretary-General stated that he is *concerned that state-developed cyberweapons will become available on the darknet in a couple of years*[244]. This was almost done by the Shadow Brokers back in 2016 when they were selling alleged NSA tools for cryptocurrency[245]. Within the darknet and underground marketplaces, it is relatively easy for threat actors with the interest and the budget to buy advanced cyber tools and increase their cyber capabilities [47]. In ETL 2021, we highlighted the trend of the rising number of hacker-for-hire threat actors and their services; this trend remained valid throughout the reporting period[47].

During the reporting period, some of the significant developments include the following.

[234] Microsoft – Digital Defence Report - https://www.microsoft.com/en-us/security/business/microsoft-digital-defense-report
[235] Intel471 - Cybercrime loves company: Conti cooperated with other ransomware gangs - https://intel471.com/blog/conti-ransomware-cooperation-maze-lockbit-ragnar-locker
[236] Intel471 - Conti and Emotet: A constantly destructive duo - https://intel471.com/blog/conti-emotet-ransomware-conti-leaks
[237] Intel471 - The relationship between access brokers and ransomware crews is growing - https://intel471.com/blog/access-brokers-ransomware-relationship-growing
[238] Sophos - The Active Adversary Playbook 2022 - https://news.sophos.com/en-us/2022/06/07/active-adversary-playbook-2022/
[239] Intel471 - Conti puts the 'organised' in organised crime - https://intel471.com/blog/conti-leaks-cybercrime-fire-team
[240] Intel471 - Move fast and commit crimes: Conti's development teams mirror corporate tech - https://intel471.com/blog/conti-leaks-ransomware-development
[241] Twitter – vx-underground - https://twitter.com/vxunderground/status/1541156954214727685
[242] Atlantic Council - Countering Cyber Proliferation – Zeroing in on Access-as-a-Service - https://www.atlanticcouncil.org/wp-content/uploads/2021/03/Offensive-Cyber-Capabilities-Proliferation-Report-1.pdf
[243] xorl %eax, %eax - Offensive Security Private Companies Inventory - https://xorl.wordpress.com/offensive-security-private-companies-inventory/
[244] CNBC - Military-made cyberweapons could soon become available on the dark web, Interpol warns - https://www.cnbc.com/2022/05/23/military-cyberweapons-could-become-available-on-dark-web-interpol.html
[245] VICE - Cryptocurrency Transactions May Uncover Sales of Shadow Broker Hacking Tools - https://www.vice.com/en/article/j5k7zp/zcash-shadow-brokers-uncover-hacking-tool-sales
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

- Threat actors continue to use private companies' tools and capabilities to conduct surveillance operations [47]. Private companies, such as the NSO Group and Candiru, have been providing (or even supplementing) the capabilities to state actors worldwide[42].
- DeathStalker[246] cyber mercenary group continued targeting law firms and financial institutions, while there are suspicions that the group started targeting travel agencies.
- Candiru [247] [234] has been using several 0-day exploits sold to governmental agencies and other actors[248]. Moreover, an interesting cyber activity linked with Candiru has been identified in the Middle East[249].
- Individual researchers, cybercriminals, and private companies have expanded the 0-day market in terms of development and trading[47]. An interesting observation is that Access-as-a-Service companies developed seven out of nine 0-days discovered by the Google Threat Analysis Group[250]. More specifically, Cytrox[251], a private surveillance company, was identified as having sold five 0-days in Google Chrome and Google Android to different state actors!
- The Access-as-a-Service companies are highly sophisticated and have developed such research and development capabilities that they can quickly retool and continue to service their clients by conducting cyber operations even after public exposure[47].
- The spyware cases of Pegasus[252] (NSO Group) and Predator[253] [254] (Cytrox) attracted huge media attention and kicked off discussions about state control, (un)lawful interception and the targeting of civil society.

Our assessment is that threat actors (mostly nation-state) will very likely continue buying such services and outsourcing cyber operations as the list of Access-as-a-Service companies grows. This outsourcing will certainly make the threat landscape more complex and will very likely contribute to increased cyber espionage and surveillance activity[159]. Thus, we need to consider the implications related to the attribution of such cyber activities, the rapid development and enablement of cyber capabilities, and the abuse of such capabilities for targeting journalists, activists and civil society [47] [270] . One noteworthy implication may be that government programs that aim for the prevention of greater harm caused by undisclosed vulnerabilities (so called vulnerability equity process) may lose their effectiveness since required vulnerability details needed for a judgement are not at the disposal of the involved entities.

The Pegasus case triggered media coverage and governmental actions. The biggest story during the reporting period was about the Israeli-based NSO Group and the Pegasus Project, where over 30,000 human rights activists, journalists, and lawyers worldwide were targeted as well as 14 world leaders[255]. While we reported on the Pegasus project in ETL 2021, there have been several developments during the reporting period.

- Israel investigated the Israeli-based NSO Group[256].
- US technology companies took legal action against the NSO Group[257] [258].

[246] LIFARS - DeathStalker: A threat group utilizing unique methods - https://www.lifars.com/2020/09/deathstalker-a-threat-group-utilizing-unique-methods/
[247] Citizen Lab - Hooking Candiru: Another Mercenary Spyware Vendor Comes into Focus - https://citizenlab.ca/2021/07/hooking-candiru-another-mercenary-spyware-vendor-comes-into-focus/
[248] Microsoft - Protecting customers from a private-sector offensive actor using 0-day exploits and DevilsTongue malware - https://www.microsoft.com/security/blog/2021/07/15/protecting-customers-from-a-private-sector-offensive-actor-using-0-day-exploits-and-devilstongue-malware/
[249] ESET - Strategic web compromises in the Middle East with a pinch of Candiru - https://www.welivesecurity.com/2021/11/16/strategic-web-compromises-middle-east-pinch-candiru/
[250] Google Threat Analysis Group - Protecting Android users from 0-Day attacks - https://blog.google/threat-analysis-group/protecting-android-users-from-0-day-attacks/
[251] Facebook - Threat Report on the Surveillance-for-Hire Industry - https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf
[252] European Parliament - Pegasus and surveillance spyware - https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf
[253] The New York Times - Senior European Parliament Member Targeted as Spyware Abuse Spreads - https://www.nytimes.com/2022/07/27/world/europe/eu-spyware-predator-pegasus.html
[254] European Parliament - E-001449/2022 Answer given by Mr Reynders on behalf of the European Commission - https://www.europarl.europa.eu/doceo/document/E-9-2022-001449-ASW_EN.pdf
[255] https://www.amnesty.org/en/latest/press-release/2021/07/world-leaders-potential-targets-of-nso-group-pegasus-spyware/
[256] MIT Technology Review - Israel begins investigation into NSO Group spyware abuse - https://www.technologyreview.com/2021/07/28/1030244/israel-investigation-nso-group-pegasus-spyware/
[257] Apple - Apple sues NSO Group to curb the abuse of state-sponsored spyware - https://www.apple.com/newsroom/2021/11/apple-sues-nso-group-to-curb-the-abuse-of-state-sponsored-spyware/
[258] Politico - NSO falters in bid to shut down suit over hacking of WhatsApp - https://www.politico.com/news/2021/04/12/nso-falters-lawsuit-whatsapp-hacking-481073

Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

- The Supreme Court in India examined the impact of the use of Pegasus spyware on Indian citizens[259].
- US State Department phones have been hacked with Pegasus[260].
- A high number of cases related to NSO's Pegasus spyware were reported in Europe[220]. For example, Spain's politicians and Catalan independence leaders have been targeted[261] [262].
- The NSO Group mentioned that five EU states use Pegasus spyware[263].

The US Department of Commerce declared that the Israeli-based Candiru and NSO Group, the Russian-based Positive Technologies, and the Singapore-based Computer Security Initiative Consultancy have been enabling or facilitating cyber activities contrary to the national security or foreign policy interests of the United States[264] [265]. Thus, the US administration applied export controls to hold these companies accountable for their cyber activity and the technologies they develop.

On 10 March 2022[266], the European Parliament set up the PEGA Committee to investigate alleged infringement or maladministration in the application of EU law in relation to the use of Pegasus and equivalent spyware surveillance software[267] [268].

The above governmental actions are aligned with what we assessed in ETL 2021 would happen (i.e. increasing state control or oversight) based on the impact of investigations related to the Pegasus Project and other commercial spyware surveillance software.

Surveillance and targeting of civil society. On the one hand, it was observed that commercial threat intelligence reporting neglects cyber threats to civil society[269]. On the other hand, the tools of the Access-as-a-Service companies are increasingly targeting dissidents, human rights activists, journalists, civil society advocates, and other private citizens [234] [270]. While the usage of spyware surveillance technologies may be legal under national or international laws, it was observed that governments often abuse these technologies for purposes not aligned with democratic values[271].

On 19 July 2021, the European Commission President Ursula von der Leyen mentioned that using spyware on journalists is unacceptable[272]. Within the EU, high-profile cases have been reported in which the Pegasus [252] [273] [274] and the Predator[275] spyware software have been used to target journalists.

[259] The Guardian - Indian supreme court orders inquiry into state's use of Pegasus spyware - https://www.theguardian.com/news/2021/oct/27/indian-supreme-court-orders-inquiry-into-states-use-of-pegasus-spyware
[260] Reuters - U.S. State Department phones hacked with Israeli company spyware - sources - https://www.reuters.com/technology/exclusive-us-state-department-phones-hacked-with-israeli-company-spyware-sources-2021-12-03/
[261] The Guardian - Use of Pegasus spyware on Spain's politicians causing 'crisis of democracy' - https://www.theguardian.com/world/2022/may/15/use-of-pegasus-spyware-on-spains-politicians-causing-crisis-of-democracy
[262] I24 News - Spain to reform secret services after NSO spying scandal - https://www.i24news.tv/en/news/international/europe/1653559492-spain-to-reform-secret-services-after-nso-spying-scandal
[263] The Register - NSO claims 'more than 5' EU states use Pegasus spyware - https://www.theregister.com/2022/06/24/nso_customers_eu_pegasus/
[264] U. S. Department of Commerce - Commerce Adds NSO Group and Other Foreign Companies to Entity List for Malicious Cyber Activities - https://www.commerce.gov/news/press-releases/2021/11/commerce-adds-nso-group-and-other-foreign-companies-entity-list
[265] Axios - Scoop: Israelis push U.S. to remove NSO from blacklist - https://www.axios.com/2022/06/08/nso-pegasus-israel-us-commerce-blacklist
[266] As of the time of writing, the inquiry is still ongoing.
[267] European Parliament -About PEGA Committee - https://www.europarl.europa.eu/committees/en/pega/about
[268] https://www.europarl.europa.eu/RegData/etudes/IDAN/2022/732268/IPOL_IDA(2022)732268_EN.pdf
[269] Lennart Maschmeyer,Ronald J. Deibert &Jon R. Lindsay - A tale of two cybers - how threat reporting by cybersecurity firms systematically underrepresents threats to civil society - https://www.tandfonline.com/doi/full/10.1080/19331681.2020.1776658
[270] Meta - Threat Report on the Surveillance-for-Hire Industry - https://about.fb.com/wp-content/uploads/2021/12/Threat-Report-on-the-Surveillance-for-Hire-Industry.pdf
[271] Google Threat Analysis Group - Spyware vendor targets users in Italy and Kazakhstan - https://blog.google/threat-analysis-group/italian-spyware-vendor-targets-users-in-italy-and-kazakhstan/
[272] Reuters - EU says use of spyware on journalists is unacceptable - https://www.reuters.com/world/europe/using-spyware-against-journalists-completely-unacceptable-eus-von-der-leyen-2021-07-19/
[273] The Guardian - Pegasus spyware found on journalists' phones, French intelligence confirms - https://www.theguardian.com/news/2021/aug/02/pegasus-spyware-found-on-journalists-phones-french-intelligence-confirms
[274] The Guardian - Hungarian journalists targeted with Pegasus spyware to sue state - https://www.theguardian.com/world/2022/jan/28/hungarian-journalists-targeted-with-pegasus-spyware-to-sue-state
[275] Euractiv - Greek intelligence service admits spying on journalist - https://www.euractiv.com/section/media/news/greek-intelligence-service-admits-spying-on-journalist/
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Big tech companies work towards protecting their customers[276][277] and defend against spyware activities regardless of who is behind these attacks or who the targets might be[270]. Moreover, big tech companies have shared their findings with security researchers and policy makers[270]. Conversely, the means of investigating mobile phone compromises for defenders are still limited and need to be further improved.

2.4 HACKTIVISTS' TRENDS

A new wave of hacktivism[278]. In ETL 2021, we highlighted the trend that hacktivist operations remain low in numbers, sophistication and impact. However, during the reporting period and especially since the Russia-Ukraine crisis began, we have observed a significant increase in hacktivist activity[279] (as was shown in the introduction).

The Ukraine-Russia conflict has been seen as an increasingly permissive (and unique) environment that mobilised hacktivist groups that chose sides[279] (around 70 hacktivist groups became involved[280]). We have observed a significant number of hacktivist groups targeting organisations (even within the critical infrastructure sectors) primarily through DDoS attacks, defacements and data leaks. Moreover, a pretty interesting point was the coordination of the cyber operations of the hacktivist groups, primarily via Telegram groups that one could easily join, participate in, and even download the tools provided to conduct cyber-attacks (e.g. DDoS).

Some of the major Hacktivist groups were: Anonymous[281], TeamOneFirst, IT Army of Ukraine (some researchers regard this group as a hybrid one since its structure contains state actor and hacktivist components[122]), GhostSec[282], Against the West[283] (ATW also announced a 0-day on Nginx[284]), NB65[285], and Belarusian Cyber Partisans[286]. On the other hand, some other hacktivist groups have targeted Ukrainian and western organisations. Some of those hacktivist groups were: the Cyber Army of Russia, KILLNET[287] [288], XakNet [288][289], and The Red Bandits.

Some of the above groups demonstrated a high level of sophistication in cyber operations[279]. Our assessment is that the operational tempo and the cyber activity from hacktivist groups will very likely remain high as the conflict between Russia and Ukraine continues. An interesting question to be answered is whether this increased hacktivism activity will continue after the Ukraine-Russia conflict winds down or if hacktivism activity will revert to its previous low levels. An additional yet equally interesting question involves the possible infiltration of hacktivist groups by state actors[290][291], similarly as is the case with ransomware groups.

From a strategic perspective, the Russia-Ukraine crisis has defined a new era for hacktivism, its role, and its impact on conflicts. In future conflicts, states will very likely adapt their cyber warfare operations and take advantage of this new 'hacktivism blueprint'[292]. However, this 'blueprint' has implications for international norms in cyberspace and, more specifically, for state sponsorship of cyberattacks and against targeting critical civilian infrastructure[293].

[276] https://nex.sx/blog/2022/07/09/a-look-at-apple-lockdown-mode.html
[277] Google - Google's efforts to identify and counter spyware - https://blog.google/threat-analysis-group/googles-efforts-to-identify-and-counter-spyware/
[278] Republic of Estonia – Information System Authority - Trends and Challenges in Cyber Security – Q1 2022 - https://www.ria.ee/en/news/trends-and-challenges-cyber-security-q1-2022.html
[279] SecAlliance - The Changing Landscape of Hacktivism - https://www.secalliance.com/blog/the-changing-landscape-of-hacktivism
[280] Cyberknow - Update 15. 2022 Russia-Ukraine war — Cyber group tracker. June 13. - https://cyberknow.medium.com/update-15-2022-russia-ukraine-war-cyber-group-tracker-june-13-35289e4bfdb7
[281] BBC - Anonymous: How hackers are trying to undermine Putin - https://www.bbc.com/news/technology-60784526
[282] Twitter – Ghost Security Group - https://twitter.com/ghostsecgroup?lang=en
[283] Cyberint - BlueHornet – One APT to Terrorize Them All - https://cyberint.com/blog/research/bluehornet-one-apt-to-terrorize-them-all/
[284] The Record - F5 investigating reports of NGINX zero day - https://therecord.media/f5-investigating-reports-of-nginx-zero-day/
[285] Twitter – NB65 - https://mobile.twitter.com/xxnb65
[286] Twitter - Belarusian Cyber-Partisans - https://twitter.com/cpartisans?lang=en
[287] Digital Shadows - Killnet: The Hactivist Group That Started A Global Cyber War - https://www.digitalshadows.com/blog-and-research/killnet-the-hactivist-group-that-started-a-global-cyber-war/
[288] CISA - Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure - https://www.cisa.gov/uscert/ncas/alerts/aa22-110a
[289] Twitter – XakNet team - https://twitter.com/XaknetTeam
[290] https://www.mandiant.com/resources/blog/apt28-a-window-into-russias-cyber-espionage-operations
[291] https://www.sentinelone.com/labs/hacktivism-and-state-sponsored-knock-offs-attributing-deceptive-hack-and-leak-operations/
[292] SecAlliance - The Changing Landscape of Hacktivism - https://www.secalliance.com/blog/the-changing-landscape-of-hacktivism
[293] Council on Foreign Relations - Cyber Proxies in the Ukraine Conflict: Implications for International Norms - https://www.cfr.org/blog/cyber-proxies-ukraine-conflict-implications-international-norms
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Hacktivist Ransomware: the new kid on the block. During the reporting period, a hacktivist collective (a regional resistance organization) called Cyber Partisans conducted several notable cyber operations. Cyber Partisans have conducted hack-and-leak operations[294] and conducted the first-ever ransomware attack of the type. In July 2021, they hacked the Belarusian Ministry of Internal Affairs and the exfiltrated data were shared with journalists (the hack-and-leak operation). The most interesting case, though, was the targeting of railway supply lines on 24 January 2022 to slow down the movement of Russian troops[295]. To achieve this, the group deployed modified ransomware to bring down the railway system and encrypted servers, databases and workstations belonging to the Belarusian railway service[296].

A hacktivist group, NB65, conducted ransomware attacks using Conti's leaked ransomware against Russian companies[297]. NB65 stated that they would not target organisations outside Russia and that the ransom payments would be donated to Ukraine[298]. Furthermore, another hacktivist group, Red Bandits, mentioned in their tweets that they might consider distributing ransomware[299].

Our assessment is that threat actors will increasingly conduct ransomware attacks with no monetary motivations. Hacktivists will likely be attracted by the effectiveness and the impact that ransomware attacks can have as well as the media attention they attract. The scale and sophistication of hacktivists' ransomware operations are not expected to be as high as the ones conducted by cybercriminals. Finally, governmental organisations are very likely the primary targets of hacktivists' ransomware operations.

[294] CERT-EU - Threat Landscape Report 2021 Q3 - Executive Summary - https://media.cert.europa.eu/static/MEMO/2021/TLP-WHITE-2021Q3-Threat_Landscape_Report-Executive-Summary-v1.0.pdf
[295] Twitter – Belarusian Cyber-Partisans - https://twitter.com/cpartisans/status/1485615555017117700
[296] Ransomware.org - A New Front: Hacktivist Ransomware - https://ransomware.org/blog/a-new-front-hacktivist-ransomware/
[297] Bleeping Computer - Hackers use Conti's leaked ransomware to attack Russian companies - https://www.bleepingcomputer.com/news/security/hackers-use-contis-leaked-ransomware-to-attack-russian-companies/
[298] Twitter – NB65 - https://twitter.com/xxNB65/status/1513593777759428624
[299] Twitter – Red Bandits - https://web.archive.org/web/20220222171652/https://twitter.com/RedBanditsRU/status/1495986961760370689

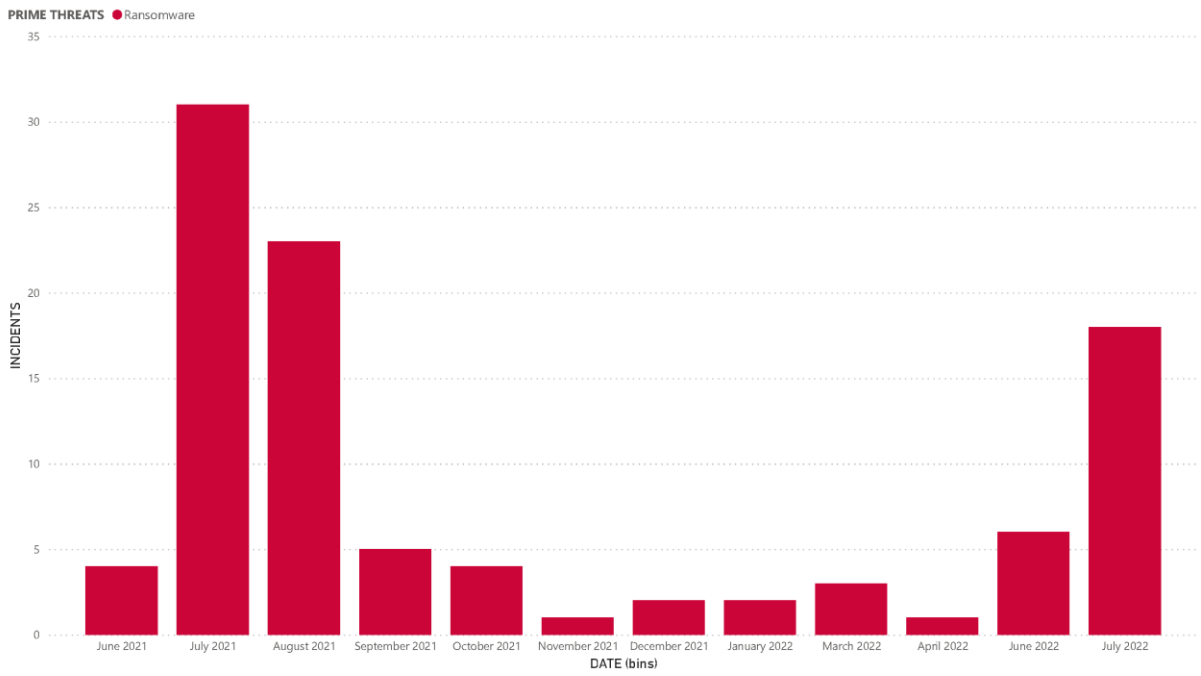
3. RANSOMWARE

In the 2022 report, ENISA's Threat Landscape for Ransomware Attacks[300], **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.* The work covers the three key elements present in every ransomware attack: assets, actions and blackmail. This action-agnostic definition was needed to cover the changing ransomware threat landscape, the prevalence of multiple extortion techniques, and the different goals other than solely financial gains. The report also covers the four high-level actions (lock, encrypt, delete and steal) used by ransomware to impact the assets' availability, confidentiality, and integrity. 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*.[301]

During this reporting period we again observed a large number of incidents concerning ransomware, proving once again that the ransomware threat is still growing. The incidents analysed are mainly focused on EU countries.

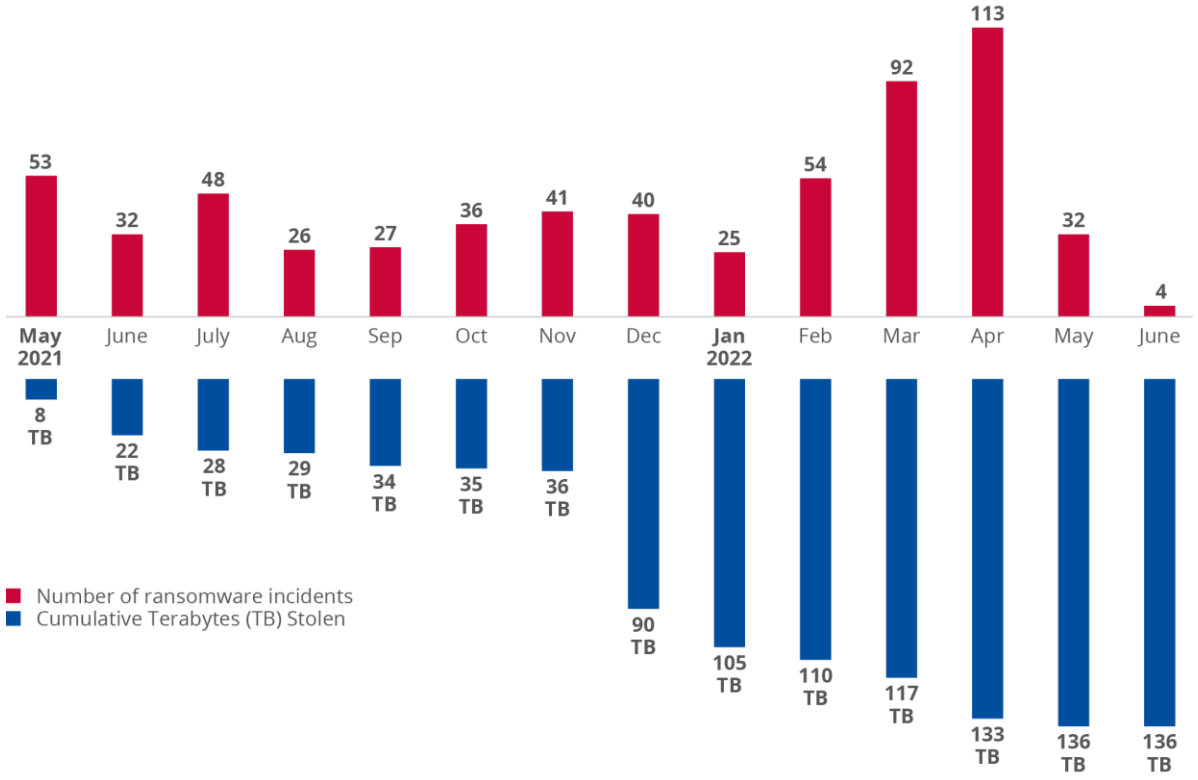
Figure 11: Time series of major incidents observed by ENISA (July 2021-June 2022)



For a more detailed analysis of the ransomware threat, ENISA published a dedicated report in Jully 2022 showcasing the analysis of 623 incidents[302].

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

Figure 12 Time series of ransomware incidents from May 2021 to June 2022. In red bars the number of ransomware incidents is shown. In blue bars the cumulative amount of stolen data is shown



3.1 TRENDS

3.1.1 Lockbit, Conti, and ALPHV lead the charts.

Research shows LockBit, Conti, and ALPHV (BlackCat) were some of the top ransomware strains used in RaaS (Ransomware as a Service) and extortion attacks in terms of victim organisations in the first quarter of 2022.[303] This data is a result of combining the leak sites of extortion groups with OSINT and infiltration operations performed by security researchers. Different statistics also confirm LockBit and Conti as the two most active ransomware gangs in Q1 2022, accounting for more than half of all ransomware incidents.[304] Over the course of Q2 2022, LockBit, Conti, and ALPHV accounted for more than half of the victims according to published statistics[305].

Note that around May 2022, as the Conti group took down its attack infrastructure, their affiliates migrated to other RaaS platforms and groupings, such as Hive, AvosLocker, and ALPHV. ALPHV emerged around the end of 2021 when the group started recruiting affiliates on hacker forums. This ransomware strain was developed in RUST and targets various versions of Linux and Windows 7 and above. The group is possibly associated with the DarkSide and BlackMatter groups, or it shares many members from these now inactive groups.[306] A report from the FBI detailing indicators of compromise also mentions that link developers and money launderers are shared between these groups.[307] The name Blackcat was initially chosen because of a cat displayed on their Tor Payment site. However, the group is officially called and referred to as ALPHV.[308]

[303] https://documents.trendmicro.com/assets/pdf/datasheet-ransomware-in-Q1-2022.pdf
[304] https://www.digitalshadows.com/blog-and-research/q1-2022-ransomware-roundup/
[305] SEKOIA Threat Intelligence FLASH Report - Mid-2022 Ransomware Overview
[306] https://www.digitalshadows.com/blog-and-research/alphv-the-first-rust-based-ransomware/
[307] https://www.ic3.gov/Media/News/2022/220420.pdf
[308] https://blog.emsisoft.com/en/40931/ransomware-profile-alphv/

Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Data from May 2022 suggest that next to ALPHV, Black Basta and Hive are also filling the gap Conti left behind[309]. Hive is a RaaS actor, active since at least June 2021, and has been confirmed responsible for a ransomware attack on Costa Rica's public health service[310]. This attack came not long after a state of national emergency was declared due to ongoing Conti ransomware attacks, impacting multiple Ministries and governmental bodies. There is at least some link between Conti and Hive, as they have leaked the same victims on both their leak sites simultaneously on multiple occasions[311].

Groups continue to disappear and (re)emerge. At the same time, their source code is often re-used or stolen, making it challenging to understand how these groups are interlinked. Researchers often make assumptions based on source code overlap or re-used wallet addresses to make sense of this changing landscape.

3.1.2 Phishing is now the most common initial vector

In line with last year's report, compromise through RDP (Remote Desktop Protocol) as an initial attack vector has continued to decline but remains the second most important vector for ransomware attacks. Threat actors brute-force weak RDP credentials, especially when MFA is not enabled. Now, phishing is the most used attack vector to gain an initial foothold in an organisation. Both these methods are cheap and thus most profitable for threat actors[312].

Reports mention rises in other categories, such as social engineering through other means besides mail and the direct compromising of insiders. Phishing attacks are carried out in high volume and target a broad audience, while other social engineering attacks make use of custom campaigns tailored to target specific employees. Using social engineering, threat actors leverage an employees' access inside an organisation to gain a technical foothold in the network from which they carry out further attacks. RDP is a popular compromise method as the threat actors use legitimate credentials, allowing them to remain unnoticed. However, brute-forcing RDP credentials is a noisy activity, and organisations with more mature security will monitor for these attempts at authentication. When the access of a compromised insider is used, it becomes more difficult for organisations to detect malicious activity in time[312].

A survey conducted at the end of 2021 and repeated this year reports that over half of respondents say they or their employees have been approached to assist in aiding ransomware attacks[313]. The rise in these statistics confirms that insider threat as an initial compromise is on the rise.

3.1.3 Extorsion techniques evolve further

Classic ransomware operations would collect information before engaging in additional actions such as extorsion with or without encrypting the files. If the company refuses to pay, the leak is made public and/or the data is made public on so-called leak sites. These leak sites group all victims of a particular RaaS threat actor and are often only available through Tor.

In June 2022, ALPHV started creating a dedicated leak site for individual victims hosted over the public internet. They leaked customer and employee information and data packs for individual employees. Using the website's functionality, employees or customers could check if they were present in the data leak[314]. The spread of information on the public internet tends to go faster, gets cached, gets indexed and therefore it could be an effective way for threat actors to leverage their victims into paying a ransom. Furthermore, it allows third-party victims whose data was leaked to investigate whether they were impacted.

We had seen and reported last year third-party victims being contacted directly when the initial victim was breached and had refused to pay the ransom. They would then either demand ransom from the third party or leverage these impacted customers to pressurise the company. Creating a public search site has become a new way for threat

[309] https://blog.malwarebytes.com/threat-intelligence/2022/06/ransomware-may-2022-review/
[310] https://twitter.com/CCSSdeCostaRica/status/1531628187846844418
[311] https://www.advintel.io/post/hydra-with-three-heads-blackbyte-the-future-of-ransomware-subsidiary-groups
[312] https://www.coveware.com/blog/2022/5/3/ransomware-threat-actors-pivot-from-big-game-to-big-shame-hunting#vectors
[313] https://www.hitachi-id.com/hubfs/A.%20Key%20Topic%20Collateral/Ransomware/%5BInfographic%5D%20The%20Rising%20Insider%20Threat%20%7C%20Hackers%20Have%20Approached%2065%25%20of%20Executives%20or%20Their%20Employees%20To%20Assist%20in%20Ransomware%20Attacks.pdf
[314] https://www.bleepingcomputer.com/news/security/ransomware-gang-creates-site-for-employees-to-search-for-their-stolen-data/
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

actors to get third-party victims to identify themselves quickly. If these affected customers contact the RaaS actor themselves, this can cause a shift-left approach[315] and limit the effort invested by the threat actor.

Industrial Spy, a dark web marketplace, launched around April 2022. The group had previously focused on data theft but, since May 2022, it has also been undertaking ransomware operations[316]. The group's initial victims only received a notice pointing to their leak site but the data itself was not encrypted. The victim was encouraged to 'buy' its data before a competitor would buy it first. This threat actor actively defaced its victims' websites to display the ransom notes[317]. This is a changing tactic, as during the initial phase of a classic ransomware infection, during a limited time window, the attack would not be made public in order to conduct negotiations and convince the company to pay the ransom. It's often only when a company refuses to pay or to cooperate that it ends up on a leak site. This increase in public shaming has a direct impact on the company's public relations and reputation.

Another new trend is a victim's data being published on leak sites without mentioning the company's name. This was the case with Midas, Lorenz, Cheerscrypt, and Everest, all smaller RaaS groups. This approach puts pressure on the victims to pay a ransom before their names are made public, but it also buys these companies some time to plan.

Novelli, a very active initial access broker (IAB), sells network access to RaaS groups and focuses on selling RDP credentials[318]. IABs play an important role in the ransomware threat landscape, as RaaS groups actively buy access. It is a way for ransomware threat actors to remain active on forums where the promotion of ransomware activities or affiliate programs has become forbidden[319].

3.1.4 Unique organisational insights from leaks

In February 2022, preceding the apparent public retirement of the Conti RaaS group, their internal chat logs were leaked, giving some unique insights into the internal organisation of the group, how it operates as a business and how the group is structured. Like a business, the group was comprised of middle management, HR managers, different technical teams with specialized capabilities, and benefits for the employees. The group worked mainly during the week, and the employees enjoyed benefits such as paid leave[320].

The logs were mainly in the Russian language, and next to chat logs, other types of files were leaked, such as documentation, internal software, screenshots, etc. One quick start guide describes general recommendations to attack and gain persistence on their victims' network. It gives a unique insight into how the organisation approaches attacks on its victims from a technical perspective. IoT devices are described as an essential initial attack surface. Next, remote access service technologies like RDP and VPN (Virtual Private Networks) are recommended as an initial backdoor. Finally, the group also documents how the AD (active directory) is often the initial target to gain a persistent presence in the organisation's network[321].

3.1.5 Rapid weaponisation of vulnerabilities

The average time to exploit is within eight days of a vendor's publication of the vulnerability. This trend highlights the importance of proper patch management and a threat-informed approach to the risk management of vulnerabilities[322].

For more information regarding the CVEs that were discovered and used during this reporting period check ANNEX C

3.1.6 The impact of law enforcement on the global scale.

In January 2022, eight members of the REvil ransomware group were arrested in Russia by the Federal Security Service (FSB)[323]. It was the second most active group in 2021, and it was most known for its attack on Colonial

[315] https://en.wikipedia.org/wiki/Shift-left_testing
[316] https://securityaffairs.co/wordpress/131754/cyber-crime/industrial-spy-cuba-ransomware.html
[317] https://twitter.com/malwrhunterteam/status/1532325586508587008
[318] KELA Cybercrime Intelligence - Ransomware victims and network access sales in Q1 2022
[319] https://www.digitalshadows.com/blog-and-research/colonial-pipeline-attack-update-cybercriminal-forum-xss-bans-all-things-ransomware/
[320] www.digitalshadows.com/blog-and-research/five-things-we-learned-from-the-Conti-chat-logs/
[321] Forescout- Vedere Labs - Analysis of Conti Leaks – March 2022
[322] https://blog.malwarebytes.com/business/2022/07/ransomware-rolled-through-business-defenses-in-q2-2022/
[323] http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10439388%40fsbMessage.html
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Pipeline and the supply chain attack on Kaseya, a tool used by global MSPs. It is believed that the people arrested were only small fish in the global REvil organisation.

Indeed, analysis of samples dating from March and April 2022 indicates the source code is being actively developed. Therefore, it is possible that the REvil group is still active in some way or that another threat actor group is further developing its code[324]. Notable differences are the removal of code verifying the ransomware is not executing within a prohibited region, and updates of the hard-coded public keys. This last element can indicate that the actors either lost the original keys or did not have access to them in the first place.

However, due to the current geopolitical situation, it is unlikely that the trial will result in a penal sentence. Indeed, reports emerged about the case falling apart due to a supposed lack of evidence and information-sharing between national law enforcement agencies[325].

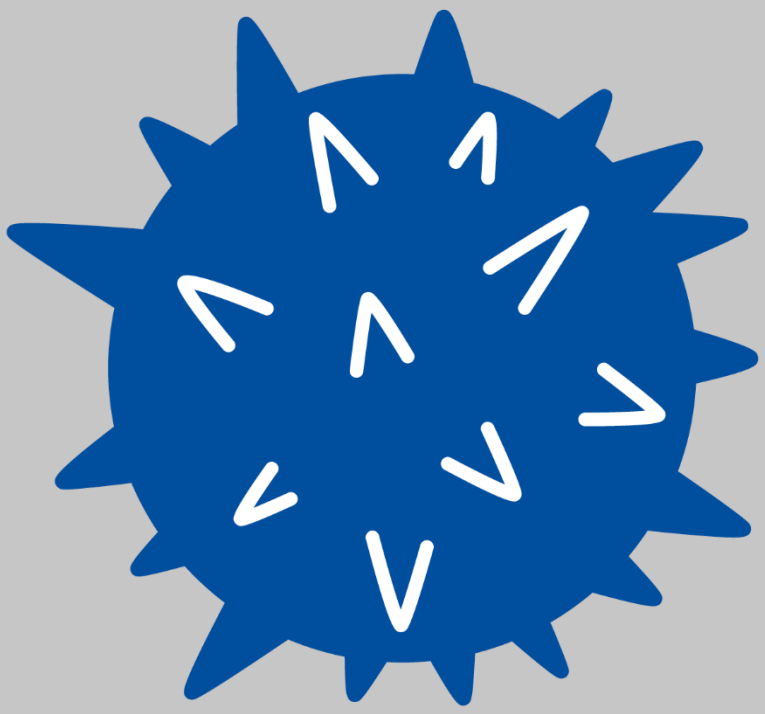
A Canadian national, active as an affiliate for the NetWalker ransomware group, was sentenced in February 2022 to seven years in prison[326]. The arrest took place in 2021 when Netwalker was still a very active ransomware group.

In 2021, we saw a lot of action from law enforcement against ransomware actors. This year, the number of publicly disclosed actions by law enforcement against ransomware threat actors was greatly reduced.

3.1.7 Payment prohibition

While the debate regarding legislation to forbid ransomware payments has long been ongoing over 2021, there was no change or progress until May 2022. North Carolina then announced that public entities were prohibited from paying ransoms. Since June 2022 the state of Florida has also been prohibiting agencies from paying ransom and is enforcing the need to give notice about any such incident[327]. In addition, the Cyber incident Reporting Act obliges mandatory incident reporting within 72 hours of experiencing a cyberattack and within 24 hours of making a ransomware payment[328]. It remains to be seen whether these undertakings will be effective, as RaaS groups will not limit themselves because of local legislation. Only in a more global context could these legal measures become more effective.

[324] https://www.secureworks.com/blog/revil-development-adds-confidence-about-gold-southfield-reemergence
[325] https://kommersant.ru/doc/5369361
[326] https://www.documentcloud.org/documents/21199313-sebastien-vachon-desjardins-guilty-plea-sentencing
[327] https://www.databreaches.net/florida-follows-north-carolina-in-prohibiting-state-agencies-from-paying-ransoms/
[328] https://www.peters.senate.gov/newsroom/press-releases/peters-landmark-provision-requiring-critical-infrastructure-to-report-cyber-attacks-signed-into-law-as-part-of-funding-bill-



4. MALWARE

Malware, also referred to as malicious code or malicious logic[329]**,** 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. Examples of malicious code types include viruses, worms, trojan horses or other code-based entities that infect a host. Spyware and some forms of adware are also examples of malicious code[330].

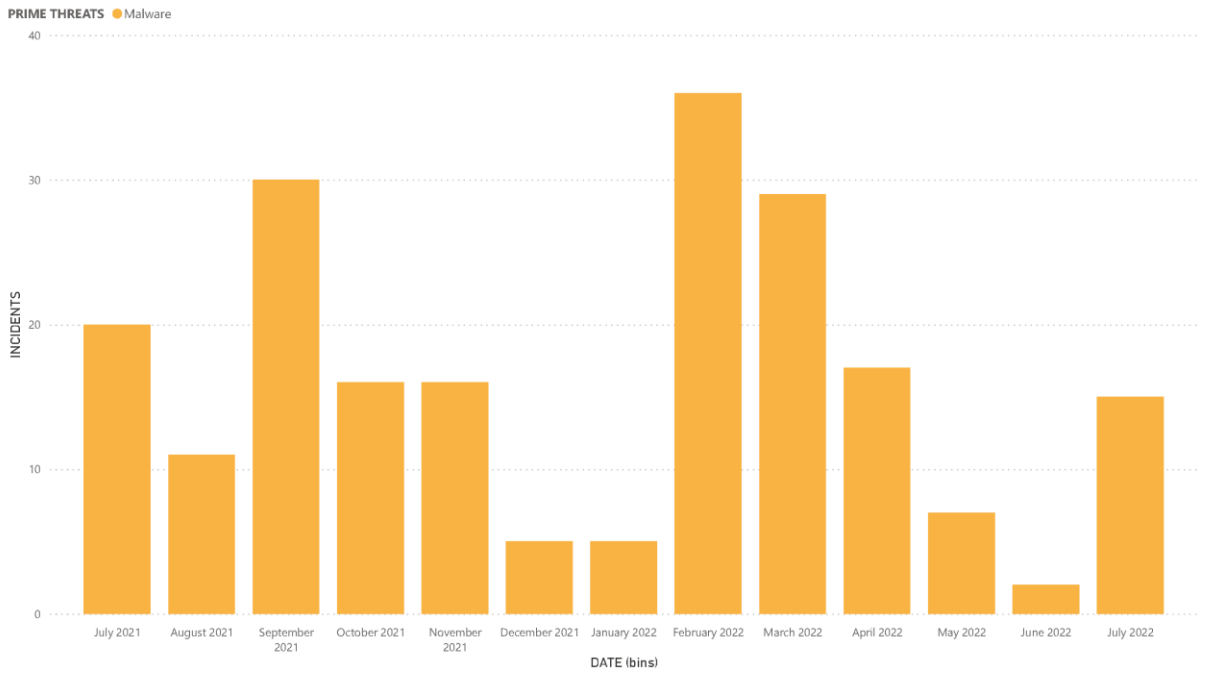
Malicious actors typically use malware throughout their campaigns. It is a fundamental capability for gaining and maintaining control of assets, evading and deceiving defences, and carrying out post-compromise actions. Viruses, worms and Trojan horses differ on many points, such as the infection vector, replication, distribution, and spread and attacker control. From a technical perspective, we can also differentiate components with different types of capability, such as payloads, droppers, post-compromise tools, backdoors and packers[331]. The malware components used in an attack depend on the goal of the threat actor. This can range from getting control over systems and networks (initial access brokers, botnets) or over data (ransomware threat actors, information stealing) to making them unavailable altogether. Ransomware was quantified[332] as a top impact threat and is described in more detail in chapter 3.

Developing the components that comprise malware requires specific expertise. As detection and blue team capabilities evolve over time, the malicious code is often in continuous development to adapt to the changing requirements of victim environments. This code is sold, shared, stolen, and re-purposed, making it challenging for researchers and law enforcement to correctly attribute the threat actors involved in a malware campaign. Malicious code is prevalent and so are new malware families and strains. Resilience against attacks and deterrence against threat actors is an ongoing and uneven battle. The following section documents high-level trends identified during the reporting period.

During this reporting period, we have again observed a large number of incidents concerning malware. The incidents analysed are mainly focused on EU countries.

[329] https://csrc.nist.gov/glossary/term/malware
[330] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf
[331] https://attack.mitre.org/techniques/T1587/001/
[332] ENISA Cybersecurity Threat Landscape (CTL) methodology, July 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology

Figure 13 Time series of major incidents observed by ENISA (July 2021-June 2022)



4.1 TRENDS

4.1.1 After the COVID-19 drop, malware detection is on the rise again

In 2020, and the beginning of 2021, a global decrease in malware was noticed. This drop was linked to the COVID-19 pandemic and the fact that employees worked from home, thus limiting the visibility of malware infections you would typically find on corporate infrastructures[333]. By the end of 2021, when more people started returning to the office, a heavy increase in malware was notified (Figure 6)[334]. However, data suggests that the increase is not linearly linked to more people being in the corporate environment, simply because there has been more malware. The rise in malware is attributed mainly to crypto-jacking and IoT malware[335].

In 2021, the most common malware families included remote access Trojans (RATs), banking Trojans, information stealers and ransomware. The most common malware strains included Agent Tesla, AZORult, Formbook, Ursnif, LokiBot, MOUSEISLAND, NanoCore, Qakbot, Remcos, TrickBot, and GootLoader[336]. Most of these strains have been active for more than five years, confirming how malware development is a continuous effort and that active development does pay off. Other data from Q1 2022 confirms this trend, where the rise of Emotet (again) is a notable change.

4.1.2 Malware targeting IoT almost doubles

IoT malware has increased over 2021. The change in the first half of 2022 shows the prevalence of IoT targeting malware almost doubling. In the first 6 months of 2022, the attack volume is already higher than had been recorded over the last 4 years[337]. Research shows that in the first months of 2022, Mirai botnets were responsible for most

[333] ENISA Threat Landscape 2021
[334] Malwarebytes Threat Review 2022
[335] Mid-Year Update: 2022 SonicWall Cyber Threat Report
[336] joint Cybersecurity Advisory (CSA) – CISA/ ACSC - 2021 Top Malware Strains
[337] Mid-Year Update: 2022 SonicWall Cyber Threat Report
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

attacks, quantified to more than 7 million attacks. Mozi, another large botnet, has grown slightly since Q3 2021 and was detected more than 5 million times[338].

In 2021 and 2022, the most common IoT targets were networking devices such as Netgear (DGN), D-Link (HNAP), and Dasan (GPON)[339].

4.1.3 Supply chain attacks targeting open-source frameworks

Malware distribution is also achieved by so-called supply chain attacks. Open-source frameworks are either cloned with infected malware, with the goal of infecting anyone who implements these as tools or packages within their projects. As anyone can publish packages to open-source platforms, malware injection often remains under the radar for a long time.

A common way this is leveraged is through 'typo squatting'. By introducing a new package in such repositories, with a name very similar to popular packages, the chance increases that the package can either be referenced unintentionally by a developer, or that the dependency is introduced by the attacker on the original project through a PR, without standing out as an attack. In August 2021, researchers tracked around 8 malicious python libraries, downloaded more than 30,000 times back then[340].

Another use case is the use of rogue python libraries to steal information such as credentials. In June 2022 *pygrata* and *loglib* were found to extract AWS keys[341]. In august 2022, research uncovered more than 10 such packages. AsciI2text is an example of this type of malware; it will look for local passwords and upload them back to the attacker's infrastructure[342].

These attacks are found on common and popular repositories like NPM[343] [344], Python[345], and RubyGems.

4.1.4 Shift away from Microsoft Office Macros

VBA macros were a widespread way for malicious actors to gain access to deploy malware and ransomware. Microsoft announced in July 2022 that Office applications would block macros in files from the internet[346]. Malware distribution campaigns shifted away from macros. Data gathered between October 2021 and June 2022 confirms this shift towards using container files (ISO, ZIP, RAR) and Windows Shortcut (LNK) files in campaigns to distribute malware.

Since this security hardening, the number of malware campaigns using VBA macros has decreased from 70% to 20%, while the number of campaigns using LNK has increased from approximately 5% to more than 70%[347]. An example of such a campaign was detailed around April 2022 using a zipped ISO attachment to deliver BumbleBee, a downloader containing anti-virtualisation checks[348].

Note that many phishing campaigns use password-protected archives to bypass detection engines.

4.1.5 Mobile malware distribution: from broad infection to targeted attacks

[338] ESET Threat Report T1 2022
[339] 2022 SonicWall Cyber Threat Report
[340] https://jfrog.com/blog/malicious-pypi-packages-stealing-credit-cards-injecting-code/#products
[341] https://blog.sonatype.com/python-packages-upload-your-aws-keys-env-vars-secrets-to-web
[342] https://research.checkpoint.com/2022/cloudguard-spectral-detects-several-malicious-packages-on-pypi-the-official-software-repository-for-python-developers/
[343] https://blog.reversinglabs.com/blog/iconburst-npm-software-supply-chain-attack-grabs-data-from-apps-websites
[344] https://www.bleepingcomputer.com/news/security/new-linux-macos-malware-hidden-in-fake-browserify-npm-package/
[345] https://medium.com/checkmarx-security/typosquatting-campaign-targeting-12-of-pythons-top-packages-downloading-malware-hosted-on-github-9501f35b8efb
[346] https://docs.microsoft.com/en-us/deployoffice/security/internet-macros-blocked
[347] https://www.proofpoint.com/us/blog/threat-insight/how-threat-actors-are-adapting-post-macro-world
[348] https://www.proofpoint.com/us/blog/threat-insight/bumblebee-is-still-transforming
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

In June 2022, adware trojans were downloaded around 10 million times, according to a report[349]. Google has been swift to remove the malicious applications but they often remain unnoticed for a long time. Adware will present intrusive ads and try to subscribe users to premium and expensive services.

Furthermore, targeted mobile malware continued to be an important threat throughout 2021 and 2022. In the previous reporting period, we talked about Pegasus, the NSO spyware. We also saw more recent targeted attacks from other organisations, such as Predator from spyware developer Cytrox[350]. Public reports show that the targets of these attacks are often members of the political opposition, journalists and activists (as seen in chapter 2)[351].

4.1.6 Malware in the context of Ukraine

In January 2022, intrusion activities were identified as Master Boot Records (MBR) Wiper activity. This malware capability was used against multiple organisations in Ukraine. The malware was designed to look like ransomware but did not contain any feature for recovery. The primary purpose of the malware was to make data and systems unavailable[352]. Since then, many destructive malware strains were identified targeting Ukraine, including WhisperGate, HermeticWiper, IsaacWiper, HermeticWizard, and CaddyWiper.

Malware spam campaigns (Agent Tesla and Remcos) were found to be re-using the escalation in the Ukraine-Russia conflict to lure victims into opening malicious attachments[353].

Also, opportunistic cybercriminals targeted Ukrainian sympathisers by hosting malware posing as offensive tools to target Russian entities. Once downloaded, these files infect users rather than delivering the tools[354].

4.1.7 Coordinated take-down of mobile malware FluBot

Flubot is mobile malware installed via text messages, asking Android users to click a link and install the application. The application then asks for accessibility permissions allowing attackers access to banking application credentials or cryptocurrency account details and disabling built-in security mechanisms.

In June 2022, Europol announced the takedown of the FluBot operation and the takeover of its infrastructure[355]. The take-down was a technically complex operation involving 11 European Countries: Australia, Belgium, Finland, Hungary, Ireland, Spain, Sweden, Switzerland, the Netherlands, and the United States. Because the attacker's infrastructure became fully controlled by law enforcement, they now had a clear picture of the number of victims.

[349] https://news.drweb.com/show/review/?lng=en&i=14520
[350] https://citizenlab.ca/2021/12/pegasus-vs-predator-dissidents-doubly-infected-iphone-reveals-cytrox-mercenary-spyware/
[351] https://about.fb.com/news/2021/12/taking-action-against-surveillance-for-hire/
[352] https://www.microsoft.com/security/blog/2022/01/15/destructive-malware-targeting-ukrainian-organizations/
[353] https://www.bitdefender.com/blog/hotforsecurity/bitdefender-labs-sees-increased-malicious-and-scam-activity-exploiting-the-war-in-ukraine
[354] https://blog.talosintelligence.com/2022/03/threat-advisory-cybercriminals.html
[355] https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones

5. 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[356]. It uses various forms of manipulation to trick victims into making mistakes or hand over sensitive or secret information. In cyber security, social engineering lures users into opening documents, files or e-mails, visit websites or grant unauthorised persons access to systems or services. And although these tricks can abuse technology they always rely on a human element to be successful.

This threat canvas consists mainly of the following vectors: phishing, spear-phishing, whaling, smishing, vishing, business e-mail compromise (BEC), fraud, impersonation and counterfeit.

Phishing aims at stealing important information like 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 financial or personal information of victims are gathered via 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 using social engineering techniques to extract sensitive information from users.

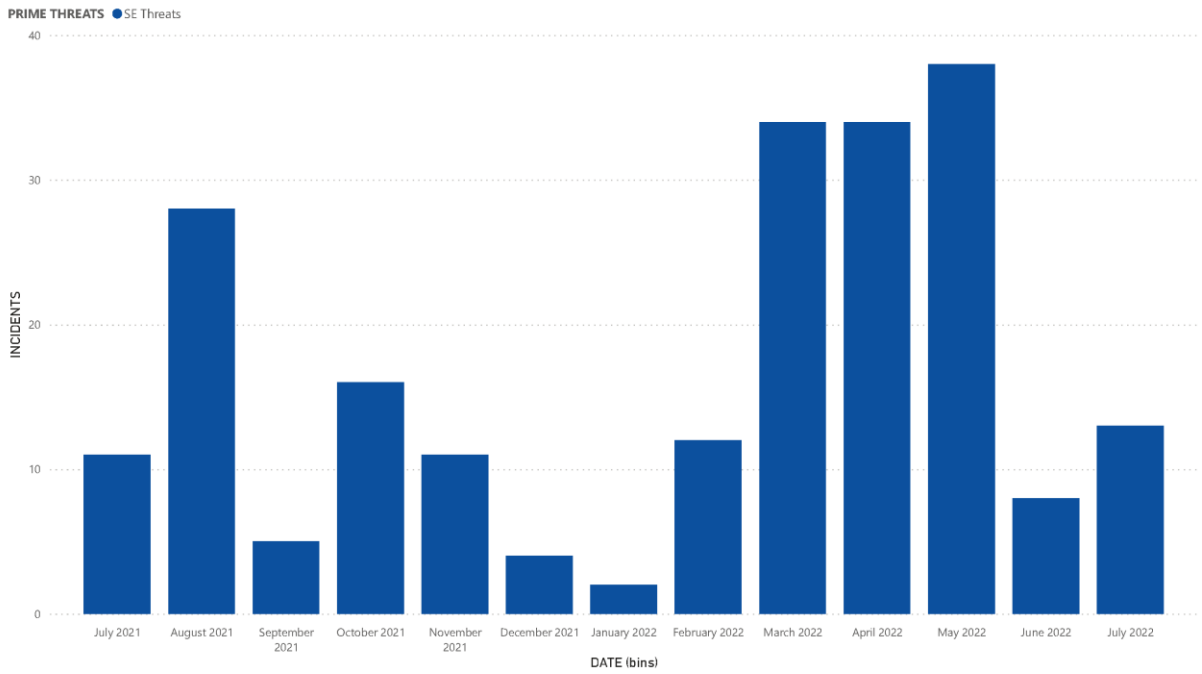
Business e-mail compromise (BEC) is a sophisticated scam targeting businesses and organisations, whereby criminals employ social engineering techniques to gain access to an employee's or executive's e-mail account to initiate bank transfers under fraudulent conditions.

Fraud[357] 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** finally is the fraudulent imitation of something.

During this reporting period, we have again observed a large number of incidents concerning social engineering threats. We are seeing a rise in 2022 which reinforces what was mentioned in chapter 3 as the common initial vector. The incidents analysed are mainly focused on EU countries.

[356] https://www.imperva.com/learn/application-security/social-engineering-attack/
[357] Fraud: https://www.britannica.com/dictionary/fraud

Figure 14: Time series of major incidents observed by ENISA (July 2021-June 2022)



5.1 TRENDS

Social engineering and especially phishing remain a popular technique for attackers to conduct their malicious activities[358] [359] [360] [361]. According to the Verizon Data Breach Investigations Report[362] (DBIR) about 82% of breaches involve a human element and no less than 60% of the breaches in Europe, the Middle East and Africa include a social engineering component. The underlying reason for the criminals' interest in social engineering is obvious. E-mail is where their potential victims are easiest reachable. And despite awareness raising campaigns and exercises, users still fall for these tricks[363]. Also according to the DBIR, attackers continue to use stolen credentials to obtain more details on a target via company e-mails. Their final goal is then to use this information to craft realistic pretexts, for example as part of BEC attacks.

The takedown[364] of Emotet by law enforcement and judicial authorities in January 2021 caused a decline in malicious activities but this was mostly cancelled out in the reporting period by prolific phishing and fraud activity[365] [366]. And despite the takedown, Emotet resurfaced in November 2021, which some researchers reported at the behest of the Conti ransomware group[367] [368]. The leak (or 'disclosure') of the playbook of this group also underlined[369] [370] [371] that ransomware groups rely heavily on well-established social engineering options[372] such as spear phishing and phone

[358] ESET threat report T32021 https://www.welivesecurity.com/2022/02/09/eset-threat-report-t32021/
[359] Microsoft Digital Defense Report https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi
[360] IBM X-Force Threat Intelligence Index 2022 https://www.ibm.com/downloads/cas/ADLMYLAZ
[361] Heimdal CyberSecurity & Threat Intelligence Report 2021 https://heimdalsecurity.com/blog/cybersecurity-threat-report/
[362] Verizon DBIR https://www.verizon.com/business/resources/reports/dbir/
[363] Acronis Cyberthreats Report 2022 https://www.acronis.com/en-us/resource-center/resource/672/
[364] Europol World's most dangerous malware EMOTET disrupted through global action https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
[365] ESET threat report T32021 https://www.welivesecurity.com/2022/02/09/eset-threat-report-t32021/
[366] IBM X-Force Threat Intelligence Index 2022 https://www.ibm.com/downloads/cas/ADLMYLAZ
[367] Cofense Phishing Takeaways from the Conti Ransomware Leaks – Part 2 https://cofense.com/blog/phishing-takeaways-from-conti-ransomeware-leaks-part-2
[368] Intel 471 Conti and Emotet: A constantly destructive duo https://intel471.com/blog/conti-emotet-ransomware-conti-leaks
[369] Tenable 2021 Threat Landscape https://www.tenable.com/cyber-exposure/2021-threat-landscape-retrospective
[370] IBM X-Force Threat Intelligence Index 2022 https://www.ibm.com/downloads/cas/ADLMYLAZ
[371] Unit 42 Ransomware Threat Report 2022 https://start.paloaltonetworks.com/unit-42-ransomware-threat-report.html
[372] CISA https://www.cisa.gov/uscert/ncas/alerts/aa21-265a
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

calls as their primary pathway for initial access. Both Europol[373] and the FBI[374] report that phishing and social engineering remain the main vectors for payment fraud, increasing in both volume and sophistication. The Ponemon Institute[375] reports that the cost of phishing in 2021 has more than tripled since 2015, with the most time-consuming tasks to resolve these attacks being the cleaning and fixing of infected systems and conducting forensic investigation.

It's worth noting that Mandiant[376] observed far fewer intrusions initiated via phishing in 2021. When the initial compromise was identified by Mandiant, phishing was the vector in only 11% of intrusions in 2021 compared to 23% in 2020. These numbers are based on Mandiant investigations and not so much on global telemetry on malicious activity, whether successful or not.

In general the objective of social engineering (and consequentially the impact for victims) is gaining access to information or services or obtaining knowledge about a specific subject but it is also used for **financial profit**. It thus comes as no surprise that during the reporting period financial institutes were among the top organisations impersonated by phishers. Next to the financial sector, the criminals themed[377] [378] [379] their social engineering campaigns around the technology sector with brands such as Microsoft, Apple and Google ranking as the top impersonated targets. We also witnessed social engineering campaigns mimicking popular cloud services used by remote workers or the platforms that are used by streaming and media providers. Cybercriminals also continued to capitalise on the Covid-19 pandemic in whatever ways they could.

Lastly, the decision by Microsoft[380] to disable Excel 4.0 macros by default is likely going to have an impact on the techniques used by threat actors to deliver their payloads. Those actors that used to rely on macros in attachments[381] for spear-phishing operations will now have to change their TTPs, for example by using LNK files, disk images or MSI installers. This will likely have an impact on the detection coverage and detection use cases of organisations.

5.1.1 Kits and services

Creating phishing websites and setting up the underlying infrastructure for a social engineering campaign can be a tedious job. Instead, criminals turn more and more to ready-made material offered by phishing kits or they make use of a service model through 'Phishing-as-a-Service'.

IBM reports[382] that deployments of phishing kits generally have a short lifespan, with almost one-third of deployed kits being used for no longer than a day. According to Microsoft[383], modern phishing kits are sufficiently sophisticated to masquerade as legitimate content in their use of spelling, grammar and imagery. In the same report Microsoft notes that the miscreants making use of these kits can also be fooled. Some of the kits contain 'added' functionality that not only sends the credentials obtained to phishers but also to the kit's originating author or a sophisticated intermediary. From a victim's point of view this can severely aggravate the impact of an incident as stolen credentials now end up in the hands of several different gangs.

Phishing kits also take into account regional differences (with geo-blocking), filter out unwelcome agents, add obfuscation options[384] and are sold as part of a software-as-a-service package: **Phishing-as-a-Service** (PhaaS). These services are not new but a report[385] from Microsoft on the BulletProofLink operation show its level of sophistication, professional business model and its use of automation.

[373] Europol IOCTA 2021 https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021
[374] FBI IC3 report https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
[375] Ponemon Institute The 2021 Cost of Phishing Study sponsored by Proofpoint https://ponemonsullivanreport.com/2021/08/
[376] Mandiant M-TRENDS 2022 https://www.mandiant.com/resources/m-trends-2022
[377] ESET threat report T32021 https://www.welivesecurity.com/2022/02/09/eset-threat-report-t32021/
[378] IBM X-Force Threat Intelligence Index 2022 https://www.ibm.com/downloads/cas/ADLMYLAZ
[379] Microsoft Digital Defense Report https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi
[380] Excel 4.0 (XLM) macros now restricted by default for customer protection https://techcommunity.microsoft.com/t5/excel-blog/excel-4-0-xlm-macros-now-restricted-by-default-for-customer/ba-p/3057905
[381] Phishing: Spearphishing Attachment T1566.001 https://attack.mitre.org/techniques/T1566/001/
[382] IBM X-Force Threat Intelligence Index 2022 https://www.ibm.com/downloads/cas/ADLMYLAZ
[383] Microsoft Digital Defense Report https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi
[384] https://www.bleepingcomputer.com/news/security/phishing-kits-constantly-evolve-to-evade-security-software/
[385] Catching the big fish: Analyzing a large-scale phishing-as-a-service operation https://www.microsoft.com/security/blog/2021/09/21/catching-the-big-fish-analyzing-a-large-scale-phishing-as-a-service-operation/
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Because of the low cost of access and the relative ease of how these campaigns can be deployed it is very likely that phishing campaigns, run via Phishing-as-a-Service infrastructure, are not going away anytime soon.

An extension of PhaaS is the use of **Initial Access Brokers** (IAB). This supply chain of social engineering specialists first opens the 'flood gates' to an organisation, after which they hand over their access, often credentials or installed remote access tools, to follow-up actors[386]. As the DBIR stated earlier, this can then be used by the attackers to engage with victims or find their way further into an organisation. This market for IAB has further flourished[387] in recent years, mostly because of the constant demand from criminal organisations for easy access to organisations.

Due to the increased diversification, professionalisation and specialisation of threat groups (groups responsible for initial access, groups for malware or ransomware and then extorsion), it is very likely that we will see more cases of initial access brokers first fighting their way into an organisation and then making their access available for follow-up criminal activity or, if that were the case, espionage campaigns.

A noteworthy campaign by an initial access broker referred to as 'Exotic Lily' was documented by Google's TAG (Threat Analysis Group)[388] in March 2022. The group used phishing e-mails to deliver an exploit for a vulnerability in Microsoft MSHTML and appears to be providing initial access for groups spreading Conti and Diavol ransomware. The payload of the mails included the use of disk image (ISO) files. But they were not the only threat actors that were observed that were using disk images.

5.1.2 Spear-phishing campaign by The Dukes

ESET[389] revealed a noteworthy spear-phishing campaign conducted by The Dukes[390], also referred to as APT29, Cozy Bear or Nobelium. In October and November 2021 this espionage group targeted various European diplomatic missions and Ministries of Foreign Affairs with approaches similar to their earlier campaigns targeting French[391] and Slovak[392] organisations. In the latest campaign the actors impersonated other government agencies and persuaded victims to open an HTML file which then downloaded a disk image (ISO or VHDX). Within this disk image the attackers stored further malware, eventually leading to a Cobalt Strike beacon. Disk images are a powerful method for evading defences to deliver malware. The Mark-of-the-Web (MOTW) cannot be applied to the files inside a disk image, and as such it evades SmartScreen and there will be no warning for users that potentially unsafe files (downloaded from the internet) are being opened[393] [394].

A similar campaign, with a little twist, was conducted earlier in July 2021. In this campaign[395] the initial e-mail, impersonating someone working at the Belgian embassy in Ireland, did not contain malicious content. It's only after replying, in which the reply was sent to a compromised account instead of to the Belgian embassy, that victims received a follow-up e-mail with a ZIP attachment, containing once again a disk image (ISO) which then leads to a Cobalt Strike.

This approach of first sending a non-malicious e-mail with a follow-up message containing payload is a technique also employed by SideWinder[396], a threat actor primarily active in Asia.

We have singled out these campaigns by The Dukes because of their specific targeting and profiling of victims, the persistence and long-term operation of their activities and not to forget the quality of their lures. The different cases observed during this reporting period demonstrate their continued activity and the fact that they remain a prime threat

[386] Microsoft Digital Defense Report https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi
[387] Initial Access Brokers in 2021: An Ever Expanding Threat https://www.digitalshadows.com/blog-and-research/initial-access-brokers-in-2021-an-ever-expanding-threat/
[388] Exposing initial access broker with ties to Conti https://blog.google/threat-analysis-group/exposing-initial-access-broker-ties-conti/
[389] ESET threat report T32021 https://www.welivesecurity.com/2022/02/09/eset-threat-report-t32021/
[390] APT29: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=APT%2029%2C%20Cozy%20Bear%2C%20The%20Dukes
[391] ANSSI CERTFR-2021-CTI-011 https://www.cert.ssi.gouv.fr/cti/CERTFR-2021-CTI-011/
[392] APT Cobalt Strike Campaign targeting Slovakia (DEF CON talk) https://www.istrosec.com/blog/apt-sk-cobalt/
[393] Threat Thursday - Evading Defenses with ISO files like NOBELIUM https://www.scythe.io/library/threat-thursday-evading-defenses-with-iso-files-like-nobelium
[394] New sophisticated email-based attack from NOBELIUM https://www.microsoft.com/security/blog/2021/05/27/new-sophisticated-email-based-attack-from-nobelium/
[395] Twitter Alex Lanstein https://twitter.com/alex_lanstein/status/1415835521553735687
[396] SideWinder https://apt.etda.or.th/cgi-bin/showcard.cgi?g=SideWinder%2C%20Rattlesnake
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

to western diplomats, NGOs and think tanks. It is very likely that we will witness further campaigns by this set of intruders.

5.1.3 Ukraine war themed attacks

A campaign highlighted in March 2022 by Proofpoint[397] is about a likely nation-state sponsored phishing campaign that used a possibly compromised Ukrainian armed service member's e-mail account to target European government personnel involved in managing the logistics for refugees fleeing Ukraine. The campaign used an e-mail with a subject referring to a decision of the Security Counsel of Ukraine.

Google's TAG has observed a continuously growing number of threat actors using the war in Ukraine as a lure in phishing and malware campaigns. One of the campaigns involved COLDRIVER, an allegedly Russian based threat actor sometimes referred to as Callisto, which used credential phishing e-mails to target government and defence officials, politicians, NGOs, think tanks and journalists[398]. COLDRIVER was previously also witnessed targeting the military of multiple Eastern European countries, as well as a NATO Centre of Excellence[399].

Based on this research from TAG, Sekoia[400] revealed a phishing based reconnaissance campaign in Europe by the threat actor Turla[401] (also referred to as Snake or Venomous Bear). In this campaign the threat actor targeted the Baltic Defence College's website as well as the Austrian Federal Economic Chamber.

Considering the type of horrific events we already witnessed, it is very likely that we will continue to see similar Ukraine war themed social engineering attacks (and very likely amongst other types of cyberattacks), targeting European governments, civilians and organisations.

5.1.4 Phishing from known accounts

The use of multi-factor authentication (MFA) has reduced the opportunities for attackers to use compromised accounts as a pivot point for starting social engineering campaigns. So instead of targeting individual mailboxes, we have witnessed attackers shifting to abuse legitimate infrastructure to execute their operations.

An example of such a shift in tactics is where attackers register trial tenants for services at Office 365 which make their e-mail appear much more legitimate[402]. Other ways include compromising a Microsoft Exchange server via ProxyShell or ProxyLogin and then distributing phishing e-mails to internal and external user accounts[403] [404]. To further deceive potential victims, attackers also hijack mail conversations and in some cases modified the typeface and language of the reply messages for each attack to increase the chances of success.

It is likely that we will see further use of known (and sometimes 'trusted') accounts or legitimate infrastructure to execute phishing campaigns, either by exploiting vulnerabilities in systems such as Microsoft Exchange or by making use of exploitation efforts by other threat actors.

The technique of hijacking mail conversations is also seen frequently in BEC attacks.

5.1.5 Business e-mail compromise

According to the Internet Crime Report[405], Business E-mail Compromise or BEC is one of the most financially impactful types of cybercrime.

[397] Asylum Ambuscade: State Actor Uses Compromised Private Ukrainian Military Emails to Target European Governments and Refugee Movement https://www.proofpoint.com/us/blog/threat-insight/asylum-ambuscade-state-actor-uses-compromised-private-ukrainian-military-emails
[398] Update on cyber activity in Eastern Europe https://blog.google/threat-analysis-group/update-on-cyber-activity-in-eastern-europe/
[399] Tracking cyber activity in Eastern Europe https://blog.google/threat-analysis-group/tracking-cyber-activity-eastern-europe/
[400] TURLA's new phishing-based reconnaissance campaign in Eastern Europe https://blog.sekoia.io/turla-new-phishing-campaign-eastern-europe/
[401] Turla: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Turla%2C%20Waterbug%2C%20Venomous%20Bear
[402] Microsoft Digital Defense Report https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFli
[403] Threat Analysis Report: DatopLoader Exploits ProxyShell to Deliver QBOT and Cobalt Strike https://www.cybereason.com/blog/research/threat-analysis-report-datoploader-exploits-proxyshell-to-deliver-qbot-and-cobalt-strike
[404] Squirrelwaffle Exploits ProxyShell and ProxyLogon to Hijack Email Chains https://www.trendmicro.com/en_us/research/21/k/Squirrelwaffle-Exploits-ProxyShell-and-ProxyLogon-to-Hijack-Email-Chains.html
[405] Crime type by victim loss in FBI IC3 report https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

One of the reasons for the 'popularity' of BECs is that instead of having to go through all the trouble of multi-stage attacks and finding their way in an unknown environment, attackers can just 'ask' to execute a financial transaction (or a variant depending on their objectives).

While a BEC attack can be seen as phishing, it does not rely as much on malware or malicious links as on abusing trust, impersonation and other social engineering techniques.

Compared to previous years, the median transaction size for business e-mail compromise attacks further increased[406] substantially. According to the DBIR[407] only 41% of BECs involved phishing and about 25% involved the use of stolen credentials against the victim organisation.

Despite the efforts of law enforcement agencies to combat BEC attacks, such as the arrest[408] by Interpol as part of Operation Delilah, these type of attacks remain very lucrative for criminals. Considering this financial aspect, it remains very likely that we will continue to see an increase in the financial impact of BECs.

5.1.6 Malicious quick response (QR) codes

In January 2022 the FBI issued a warning[409] concerning criminals using QR codes to redirect victims to malicious sites that steal login and financial information. A similar effort was observed by the Phishing Defence Centre where threat actors used malicious QR codes to target users of German banking[410]. It is important to realise is that these type of scams can happen both in the digital space as well as in the physical realm[411].

It is likely that the trend of abusing QR codes for phishing will further continue, especially considering the wide adaptation of QR codes in everyday life.

5.1.7 Consent phishing

Both Microsoft[412] and Mandiant[413] report on cases where attackers use consent phishing to send users links that, if clicked, will grant the attacker access and permissions to applications and services.

Threat actors create and register malicious applications in, for example, Azure to attempt to gain persistent access to data and applications such as Exchange Online. Once a non-privileged user has approved consent, they collect the access token and then have account-level access to the victim's data without the need for the user's credentials.

Because of the technical requirements and investments in resources (after all, developing an 'app' requires more effort than subscribing to a PhaaS) and considering that there are still far easier approaches for obtaining a social engineering objective, this type of attack might not be the first choice for many threat groups. But considering the potential impact and also the lower chance of being detected, either because of a lack of visibility or of knowledge by most organisations, it is likely we'll see an increase of consent phishing attacks.

5.1.8 Automation

Threat actors employing social engineering attacks are further automating their operations[414]. We do not have an immediate expectation that artificial intelligence will be driving phishing e-mails but with increased automation there are worrying evolutions on the horizon[415].

[406] FBI IC3 report https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf
[407] Verizon DBIR https://www.verizon.com/business/resources/reports/dbir/
[408] Operation Delilah: Unit 42 Helps INTERPOL Identify Nigerian Business Email Compromise Actor https://unit42.paloaltonetworks.com/operation-delilah-business-email-compromise-actor/
[409] FBI Cybercriminals Tampering with QR Codes to Steal Victim Funds https://www.ic3.gov/Media/Y2022/PSA220118
[410] German Users Targeted in Digital Bank-Heist Phishing Campaigns https://cofense.com/blog/german-users-targeted-in-digital-bank-heist-phishing-campaigns/
[411] Hidden Scams in Malicious Scans: How to Use QR Codes Safely https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/hidden-scams-in-malicious-scans-how-to-use-qr-codes-safely
[412] Microsoft Digital Defense Report https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi
[413] Mandiant M-TRENDS 2022 https://www.mandiant.com/resources/m-trends-2022
[414] Microsoft Digital Defense Report https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi
[415] Acronis Cyberthreats Report 2022 https://dl.acronis.com/u/rc/White-Paper-Acronis-Cyber-Threats-Report-2022-EN-US.pdf
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Threat actors will likely employ increased customised, individualised and personalised attacks with victim information pulled directly from published data breaches and, in some cases, combining information from multiple data dumps. Furthermore, complementing this data with open source information such as social media profiles, company and personal websites as well as published documents will provide new opportunities for miscreants[416] and is something we will likely observe in the near future.

5.1.9 Smishing via FluBot

A mobile banking malware that's been heavily observed is FluBot. It targets users of Android devices in most of Europe and is spread via SMS and MMS. Victims first receive an SMS message (called smishing or SMS phishing) that impersonates parcel delivery companies, voicemail memos or fake software. The message contains a link that points to a website, instructing the victim to install an app. Once the app is installed, the requested permissions are granted or, sometimes, security features are disabled. FluBot spreads through self-propagation by sending phishing text messages from the infected device to its contact list. It will also share this contact list with the campaign operators but, most problematic for the victims, it also collects credit card numbers and online banking credentials, intercepts SMS messages (such as one-time passwords) and captures screenshots[417] [418] [419] [420] [421].

And although FluBot does not run on Apple devices (iOS), iPhone users are not safe either. If users follow the links in the SMS messages, they are redirected to more 'traditional' phishing sites and subscription scams.

In June 2022 an international law enforcement operation[422] resulted in the takedown of FluBot. Although there are no immediate signs that this exact mobile malware strain will resurface, considering the financial gain, the large available target base and the relative ease of infection and propagation it is very likely we will see other criminal groups filling in the void in the mobile malware landscape.

5.1.10 Increase of attacks on crypto exchanges and cryptocurrencies owners

Cryptocurrencies have always been a preferred choice of payment for cyber criminals. But as these cryptocurrencies become more and more popular, criminals also turned their attention directly into targeting crypto exchanges and cryptocurrencies owners. This was already demonstrated early in 2021 with the attacks on the users of Coinbase, and most likely we can expect more similar attacks in 2022[423].

Another related area that is offering opportunities for social engineering attacks by criminals is the non-fungible tokens (NFT) market. The methods used are no different than those used for 'traditional' markets, including fake profiles on social media, social media account hijacking, counterfeit material (fake mints), phishing fraud and impersonation attacks[424].

As cryptocurrencies and derivates gain in popularity, social engineering attacks against these phenomena will likely follow and occur more frequently.

5.1.11 Vishing using the safe account scams

According to Europol[425] the safe account scam is an emerging modus operandi in vishing. In such a scam attackers convince victims into transferring funds to a 'safe account' by telling them their bank account has been compromised. To make the story more convincing, they often pose as a police officer or an employee of their financial institution.

[416] The Coming AI Hackers https://www.belfercenter.org/publication/coming-ai-hackers
[417] FluBot NCSC-FI https://www.kyberturvallisuuskeskus.fi/en/varoitus_1/2022
[418] FluBot Safeonweb.be https://www.safeonweb.be/nl/actueel/opgepast-voor-het-gevaarlijke-flubot-virus-klik-niet-op-verdachte-smsjes
[419] Europol IOCTA 2021 https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021
[420] FluBot malware now targets Europe posing as Flash Player app https://www.bleepingcomputer.com/news/security/flubot-malware-now-targets-europe-posing-as-flash-player-app/
[421] New FluBot Campaign Sweeps through Europe Targeting Android and iOS Users Alike https://www.bitdefender.com/blog/labs/new-flubot-campaign-sweeps-through-europe-targeting-android-and-ios-users-alike
[422] Europol Takedown of SMS-based FluBot spyware infecting Android phones https://www.europol.europa.eu/media-press/newsroom/news/takedown-of-sms-based-flubot-spyware-infecting-android-phones
[423] Acronis Cyberthreats Report 2022 https://dl.acronis.com/u/rc/White-Paper-Acronis-Cyber-Threats-Report-2022-EN-US.pdf
[424] Common NFT scams and how to avoid them https://www.welivesecurity.com/2022/05/23/common-nft-scams-how-avoid-them/
[425] Europol IOCTA 2021 https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment-iocta-2021
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Unfortunately this so called safe account is under the control of fraudsters and after the money transfers have been completed victims find that they have lost their life's savings in the space of a few minutes.

The volume of vishing cases has also increased substantially, according[426] to Agari and PhishLabs, no less than 550 per cent over the last twelve months (Q1 2022 compared to Q1 2021). It is very likely we will continue to witness this trend in the near future.

5.1.12 Long running social engineering attacks

Earlier we covered the case of The Dukes as an APT relying on social engineering as a prime technique for their operations. But they are not the only one.

Iranian threat groups such as APT34[427] (OilRig or TA452), APT35[428] (Charming Kitten or TA453) or TA456[429] (Imperial Kitten or Tortoiseshell) employ long running social engineering campaigns for cyber espionage and information operations. In the Operation SpoofedScholars[430], revealed in July 2021, the threat group TA453[431] masqueraded as UK scholars with the University of London's School of Oriental and African Studies (SOAS). They targeted senior think tank personnel, journalists focused on Middle Eastern affairs as well as professors with very targeted fake invitations to conferences. These invitations eventually led to credential stealing websites.

Whereas this group used the professional background of their identified targets to build a story, other campaigns such as those run by Curium[432] (TA456[433]) focus on romantic engagements. Their playbook typically consists of masquerading as an attractive woman on social media, establishing connections via both corporate and personal platforms (to increase the bond of trust), sharing malicious documents and then convincing the target to open the document with the goal of exfiltrating sensitive information.

Considering the success of previous campaigns it is very likely that we will continue to see similar social engineering tradecraft, persistency and determination being used by threat actors coming from the Iranian region.

[426] Quarterly Threats Trends & Intelligence https://info.phishlabs.com/quarterly-threat-trends-and-intelligence-may-2022
[427] APT34: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=OilRig%2C%20APT%2034%2C%20Helix%20Kitten%2C%20Chrysene
[428] APT35: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Magic%20Hound%2C%20APT%2035%2C%20Cobalt%20Gypsy%2C%20Charming%20Kitten
[429] Tortoiseshell: https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Tortoiseshell%2C%20Imperial%20Kitten
[430] Operation SpoofedScholars: A Conversation with TA453 https://www.proofpoint.com/us/blog/threat-insight/operation-spoofedscholars-conversation-ta453
[431] The operation was documented by Proofpoint, hence we use the threat actor naming convention of Proofpoint as the first reference
[432] Evolving trends in Iranian threat actor activity – MSTIC presentation at CyberWarCon 2021
https://www.microsoft.com/security/blog/2021/11/16/evolving-trends-in-iranian-threat-actor-activity-mstic-presentation-at-cyberwarcon-2021/
[433] I Knew You Were Trouble: TA456 Targets Defense Contractor with Alluring Social Media Persona https://www.proofpoint.com/us/blog/threat-insight/i-knew-you-were-trouble-ta456-targets-defense-contractor-alluring-social-media

6. THREATS AGAINST DATA

Today, we live in an interconnected society where cloud, edge and IoT technologies and applications produce huge amounts of data every second. 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, Machine Learning (ML) and Artificial Intelligence (AI) are increasingly being adopted and are boosting the migration from traditional software systems based on deterministic algorithms to systems where ML or AI models use reason on data to calculate a solution for individual instances of a problem. This migration poses a new wave of risks that push towards the 'AI Act',[434] a proposed European law on artificial intelligence (AI) – the first law on AI by a major regulator anywhere.

The central role assumed by data as the enabler of a data-driven economy makes data a major target for cybercriminals. **Threats against data** form a collection of threats that target data sources with the aim of gaining unauthorised access and disclosure, as well as the manipulation of data to interfere with system behaviour. These threats are also at the basis of many of the existing threats, also discussed in this report. For instance, ransomware, RDoS, DDoS aim to deny access to data and possibly collect a payment to restore this access. Disinformation and misinformation build on data manipulation. Phishing, also in its novel implementation based on deepfakes, builds on data manipulation.

A data breach is defined in the GDPR[435] 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 in data breach and data leak. Though often used as interchangeable concepts, they entail fundamentally different concepts that mostly lie in how they happen[436] [437].

Data breach is an intentional attack brought by a cybercriminal with the goal of gaining unauthorised access and the release of 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 of stealing data.

Data leak is an event that can cause the unintentional release of sensitive, confidential or protected data due to, for example, misconfigurations, vulnerabilities or human errors. It does not include intentional attacks.

In a nutshell, data breaches can occur as a result of a cyberattack while data leaks consist of unintentional loss or exposure of data. Data breaches are the most long-lived threat to data. However, the exponential growth of connected systems and the digital transformation have increased the relevance of data leaks due to the increasing expansion of the attack surface as well as the increasing involvement of users in the workings of software systems[438].

In addition to data leak and data breach, the increasing adoption of ML or AI models at the core of novel distributed systems and decision-making put **data manipulation** under the spotlight. **Data poisoning** and adversarial attacks become widespread with the aim of undermining trust in IT and production systems and, more generally, in society as a whole. On one side, data manipulation attacks target modern systems affecting the accuracy of their results; on the other side, data manipulation attacks target people disseminating disinformation (see chapter 9).

Threats against data consistently rank high among the leading threats of the ETL and this trend continued in the reporting period of the ETL 2022. Adversaries explore a series of new techniques and exploit the increasing online

[434] https://artificialintelligenceact.eu/
[435] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:02016R0679-20160504&from=EN
[436] https://blog.f-secure.com/data-breach-and-data-leak-whats-the-difference/
[437] https://www.upguard.com/blog/data-breach-vs-data-leak#:~:text=Simply%20put%2C%20a%20data%20leak,Apps%20data%20leak%20in%202021
[438] https://www.upguard.com/blog/data-breach-vs-data-leak#:~:text=Simply%20put%2C%20a%20data%20leak,Apps%20data%20leak%20in%202021
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

presence and use of online services by the general public. Data exfiltration (aka data theft) is used by malicious actors to target, copy and transfer sensitive data. A particular case of the use of exfiltrated data is identity theft, where malicious actors use personal identifiable information (PII) to impersonate a user. 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 (DDoS) and disinformation. It is noteworthy that in the ENISA threat landscape for supply chain attacks report[439] in 2021, for about 58% of the supply chain incidents analysed, the customer assets targeted were predominantly customer data, including personally identifiable information (PII) data and intellectual property.

6.1 TRENDS

The data never sleep infographic, version 9.0, shows that the increase in data collection, sharing and analysis brought by the pandemic did not decrease in 2021[440]. These trends are all increasing. According to Statista the entire world produced and consumed a total of 79 zettabytes and this is predicted to grow to over 180 zettabytes by 2025.

The Verizon data breach investigation report (DBIR) presents a detailed overview of data breaches (in its wider term including data leaks) in 2021[441]. Verizon observes that around 80% of total data compromises comes from outside the target organisation, while around 20% comes from inside. The motivation is still mainly financial gain (around 90%) and, second by far, espionage (less than 10%). Web applications, e-mails, and carelessness (e.g. errors and misconfigurations) are among the main data breach vectors, coupled with the use of stolen credentials, ransomware and phishing as the types of action forming the basis of breaches. This again shows the importance of human involvement when a data breach is executed, as well as the central role of the Internet. In fact, 82% of data breaches involve a human element; this can be easily explained by considering that both social engineering and miscellaneous errors (misdelivery and misconfiguration) are among the main attack patterns, third and fourth respectively, only outperformed by system intrusion (which also involves social attacks) and basic web application attacks. According to the ITRC, e-mail and weak cloud configurations are also among the most important human errors[442].

Despite the importance of humans in data breaches, it is important to note that the exploitation of vulnerabilities as the causes of of data breaches has doubled, reaching 7% of breaches this year.

Threats and actions causing a data breach mainly involved hacking (~50%), malware (~40%), social (~20%) and error (13%)[443]. Servers were the most important assets targeted by an attack (almost 90%), followed by persons (less than 30%) and user dev (less than 20%). Web applications and mail servers are in the first two spots in terms of the importance of server assets, with database servers reaching the fifth place; desktop or laptop (third place) and finance (sixth place) are the most important for user dev and persons, respectively.

The DBIR also shows how credentials and personal data are the top two types of data an attacker wants to collect maliciously[444] [445]. Credentials are critically important for an attacker to cover up his or her activities, while personal data are useful for financial fraud and resale. Payment data observed a continuous decline with less than a 10% share in 2021.

Similarly to 2020, considering data breaches, the industry sectors suffering the most from internal errors are finance and insurance, healthcare, public administration and professional. In the financial sector, financially motivated organised crime uses social actions (phishing), hacking (use of stolen credentials) and malware (ransomware) to target a victim. Servers are involved in 90% of data breaches, with an increase to 51% of web applications. Basic web application attacks, system intrusion and miscellaneous errors represent 79% of breaches. In the healthcare sector, basic web application attacks, miscellaneous errors and system intrusions represent 76% of breaches, with internal threat actors still prominent (39%). In the information sector, system intrusions, basic web application attacks

439 https://www.enisa.europa.eu/news/enisa-news/understanding-the-increase-in-supply-chain-security-attacks
440 https://www.domo.com/learn/infographic/data-never-sleeps-9
441 https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf
442 2022 ITRC Annual Data Breach Report
443 https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf
444 https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf
445 2022 ITRC Annual Data Breach Report

and miscellaneous errors represent 81% of breaches. In the public administration sector, personal data and credentials account for 46% and 34% of compromised data, respectively.

Concerning the geographical spread, DBIR observed *i)* a high number of social and hacking related attacks in APAC, with a much lower number of ransomware cases; *ii)* an increase of social engineering in EMEA with credential theft the largest problem; *iii)* the system intrusion pattern becoming the most important pattern in NA, with social engineering retaining an important role; *iv)* ransomware and denial-of-service attacks accounting for 37% and 27% of incidents, respectively, in LAC.

6.1.1 Attack vectors, assets and motivations remain similar to 2021

During the reporting period, trends related to attack vectors, assets and motivations remained similar to 2021[446].

Regarding attack vectors, and in particular the types of action used as the basis of a breach, the use of stolen credentials, ransomware and phishing are still in the top five. With respect to 2021, the use of stolen credentials took the lead (around 40%), with ransomware showing a substantial increase of 13% to reach 25% in total, and phishing showing a decrease of around 20% in total. The importance of ransomware and phishing was also observed in the USA[447].

Server, person and user devices remain in the first three spots of the main targeted assets, with the same ordering and similar shares. Same discussion holds for the types of assets, where web applications, mail, and desktop or laptop remain at the first three spots in the rankings.

As in past years, financial gain continues to be the most common motivation. Financially motivated attacks have increased to almost 90% of cyberattacks, such as stealing money directly from financial accounts, stealing credit card information or other types of data that can be monetised or demanding ransom. Espionage as a motivation accounts for around 10% of cyberattacks[448].

6.1.2 Data compromise increasing year over year

The central role of data in our society produced a sharp increase in the amount of data collected and in the importance of proper data analysis. The price we pay for such importance is a continuous and unstoppable increase in data compromises.

According to Eva Velasquez, President and CEO of the Identity Theft Resource Centre (ITRC), *In 2021, there were more data compromises reported in the United States of America than in any year since the first state data breach notice law became effective in 2003*, while, at the same time, *less than 5 per cent take the most effective protective action after receiving a data breach notice*[449].

The number of data compromises increased by 68% over 2020, and 23% over the previous record[450]. This surge in compromises is independent of sector, showing an increase in every primary sector but one – the Military.

6.1.3 Identity theft and synthetic identity

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. According to the US Federal Trade Commission (FTC), 1.4 million reports of identity theft have been received in 2021 and the most targeted victims are between 30 and 39 years old[451]. According to McAfee[452], credit card fraud is the most common type of identity theft.

[446] https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf
[447] 2022 ITRC Annual Data Breach Report
[448] https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf
[449] 2022 ITRC Annual Data Breach Report
[450] 2022 ITRC Annual Data Breach Report
[451] https://www.ftc.gov/system/files/ftc_gov/pdf/CSN%20Annual%20Data%20Book%202021%20Final%20PDF.pdf
[452] https://www.mcafee.com/blogs/tips-tricks/a-guide-to-identity-theft-statistics-for-2022/#:~:text=An%20estimated%2015%20million%20Americans,Fraud%20Study%3A%20The%20Virtual%20Battlegroun)
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

According to ETL 2021[453], a lot of incidents could have involved synthetic identities. Synthetic identity theft is a type of fraud in which criminals combine real and fake information to create a new identity. Incidents with synthetic identities tend to be more common in the United States because of static personally identifiable information, which is used to verify someone's identity, according to the Federal Reserve[454]. Synthetic identity fraud still increased over 2021, while FiVerity estimated that losses grew to $20 billion[455].

6.1.4 Actors privilege highly rewarding data

The Identity Theft Resource Centre also reported in its 2022 Annual Data Breach Report that the motivation of cybercriminals has shifted and instead of targeting consumers in order to steal large amounts of personal information, they focus on specific data types. A typical example involves stolen credentials.

This results in a decrease by 5% of the number of victims, though the total number of victims remains impressively high.

6.1.5 Ransomware

As already discussed in chapter 3, ransomware-related data breaches are increasingly gaining importance and it was one of the first three root causes of compromise during the last year[456] [457]. Ransomware is also increasingly used in combined attacks that target the CIA triad of systems and corresponding data. For instance, Ransom Denial of Service (RDoS) is the new frontier of denial of service attacks. 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. EUROPOL reported in its IOCTA 2021[458] the comeback of DDoS attacks followed by ransom demands, with an increase in high-volume attacks compared to the previous year. We recall that, according to Cloudflare, in Q4 2021, ransom DDoS attacks increased by 29% year-over-year and 175% quarter-on-quarter[459].

6.1.6 Data poisoning and manipulation

The EU H2020 project CONCORDIA identified data poisoning as one of the major threats in the data domain[460]. Trustworthy data are in fact a prerequisite for implementing safe autonomic and adaptive systems built on data. In particular, the central role of collected data and corresponding inferences on the behaviour of modern systems increases the risk introduced by data poisoning and manipulation. The latter then become fundamental threats to data-driven systems, where data integrity is not the only property to protect and guarantee, but also data provenance, non-repudiation, and accountability should be supported.

In this context, Ransomware attacks (see chapter 3) as well as deepfakes (see chapter 9) are spreading and target the integrity and availability of data, introducing substantial risks to decisions built entirely on unverified data. For instance, a deepfake voice call resulted in a fraudulent bank transfer of nearly $35 million[461].

6.1.7 Data extraction from ML models

Machine Learning (ML) models are at the core of modern distributed systems and are increasingly becoming the target of attacks[462].

A direct consequence of data poisoning and manipulation is a decrease in the accuracy of machine learning models. On one side, according to EU H2020 project CONCORDIA in its deliverable D4.1,[463] machine learning models can be attacked by poisoning data used for the training of the model. The resulting model will then learn a behaviour different from the real and correct behaviour of the target system, forcing the system to take wrong decisions. On the other

[453] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
[454] https://fedpaymentsimprovement.org/wp-content/uploads/frs-synthetic-identity-payments-fraud-white-paper-july-2019.pdf
[455] https://www.fiverity.com/resources/fiverity-introduces-2021-synthetic-identity-fraud-report2
[456] 2022 ITRC Annual Data Breach Report
[457] https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf
[458] https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf
[459] https://blog.cloudflare.com/ddos-attack-trends-for-2021-q4/
[460] https://www.concordia-h2020.eu/wp-content/uploads/2020/06/D4.1_Ready_for_Submission_D4.1-final_revised.pdf
[461] https://www.forbes.com/sites/thomasbrewster/2021/10/14/huge-bank-fraud-uses-deep-fake-voice-tech-to-steal-millions/
[462] Deliverable D4.3, EU H2020 project CONCORDIA, https://www.concordia-h2020.eu/wp-content/uploads/2022/07/CONCORDIA-D4.3.pdf
[463] https://www.concordia-h2020.eu/wp-content/uploads/2020/06/D4.1_Ready_for_Submission_D4.1-final_revised.pdf
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

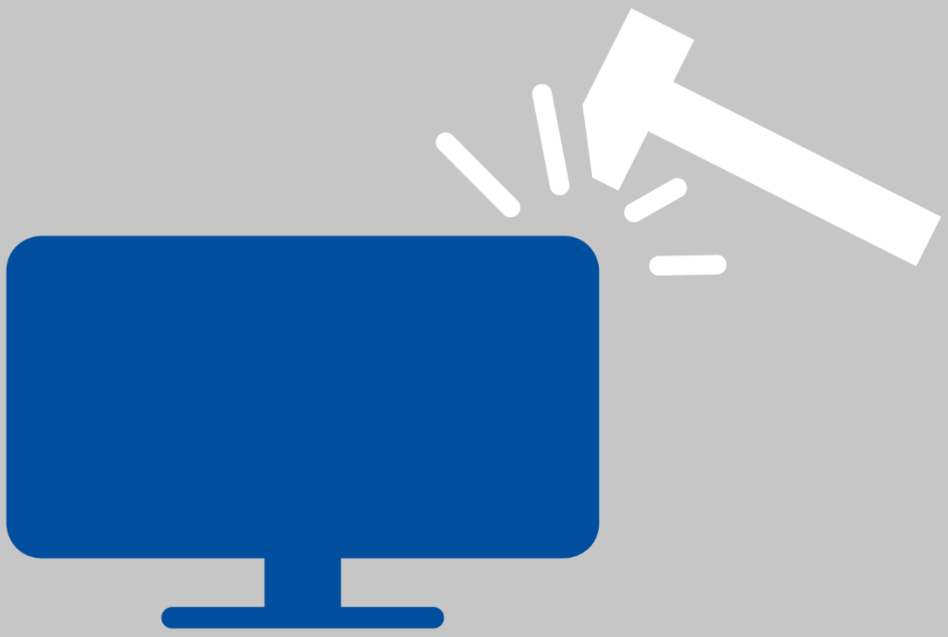
side, machine learning models can be the target of adversarial attacks that aim to confuse ML models with malicious data points crafted at inference time. These attacks are growing and represent a major threat in ML or AI domains[464].

In addition, model stealing or extraction aims to reconstruct a black-box model or extract data from it[465]. In this context, membership inference attacks aim to recover the training set from a deployed ML model. A seminal work in 2017 allowed the presence of a specific data point to be inferred in the training set based on model predictions only[466]. This attack was later executed on large models,[467] introducing major privacy and economic risks.

6.1.8 Additional trends

- The number of data breaches without root causes is increasing, making 'unknown' root cause the largest attack vector in Q1 2022[468]. This number has increased by 190% since 2020 in the USA,[469] a 40% increase overall[470].
- Cybercriminals target specific data types rather than mass data acquisition, causing a decrease in the number of victims (-5% in 2021). However, the number of consumers with data that was compromised multiple times remains very high[471].
- According to IBM, 2021 had the highest average cost of USD 4.24 million, with the additional impact brought about by remote working and cloud migration[472]. Compromised credentials were the most important vector of data breach.
- Security AI produced the biggest cost mitigating effect[473].
- As discussed in chapter 3, ransomware has changed the shape of data breaches and is asking enterprises to modify their responses[474].
- Cloud migration continuously increased in the last few years and is now moving to multi-cloud strategies, but data management and protection are still lagging[475]. According to Thales: *there is a lack of maturity in cloud data security with limited use of encryption, perceived or experienced multi-cloud complexity and a rapid growth of enterprise data.*
- According to Thales, there is a clear correlation between investment in compliance and resilience against data breaches, meaning that *improved compliance leads to better security outcomes*[476].
- According to Tenable Research, data breaches continue their sharp increase with over 2.5 times more breaches reported in 2021 than in 2020. This increase comes with a 78% increase in the number of records exposed[477]. The amount of data stolen is said to reach over 260 terabytes with over 1.8 billion files, documents or e-mails.

[464] https://venturebeat.com/2021/05/29/adversarial-attacks-in-machine-learning-what-they-are-and-how-to-stop-them/
[465] https://venturebeat.com/2021/05/29/adversarial-attacks-in-machine-learning-what-they-are-and-how-to-stop-them/
[466] 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.
[467] 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.
[468] https://www.idtheftcenter.org/post/data-breach-increase-14-percent-q1-2022/
[469] https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf
[470] https://www.idtheftcenter.org/post/data-breach-increase-14-percent-q1-2022/
[471] https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf
[472] Cost of a data breach report, IBM, https://www.ibm.com/security/data-breach
[473] Cost of a data breach report, IBM, https://www.ibm.com/security/data-breach
[474] 2022 Thales Data Threat Report
[475] 2022 Thales Data Threat Report
[476] https://mb.cision.com/Public/20506/3530950/b55a39d9e52a4074.pdf
[477] Tenable's 2021 Threat Landscape Retrospective



7. 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 has a significant role in the cybersecurity threat landscape[478] [479]. 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 component of the network infrastructure[480].

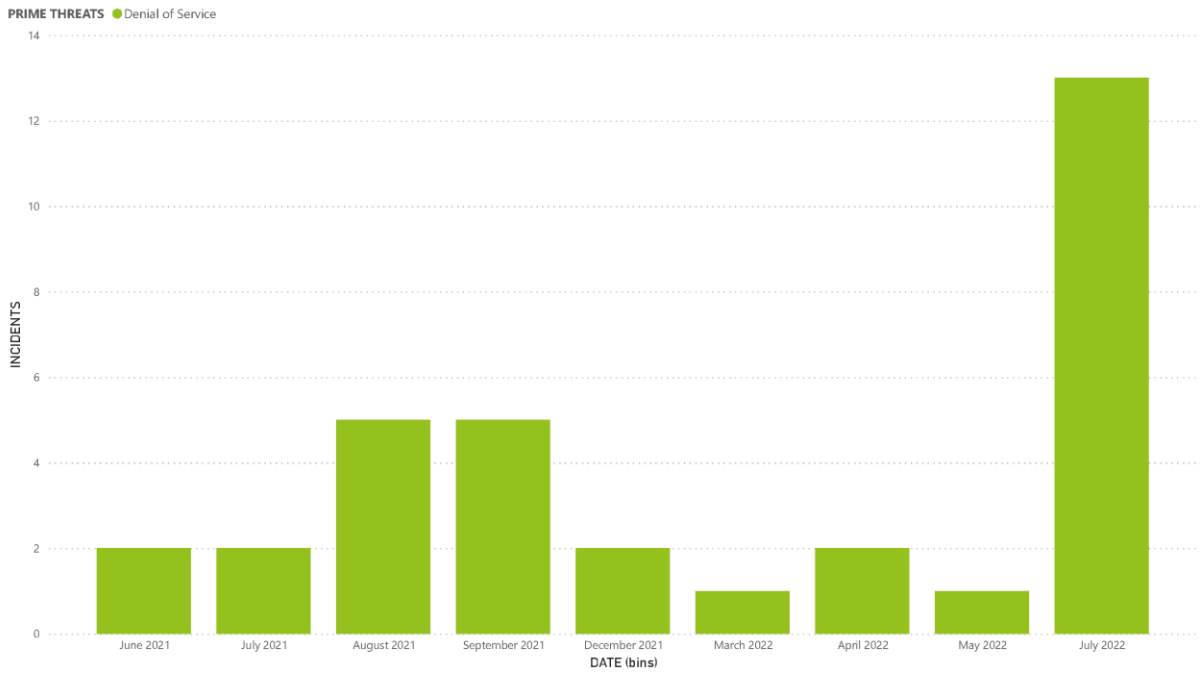
DDoS attacks can be built on a web-based attack (see chapter 8), which are often distributed through web applications, and use cloud as a primary threat vector. For instance, web-based attacks can be adopted to build a botnet on the cloud that is then used to carry out a denial of service attack aimed at making a system unavailable[481].

While defence mechanisms and strategies are becoming more robust, malicious actors are also advancing their technical skills, better adapting to the new norm introduced by COVID-19. In this context, Ransom Denial of Service (RDoS) mixes 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 and the Armada Collective carrying out these campaigns) analyse target businesses to find those with weak and vulnerable systems. They then threaten these businesses by sending an extortion letter asking for a ransom to not attack the system[482] [483]. The simplicity of RDoS attacks is at the basis of their adoption. Thanks to Cybercrime as a Service (CaaS) tools, launching a RDoS attack is becoming increasingly simpler while it is still difficult to spot its origin. Spreading a malware or ransomware instead requires an important effort in terms of time and planning[484].

During this reporting period, we again observed a large number of incidents involving Denial of Service. We saw a rise in July 2022, a month that featured many DoS attacks. These peeked with the largest ever recorded attack launched against a European customer on the Prolexic platform[485], using globally distributed attack traffic that reached its pinnacle at 853.7 Gbps and 659.6 Mbps over 14 hours.

[478] Federal Office for Information Security (BSI), The State of IT Sec in Germany, September 2020
[479] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020
[480] CISA, Understanding Denial-of-Service Attacks, November 2019. https://www.uscert.gov/ncas/tips/ST04-015
[481] ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
[482] 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/
[483] CloudBric, DDoS Extortion Campaigns (Ransom DDoS, or RDoS) To Watch Out For, https://www.cloudbric.com/blog/2020/11/ddos-rdos-extortion-ransomware-campaign/
[484] 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
[485] https://www.akamai.com/blog/security/largest-european-ddos-attack-ever

Figure 15: Time series of major Incidents observed by ENISA (July 2021-June 2022)



7.1 TRENDS

DDoS is one of the most critical threats to IT systems, targeting their availability by exhausting resources, causing decreased performance, loss of data and service outages[486]. DDoS recently moved to mobile and sensor-based scenarios, where the availability of devices and sensors is decreased by speeding up battery consumption. DDoS attacks have maintained a stable shape over the years, while some interesting points on their evolution may be noted.

In 2021-22, while the COVID-19 pandemic still had an important impact on DDoS, the Russia-Ukraine cyberwarfare monopolised and influenced the shape of DDoS like never before. DDoS threats are finally becoming the fifth dimension of warfare, after battles in the air, sea, land and even space.[487] The threats and levels of extortion exploded, moving DDoS towards being a state-sponsored attack. In this context, cloud computing is increasingly being used as a threat vector for DDoS attacks on the one side, and as a primary target of the attacks on the other side[488].

7.1.1 Attacks are getting larger and more complex

The trend in the increasing dimension and complexity of DDoS attacks was also confirmed this year. According to NETSCOUT[489] and its recent threat intelligence report: *the reality is that attackers are constantly innovating and adapting new techniques, including the use of server-class botnets, DDoS-for-Hire services, and the increased use of direct-path attacks that continually perpetuate the advancement of the threat landscape.*

According to F5Labs,[490] the size of DDoS attacks increased remarkably over 2021 culminating in many attacks in the order of Tbps (with the largest identified by F5Labs in November 2021 at around 1.4Tbps targeting an ISP/hosting

[486] 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
[487] Vova Kamenker, DDoS Threats: The Fifth Dimension of Warfare, September 2021, https://blog.mazebolt.com/ddos-threats-the-fifth-dimension-of-warfare
[488] Tom Emmons. 2021: Volumetric DDoS Attacks Rising Fast, March 2021, https://blogs.akamai.com/2021/03/2021-volumetric-ddos-attacks-rising-fast.html
[489] https://www.netscout.com/threatreport
[490] 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

customer). By analysing the frequency of attacks by their size, though the majority of attacks were small, it emerges that attacks between 1 and 3 Gbps are preferred over smaller attacks. Similarly, attacks between 10 and 30 Gbps are more popular than attacks between 6 and 10 Gbps. F5Labs also observed an increase in the number of application (+2.2%) and protocol (+4,7%) attacks, with a decrease in volumetric attacks (-6.9%). This exemplifies the increased complexity of the attacks; protocol and application attacks are in fact more challenging to defend against, since they can appear as genuine application traffic. They contributed to the increase in the cardinality of attacks based on TCP, which is mandatory for attacking complex protocols and applications[491].

Multi-vectored attacks are prevalent[492] and their frequency in the last year was greater than single-vectored attacks.[493] The above mentioned 1.4Tbps attack targeting an ISP/hosting customer in November 2021 was a combination of DNS reflection and HTTP GET requests.

Cloudfare recorded one of the largest HTTP attacks peaking at 17.2M rps (requests per second) and targeting a customer in the financial services industry[494]. It was based on the Meris botnet[495] [496] [497]. Cloudfare also observed, in November 2021, the largest DDoS attack that peaked just below 2 Tbps. The attack was multi-vector combining DNS amplification attacks and UDP floods, and lasted one minute. It was based on a botnet running a variant of the original Mirai code on IoT devices and unpatched GitLab instances[498]. Similarly to F5Labs, Cloudfare observed that while the majority of attacks was small, there were also larger attacks. Terabit-strong attacks increased in the second half of 2021[499].

According to Neustar[500], 2021 was the largest and most intense DDoS year, with the longest attacks.

7.1.2 DDoS attacks are increasingly moving towards mobile networks and IoT

As already discussed in ETL 2021: *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 protection. Devices are simple to corrupt, often coming with misconfigurations (e.g. weak passwords)[501]. At the same time, the increasing complexity of these mobile systems make users' shortage of 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 also have the potential to threaten the safety of 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 was also confirmed in the last reporting period when DDoS attacks were often launched from compromised servers or consumer devices, such as Internet-of-Thing (IoT) products and broadband routers[502]. This is often caused by delays by smart device owners in updating and patching devices[503]. For instance, the Mozi Botnet still uses vulnerabilities discovered eight years ago and compromises unpatched devices building botnets with hundreds of thousands of bots. This was also confirmed by an experiment at the US National Institute of Standards and Technology (NIST), where NIST researchers observed that 'admin' (username) and '1234' (password) was the most common combination used in attacks against IoT[504].

[491] Mitre Att&ck, Endpoint Denial of Service, https://attack.mitre.org/techniques/T1499/
[492] https://azure.microsoft.com/en-us/blog/azure-ddos-protection-2021-q3-and-q4-ddos-attack-trends/
[493] 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
[494] https://blog.cloudflare.com/cloudflare-thwarts-17-2m-rps-ddos-attack-the-largest-ever-reported/
[495] https://blog.cloudflare.com/ddos-attack-trends-for-2021-q3/
[496] https://portswigger.net/daily-swig/meris-botnet-leverages-http-pipelining-to-smash-ddos-attack-records
[497] Neustar, Cyber Threats & Trends Report: Defending Against A New Cybercrime Economy
[498] https://blog.cloudflare.com/cloudflare-blocks-an-almost-2-tbps-multi-vector-ddos-attack/
[499] https://blog.cloudflare.com/ddos-attack-trends-for-2021-q4/
[500] Neustar, Cyber Threats & Trends Report: Defending Against A New Cybercrime Economy
[501] Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020, https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2020
[502] 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
[503] ESET Threat Report, T2 2021
[504] ESET Threat Report, T3 2021

Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

TrendMicro also observed that escalated cyberattacks have compromised and hijacked smart devices at the core of the attacks[505]. Attacks increasingly target smart cities as well as fleets of connected cars possibly causing catastrophic events[506].

NETSCOUT observed that the increase in IoT botnets was accompanied by the involvement of high-powered servers in larger botnets[507]. Focusing on IoT botnets, compromised IoT devices are orchestrated under a common command-and-control infrastructure. This trend is predicted to increase due to multigigabit consumer wireline and wireless 5G broadband internet connectivity. It is especially due to weak configurations and little to no security protection of IoT devices.

7.1.3 DDoS and cyberwarfare

The DDoS landscape, similar to what happened for COVID-19 after 2019, was affected by the geopolitical changes introduced by the Russia-Ukraine war that began 24 February 2022 when a coordinated set of attacks was launched against Ukrainian government and financial institutions. A significant part of the DDoS-related attacks in the reporting period concerned this event and involved actors at different layers, from states to simple users devoting their resources to the cyberwar. It is important to note that state-sponsored attacks are not only directly bound to the war, but had been raised well before the war began. For instance, F5Labs reported a number of politically motivated DDoS attacks in various countries in Q3 2021. In early and mid-July, unknown actors flooded the security agencies of Russia and Ukraine with junk traffic[508]. These attacks also involved other countries such as, in mid-August, when attackers tried to stop users from accessing the web resources of the Philippine human rights organisation Karapatan. At the end of August, linked to the September elections of the Bundestag in Germany, the website of Germany's Federal Returning Officer was attacked.

Cloudfare in its document 'DDoS Attack Trends for 2022 Q1'[509] discussed the important role of the Russian and Ukrainian war in shaping the current status of DDoS. The most targeted industries in the two countries were online media and broadcast media, followed by the internet industry, cryptocurrency and retail. Attacks on Russian cryptocurrency companies originated in Ukraine or the USA first and then Russia. HTTP DDoS attacks on Russian companies originated from Germany, the USA, Singapore, Finland, India, the Netherlands and Ukraine. Attacks on Ukraine targeted broadcast media and publishing websites and originated from many countries with most of the traffic coming from the USA, Russia, Germany, China, the UK and Thailand.

Both sides of the war were the target of substantial attacks. Ukraine declared itself to be the target of cyberattacks including DDoS, which according to the government were *on a completely different level*[510] [511]. Russia's Ministry of Digital Development and Communications declared that the volume of DDoS attacks in the country had become *unprecedented*[512]. A game *play for Ukraine* was used to launch DDoS attacks against Russian web sites[513]. This increasing involvement of users in DDoS however opened the door to risks for users when tools supposed to be used to attack Russian web sites were instead infostealers[514].

7.1.4 DDoS and Covid-19

In the last few years, the COVID-19 pandemic has been used as an amplifier of existing threats to exploit the uncertainties characterising the pandemic[515]. According to ETL 2021, during COVID-19, RDoS or extortion by DDoS had a rise starting July/August 2020, mostly targeting businesses in the e-commerce, finance and travel sectors on a

[505] TrendMicro, IoT Security Issues, Threats, and Defenses, July 2021
https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/iot-security-101-threats-issues-and-defenses
[506] Numaan Huq, Craig Gibson, Vladimir Kropotov, Rainer Vosseler, TrendMicro, In Transit, Interconnected, At Risk - Cybersecurity Risks of Connected Cars, February 2021, https://www.trendmicro.com/vinfo/us/security/news/internet-of-things/in-transit-interconnected-at-risk-cybersecurity-risks-of-connected-cars
[507] ISSUE 8: FINDINGS FROM 2ND HALF 2021 NETSCOUT THREAT INTELLIGENCE REPORT
[508] https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-ddos-attack-trends
[509] https://blog.cloudflare.com/ddos-attack-trends-for-2022-q1/
[510] https://www.bbc.com/news/technology-60500618
[511] https://www.netscout.com/blog/asert/ddos-threat-landscape-ukraine
[512] https://www.nbcnews.com/tech/security/hacktivists-new-veteran-target-russia-one-cybers-oldest-tools-rcna20652
[513] https://www.fastcompany.com/90732766/ddos-play-for-ukraine-russian-cyberattack
[514] https://threatpost.com/malware-posing-russia-ddos-tool-bites-pro-ukraine-hackers/178864/
[515] Europol, 'Internet Organised Crime Threat Assessment 2020 (IOCTA)'.
https://www.europol.europa.eu/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2020.pdf
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

global scale[516]. This trend continues to materialize in 2021-22. For instance, sites used to fight COVID-19 are still a primary target of DDoS. In August, the vaccination registration portal in the Philippines was hit by a DDoS attack[517], while in September it was the turn of the Dutch website CoronaCheck distributing QR codes required to visit cafes and cultural sites[518]. Also, Italian and Bulgarian COVID-19 related services have been hit by DDoS attacks, with an overall *increase in government agencies, including those in the EU, being the victim of DDoS extortion attacks linked to government Covid-19 protocols, affecting critical service availability.*

7.1.5 Ransom Denial of Service (RDoS)

Ransom Denial of Service (RDoS) is the new frontier of denial of service attacks. 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 or *ii)* extortion first. Point *i)* considers a scenario where a DDoS attack is implemented and a ransom is requested to stop it. Point *ii)* considers a scenario where an extortion letter and a proof in the form of a small-scale DoS is sent with a request to pay a ransom. RDoS attacks are even more dangerous than traditional DDoS since it can be completed even if the attacker does not have enough resources[519]. RDoS is a complex attack that mixes several approaches and techniques such as Denial of Service, Ransomware, identity spoofing, to name but a few[520].

EUROPOL reported in its IOCTA 2021[521] the comeback of DDoS attacks followed by ransom demands, with an increase in high-volume attacks compared to the previous year. RDoS targeted ISPs, financial institutions, and small and medium-sized businesses (SMBs), and its success is due to the spread of online services. In addition to traditional double-extortion methods by exfiltrating victims' data and threatening to publish it, we observe an enlargement of the target boundaries that often involve clients, business partners and employees of the victim. RDoS is then used to force victims into complying with the ransom request threatening them at several levels, such as, denial of service, publication of confidential data and the involvement of associated partners. A step further consists in the migration from a one-time ransom to a request for 1 BTC a day in exchange for 'protecting' the victim company from their attacks[522].

We are then moving from double-extortion to quadruple-extortion tactics[523] [524] [525] [526]. 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 affected organisation*[527] [528]. In quadruple extortion attacks,[529] *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 2021, the names and proof of compromise for 2,566 victims were publicly posted on ransomware leak sites, an 85% increase compared to 2020[530].

RDoS often involves identity spoofing,[531] where cybercriminals used the identity of APT groups to force their targets into paying the ransom. As an example, in Q3 2021 a wave of attacks targeted VoIP providers which affected companies in Britain, Canada and the USA. The attackers claimed to be part of the ransomware group REvil before issuing their request for ransom. No evidence was released to confirm the group's identity as REvil.

[516] ETH Zürich, Center for Security Studies (CSS), The Evolving Cyber Threat Landscape during the COVID Crisis, 2020
[517] https://www.manilatimes.net/2021/08/14/opinion/columns/cyberhackers-sabotaging-manilas-vaccination-program/1810897
[518] https://nltimes.nl/2021/09/26/saturday-night-ddos-attack-coronacheck-system-resolved
[519] CloudBric, DDoS Extortion Campaigns (Ransom DDoS, or RDoS) To Watch Out For, https://www.cloudbric.com/blog/2020/11/ddos-rdos-extortion-ransomware-campaign/
[520] Neustar, Pay Or Else: DDoS Ransom Attacks
[521] https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf
[522] https://threatpost.com/massive-meris-botnet-embeds-ransomware-notes-revil/178769/
[523] Unit42_Ransomware_Threat_Report_2022_1650614560
[524] IBM_X_Force_Threat_Intel_Index_2022
[525] ISSUE 8: FINDINGS FROM 2ND HALF 2021 NETSCOUT THREAT INTELLIGENCE REPORT
[526] The Global Economic Forum, The Global Risks Report 2022 17th Edition, 2022 https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
[527] IBM_X_Force_Threat_Intel_Index_2022
[528] BleepingComputer, 'US and Australia warn of escalating Avaddon ransomware attacks', https:// www.bleepingcomputer.com/news/security/us-andaustralia-warn-of-escalating-avaddon-ransomwareattacks/ , 2021
[529] The Global Economic Forum, The Global Risks Report 2022 17th Edition, 2022 https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
[530] Unit42_Ransomware_Threat_Report_2022_1650614560
[531] https://www.europol.europa.eu/cms/sites/default/files/documents/internet_organised_crime_threat_assessment_iocta_2021.pdf
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

RDoS can also be used as a mechanism for compromising the systems of a target using malware[532]. In Q3 2021, DDoS was used as a tool for intimidation, where the targets received an e-mail claiming they were used to execute DDoS attacks and could face legal problems. The mail included a link to a cloud directory where details about the incidents could be accessed, but instead it contained the BazarLoader malware loader.

According to Cloudfare in Q4 2021, RDoS attacks increased by 29% year-on-year and 175% quarter-on-quarter[533]. This percentage was retrieved by asking customers of Cloudfare that received a DDoS attack whether they also received a ransom note. These numbers decreased sharply in Q1 2022 probably due to the war between Russia and Ukraine which monopolised the denial-of-service domain[534].

7.1.6 Shift from UDP-based to TCP-based attacks

Following the trend on the increase of protocol and application attacks, 2021 saw a sharp increase in TCP-based attacks[535]. Still, being stateless, UDP is still the favoured transport protocol supporting IP address hiding and simple reflection attacks[536]. However, in 2021, TCP has been used for 27% of attacks, an increase of 10%. As stated already, this is strongly coupled with more complex protocol and application DDoS attacks, which often builds on the TCP protocol.

This attack, defined in theory at the University of Maryland and University of Colorado Boulder, aims to weaponize middleware in providing TCP reflected amplification[537] [538]. According to researchers explaining this attack, *TCP-based amplification is possible and can be orders of magnitude more effective than the well-known UDP-based amplification*. Beginning of 2022, Akamai Security Researchers detected and analysed TCP reflection attacks, peaking at 11 Gbps at 1.5 Mpps[539].

On average, TCP DDoS attacks almost doubled in 2021 compared with 2020 and accounted for 27% of all attacks[540].

7.1.7 Cloud and DDoS

The rapid adoption of cloud computing and its movement towards edge computation increased the attack surface and the opportunities for cybercriminals[541]. 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. Cloud brings a false sense of security, reducing the effort spent by organisations in monitoring cloud infrastructures and platforms with respect to their counterparts on premises. As a result, cybercriminals are targeting cloud services and take advantage of deficiencies in cloud assets and configuration management.

On the other side, 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[542]. Public APIs can be used as attack vectors to gain access to individual endpoint devices. For instance, a cloud-centric toolset from TeamTNT installed a bot named *Tsunami* onto compromised systems to abuse public-facing infrastructures to execute, among others, distributed denial-of-service attacks.

7.1.8 DDoS attacks spread

7.1.8.1 Geographical Spread

[532] https://www.bleepingcomputer.com/news/security/fake-dmca-and-ddos-complaints-lead-to-bazaloader-malware/
[533] https://blog.cloudflare.com/ddos-attack-trends-for-2021-q4/
[534] https://blog.cloudflare.com/ddos-attack-trends-for-2022-q1/
[535] 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
[536] https://azure.microsoft.com/en-us/blog/azure-ddos-protection-2021-q3-and-q4-ddos-attack-trends/
[537] https://www.usenix.org/system/files/sec21fall-bock.pdf
[538] https://portswigger.net/daily-swig/nation-state-threat-how-ddos-over-tcp-technique-could-amplify-attacks
[539] https://www.akamai.com/blog/security/tcp-middlebox-reflection
[540] 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
[541] Accenture-2021-Cyber-Threat-Intelligence-Report fornito da enisa
[542] Accenture-2021-Cyber-Threat-Intelligence-Report Volume 2, https://www.accenture.com/_acnmedia/PDF-173/Accenture-Cyber-Threat-Intelligence-Report-Vol-2.pdf
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

The geographical spread of DDoS attacks in 2021-22 shows the following highlights [543].

- The USA and China confirm the trends of past years and are at the top of the rankings as target countries for DDoS attacks. Q3 and Q4 2021 saw a sharp increase for Hong Kong that took the second spot of the rankings.
- Germany, the United Kingdom, France and Canada have been in the top places for the whole period.
- The USA, Netherlands and Germany account for the highest distribution of botnet C&Cs, accounting for 48.49%, 9.17%, and 8.69% of botnet C&Cs respectively on average.

Cloudfare analysed the geographical spread of DDoS distinguishing between application (L7) and network (L3/L4) layers, and considering the percentage of attack traffic to total traffic[544] [545] [546].

- **Application Layer:** China and the USA are often in the top spots as both sources and targets of application-layer attacks. The only exceptions were: *i)* Q3 2021, where attacks on UK-based and Canada-based companies jumped to be the second and third most targeted countries, *ii)* Q4 2021, where Canada took the second spot and China the eight spot as the most targeted countries.
- **Network Layer:** DDoS attacks increased by 44% worldwide in Q3 2021, with the Middle East and Africa experiencing an increase in attacks of approx 80% with Morocco in the top spot as a source of network layer attacks, closely followed by Asian countries (e.g. Philippines, Vietnam). In Q4, Moldova hit the top spot with the highest percentage of network-layer DDoS activity.

7.1.8.2 Industry sector spread

F5Labs observed that the most attacked industry sector over 2021 was the banking, financial services, and insurance (BFSI) sector with over 25% of the attacks[547]. Telecommunications and technology were in the second and fourth spots respectively, while education is still a preferred sector at third place and was hit particularly hard during September and January (beginning of new terms). When attacks are divided by DDoS type, F5Labs found that telecommunications and education are the most targeted sectors by volume of attacks, while other sectors including BFSI show a more balanced picture. Considering the largest attacks, ISP/Hosting takes the lead followed by recreation, BFSI and technology. Recreation is the sector with the largest average attack size. Neustar also identifies telecommunications and financials as preferred targets for DDoS, as well as gaming, ecommerce and healthcare pulled by the transition to online technology during the pandemic[548].

Cloudfare also analysed the industry sector spread of DDoS attacks at the application (L7) layer[549] [550] [551]. Attacks on computer software, gaming/gambling, IT and Internet companies increased by an average of 573% in Q3 2021, where attackers targeted VoIP service providers with massive DDoS attack campaigns. The top targeted application layer sectors were technology (including software, internet and information technologies) and gaming in Q3 2021, manufacturing, gaming and business services in Q4 2021, and consumer electronics, online media and computer software in Q1 2022.

7.1.9 Attack vectors

F5Labs classifies DDoS attacks into three categories, i.e. volumetric, application and protocol, and analyses their frequency[552]. F5Labs identified simple UDP (non-reflection) attacks as the DDoS method with the highest frequency in 2021. However, although volumetric attacks are still more than a half of all attacks (59%), the third, fourth, and fifth most common attack types were protocol- and application-based. The largest attack of 1.4 Tbps attack observed by

[543] https://blog.cloudflare.com/ddos-attack-trends-for-2021-q3/
[544] https://blog.cloudflare.com/ddos-attack-trends-for-2021-q3/
[545] https://blog.cloudflare.com/ddos-attack-trends-for-2021-q4/
[546] https://blog.cloudflare.com/ddos-attack-trends-for-2022-q1/
[547] https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-ddos-attack-trends
[548] Neustar, DDoS DISRUPTION IMPACTS - The Need for Always-On Security
[549] https://blog.cloudflare.com/ddos-attack-trends-for-2021-q3/
[550] https://blog.cloudflare.com/ddos-attack-trends-for-2021-q4/
[551] https://blog.cloudflare.com/ddos-attack-trends-for-2022-q1/
[552] https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-ddos-attack-trends
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

F5Labs was based on HTTP(S) denial-of-service techniques, the less frequent form of DDoS attack, and involved DNS reflection and HTTPS GET requests.

In 2021, F5Labs also observed that UDP was the most used transport protocol, since it is stateless and easily supports reflection attacks, though TCP increased by 10% to be used for 27% of attacks[553].

On the contrary, Cloudfare reported SYN floods as the most favourite method of attack, with UDP showing a peak in Q4 2021, still confirming the increase in TCP-based attacks.

7.1.10 VoIP providers observed an increased amount of DDoS extortion attacks

Voice providers are increasingly becoming a preferred target for DDoS cybercriminals[554] [555]. According to NETSCOUT[556], DDoS extortion and RDoS attacks to VoIP Services increased and reached several SIP/RTP VoIP operators. First, the attack targeted retail and wholesale VoIP providers in the UK then it moved to VoIP operators in Western Europe and North America. One VoIP service provider reported $9M-$12M in revenue losses due to DDoS attacks.

7.1.11 Additional trends

- As noted in ETL 21, cybercrime-as-a-service tools were increasingly used as facilitators for reducing the effort needed to manage high-volume and complex attacks, making DDoS adaptive, lightweight and heterogeneous. This was confirmed in 2021-22 when, according to NETSCOUT, DDoS-for-Hire Free-for-All services were spreading with a free account to launch DDoS attacks[557]. Users could test basic DDoS attacks and then pay to increase attack power.
- Artificial Intelligence is permeating our systems and is often used as a means to increase the security and safety of our systems, detect anomalies in IT systems and automatically configure IT assets. It is quickly becoming a target for cybercriminals attacking the logic within AI models. A successful attack that reverses the decision made by an AI model permits the cybercriminals to hide their activities, on one side, or even produce a DDoS attack, on the other side[558].
- F5Labs observed an increase in the number of DDoS attacks in Q3 2021 both with respect to Q3 2020 and Q2 2021 [559]. Verizon counted DDoS as 46% of the total number of attacks[560].
- According to NETSCOUT, in the second half of 2021, cybercriminals launched approximately 4.4 million DDoS attacks.
- CVE-2021-45105 (log4j vulnerability) facilitates cybercriminals in executing a denial of service attack via infinite recursion when the application encounters inputs with recursive lookups[561].

[553] https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-ddos-attack-trends
[554] https://news.lumen.com/2022-02-17-Lumen-scrubbed-more-than-20,000-enterprise-DDoS-attacks-in-2021
[555] Neustar, Cyber Threats & Trends Report: Defending Against A New Cybercrime Economy
[556] ISSUE 8: FINDINGS FROM 2ND HALF 2021 NETSCOUT THREAT INTELLIGENCE REPORT, https://www.netscout.com/sites/default/files/2022-03/ThreatReport_2H2021_WEB.pdf
[557] ISSUE 8: FINDINGS FROM 2ND HALF 2021 NETSCOUT THREAT INTELLIGENCE REPORT, https://www.netscout.com/sites/default/files/2022-03/ThreatReport_2H2021_WEB.pdf
[558] Acronis_Cyber_Threat_Report_2022_1649135585
[559] https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-ddos-attack-trends
[560] The Global Economic Forum, The Global Risks Report 2021 16th Edition, 2021 http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf
[561] Accenture-2021-Cyber-Threat-Intelligence-Report

8. THREATS AGAINST AVAILABILITY: INTERNET THREATS

Internet use and the free flow of information is impacting the lives of all Europeans. For many people, access to the internet has become a basic necessity for working, studying and exercising freedom of expression, political freedom and for social interaction. This chapter covers threats that impact the availability of the internet. DDoS is covered in a separate section due to its individual impact in the threat landscape.

8.1 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 relinquish control of the networks and then physically rerouted mobile and internet traffic over Russian-owned network infrastructure. This allows Russia to block access to social media, prevent information leakage, have more control over the narrative surrounding the war and perform surveillance activities.

Ukraine cellular networks are being 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[562,563]. This has led Ukraine's Ministry of Digital Transformation to seek alternative means to ensure the operations of the country's critical infrastructure, e.g. via the use of satellite internet systems.[564]

8.2 ACTIVE CENSORING

Since February 2022, around 3,000 websites have been blocked in Russia. The blocks are related to the Russian invasion of Ukraine. 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[565].

OONI Probe is a software designed to measure various forms of internet censorship and is run by volunteers in around 160 countries monthly. The data is collected and published in real-time. Data analysis of Russian traffic shows that the most common method used for censorship (in terms of the number of ISPs relying on it) is the injection of a RST packet following the initial phase of the TLS handshake. The second most common method is DNS-based filtering. Since December 2021, Tor had also been subject to blocking. While still accessible on most networks in Russia, data of 15 out of 65 tested AS networks indicate that Tor is being blocked[566].

Europe, in turn, also announced the suspension of the media broadcasting activities of Sputnik and RT in the EU over disinformation on Ukraine[567]. While the decision is related to the media broadcasting activities of RT, some European countries, as well as social media platforms, are also blocking access to the websites of Russian outlets.

562 https://www.nytimes.com/interactive/2022/08/09/technology/ukraine-internet-russia-censorship.html
563 https://www.reuters.com/world/europe/russia-reroutes-internet-traffic-occupied-ukraine-its-infrastructure-2022-05-02/
564 https://www.commsupdate.com/articles/2022/08/23/starlink-delivered-more-than-13000-satellite-terminals-to-ukraine/
565 https://www.top10vpn.com/research/websites-blocked-in-russia/
566 https://ooni.org/post/2022-russia-blocks-amid-ru-ua-conflict/
567 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/
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

8.3 STATE-OWNED CERTIFICATE AUTHORITY

Following the war in Ukraine, Russia was sanctioned by many western governments. Sanctions on financial institutions prevented Russian users from renewing their TLS certificates. Consequently many websites began presenting expired certificates resulting in untrusted connections for the user. The Russian Ministry of Digital Development began providing a free alternative for legal entities in Russia to create a certificate[568].

Certificate authorities issue certificates and are, when vetted, considered trusted parties. When the state owns this certificate authority (CA), it becomes straightforward for them to perform HTTPS traffic interception and man-in-the-middle attacks on its citizens. Due to the ongoing attacks and the global lack of trust in Russia as a partner, the CA is only trusted on two browsers, Yandex and Atom. Any other web browser will warn or prevent a user from accessing the website. For end-users in Russia, the limitations on purchasing certificate renewals have caused a negative impact on their internet security and privacy.[569]

8.4 BGP HIJACKING

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 its 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 cause a significant impact as they may spread beyond the original target area. As an erroneous announcement of ownership can also result from a misconfiguration, telling whether a BGP hijacking incident is indeed malicious or whether it is unintentional is not always straightforward.

BGPStream is an open-source software framework for live and historical BGP data analysis[570]. In 2021, BGPStream collectors identified approximately 775 incidents categorised as 'Possible Hijacks'. Compared to 2020, there were fewer incidents in 2021[571]. Other data suggest that in the last quarter of 2021, the most significant number of hijacks took place. The results for Q1 2022 are a bit lower but comparable to Q4 2021[572].

In February 2021, hackers stole almost two million dollars from the South Korean cryptocurrency platform *KLAYswap*. They launched a BGP hijack against the server infrastructure of one of its providers, KakaoTalk, advertising the ownership of one of its websites. Through the hijacking that lasted two hours, the attackers served a malicious JavaScript SDK file. When a transaction on the platform was detected, the added code hijacked the funds and sent the assets to the wallet of an attacker[573].

In March 2022, Twitter was briefly hijacked through a Russian ISP. It was believed to be the consequence of a misconfiguration[574] [575].

In July 2022, Apple was also hijacked by a Russian ISP, Rostelecom. Apple only announces their larger 17.0.0.0/9 block. As the ISP announced a smaller block 17.70.96.0/19, this route got hijacked. To regain control, Apple started announcing an even smaller block, 17.70.96.0/21, to direct traffic to the right AS. It took 12 hours before the wrong routes were corrected[576].

[568] https://www.gosuslugi.ru/tls
[569] https://www.bleepingcomputer.com/news/security/russia-creates-its-own-tls-certificate-authority-to-bypass-sanctions/
[570] https://bgpstream.caida.org/
[571] https://www.manrs.org/2022/02/bgp-security-in-2021/
[572] https://habr.com/en/company/qrator/blog/663250/
[573] https://therecord.media/klayswap-crypto-users-lose-funds-after-bgp-hijack/
[574] https://bgpstream.crosswork.cisco.com/event/288327
[575] https://isc.sans.edu/diary/BGP+Hijacking+of+Twitter+Prefix+by+RTComm.ru/28488
[576] https://www.manrs.org/2022/07/for-12-hours-was-part-of-apple-engineerings-network-hijacked-by-russias-rostelecom/
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

8.5 BGP WITHDRAW

As BGP routes are announced, they are also constantly being withdrawn. In October 2021, Facebook accidentally disconnected its entire backbone because of an incorrect configuration. When the DNS servers noticed the network backbone was no longer talking to the internet, they stopped sending out BGP advertisements, instead withdrawing them[577]. The outage lasted about seven hours and also impacted Instagram and WhatsApp.

In June 2022, Cloudflare endured a similar incident where a BGP configuration change caused a prefix to withdraw, rendering 19 of its data centres inaccessible. In less than one hour, all data centres were brought online again[578]. As many websites are using Cloudflare, the incident affected many users.

8.6 ADOPTION OF RPKI REMAINS SLOW

Resource Public Key Infrastructure (RPKI)[579] is a way to sign certificates that will attest to holding the IP address space and AS number. The framework can help to better protect the BGP infrastructure against BGP Hijack attacks. It provides an out-of-band method to help manage which network can announce which route. While RPKI is not new, adoption still remains low. In 2021, Comcast, and in 2022, KPN and Orange joined the list of operators successfully implementing RPKI. While the list of safe ISP and transit providers is growing, the road to full adoption is still long[580]. From January 2021 to January 2022, RPKI adoption grew from 28% to 34,7%[581].

[577] https://engineering.fb.com/2021/10/04/networking-traffic/outage/
[578] https://blog.cloudflare.com/cloudflare-outage-on-june-21-2022/
[579] https://tools.ietf.org/html/rfc6480
[580] https://isbgpsafeyet.com/
[581] https://www.manrs.org/2022/02/bgp-security-in-2021/

9. DISINFORMATION-MISINFORMATION

Digital platforms are nowadays the norm for news and media. Social sites, news and media outlets and even search engines are now sources of information for many people. Due to the nature of how these sites operate, which is by attracting people and generating traffic to the sites, the information that generates more viewers is usually the one promoted, sometimes without it being validated. Topics of the day, such as the Russia and Ukraine conflict, have generated a lot of stories that brought enormous attention. The differences between wrong or purposely falsified information are due to different motives. This is where the definitions of misinformation[582] and disinformation[583] come into play.

Cloud computing, AI tools and AI algorithms support malicious actors in fabricating malicious information. This success has both technical and social foundations, and provides state and non-state actors with powerful channels and tools for fabricating and distributing disinformation[584] [585] [586]. The above platforms and services also give malicious actors the ability to experiment, monitor, iterate and optimise the impact of disinformation campaigns[587]. These campaigns are usually the first step before launching other attacks, such as phishing, social engineering or malware infection.

For example, a 2022 study from GlobalData estimated 10% of active accounts on Twitter are posting spam content[588]. Twitter claims the number is well below 5%[589].

An overview of the targets, means and goals of misinformation and disinformation threats is presented in Table 2[590].

Table 2: Disinformation and misinformation: Target, Means and Goals

Target	Means	Goal
People	Disinformation, misinformation, fake news	Reduce perceived honesty and trustworthiness of individuals
Enterprises	Market distortion, misinformation, disinformation, smear campaigns, fake news, propaganda	Affect brand reputation, financial solidity of the company and the trustworthiness of the management
Society	Disinformation, fake news	Induce the inability to distinguish real and fake news, apathy, exhaustion in trying to find the truth, the manipulation and misleading of public-opinion

[582] Misinformation is an unintentional attack, where sharing of information is done inadvertently. Inaccuracy carried by the information is unintentional and could happen for example when a journalist reports wrong information in good faith or reports information by mistake. ENISA ETL 2020
[583] Disinformation is an intentional attack that consists of the creation or sharing of false or misleading information. ENISA ETL 2020
[584] Caroline Jack, 'Lexicon of Lies: Terms for Problematic Information' (New York: Data & Society, 2017), https://datasociety.net/pubs/oh/DataAndSociety_LexiconofLies.pdf .
[585] Europol, EU SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT (SOCTA 2021), 2021
[586] Microsoft FY21 Digital Defense Report
[587] Microsoft FY21 Digital Defense Report
[588] https://www.globaldata.com/media/business-fundamentals/10-twitters-active-accounts-posting-spam-content-says-globaldata/
[589] https://twitter.com/paraga/status/1526237588746403841
[590] ENISA Threat Landscape 2021.
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Any	Sharing of inaccurate information	Make money based on advertising

The flow of disinformation or misinformation and related cyber operations by state and non-state actors is flooding people with the goal of causing uncertainty, apathy towards truth, exhaustion in trying to find it, and fear[591]. It is becoming increasingly clear that disinformation and misinformation are major threats to democracy, open debate, and a free and modern society[592], and that policy-makers should put disinformation at the core of their agenda, while also including security and privacy implications[593]. This scenario has been further boosted and brought to the attention of the research community, governments and public community by the huge wave of disinformation attacks that anticipated and accompanied the war between Russia and Ukraine[594] [595]. In this context, the European Parliament released a resolution on 9 March 2022 on foreign interference in all democratic processes in the European Union, including disinformation (2020/2268(INI))[596].

9.1 TRENDS

Similarly to 2021, the Global Risks Report of the World Economic Forum 2022[597] stated that *the interaction between digitalisation and growing cyberthreats carries intangible consequences as well. The growth of deepfakes and 'disinformation-for-hire' is likely to deepen mistrust between societies, businesses and governments. For example, deepfakes could be used to sway elections or political outcomes.* On top of this, disinformation is one of the dimensions with an adverse impact on public trust in digital systems. It is also affecting the collaboration between states, as cybersecurity becomes a source of divergence rather than of collaboration. According to the Global Risks Perception Survey (GRPS), cross-border cyberattacks and misinformation are identified as those areas where the current state of efforts to mitigate risk are 'not started' or in 'early development'.

According to EU Project CONCORDIA, deep fakes, propaganda, misinformation, and disinformation campaigns are everywhere, designed to lead users into making mistakes. These campaigns directly impact people's daily life and society[598].

Specifically, the following trends are emerging.

9.1.1 Russia-Ukraine war

Disinformation as a method of information warfare dates back to the Cold War and had a revival in the United States after the 2016 election, when Russia was accused to have interfered with the US election process[599]. The central role of disinformation in the cyberwar has been clarified in the war between Russia and Ukraine, where cyberwar moved from cyberattacks to disinformation[600].

Disinformation was being used even before the 'physical' war started as a preparatory activity for Russia's invasion of Ukraine. Mass disinformation campaigns targeted Ukraine before the invasion and continued to escalate during it[601]. As an example, Euronews presented a report by the European Expert Association, lately independently evaluated by the Global Disinformation Index, on different unsubstantiated claims used as a justification for the military action by Russia, such as the news that Ukraine was preparing an attack on the Donbas[602]. In this context, according to Maria Avdeeva, the Ukrainian founder and research director of the European Experts Association, the approach taken to disinformation was to favour *quantity over quality*, trying to exhaust the ability of people to distinguish real information

[591] Microsoft FY21 Digital Defense Report
[592] Microsoft FY21 Digital Defense Report
[593] The Global Economic Forum, The Global Risks Report 2021 16th Edition, 2021 http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf
[594] https://www.washingtonpost.com/politics/2022/03/31/ukraine-war-is-more-about-disinformation-than-cyberattacks/
[595] https://www.dw.com/en/fact-check-the-deepfakes-in-the-disinformation-war-between-russia-and-ukraine/a-61166433
[596] https://www.europarl.europa.eu/doceo/document/TA-9-2022-0064_EN.html
[597] The Global Economic Forum, The Global Risks Report 2022 17th Edition, 2022 https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
[598] D4.3 CONCORDIA
[599] Microsoft FY21 Digital Defense Report
[600] https://www.washingtonpost.com/politics/2022/03/31/ukraine-war-is-more-about-disinformation-than-cyberattacks/
[601] https://www.euronews.com/my-europe/2022/02/25/the-disinformation-war-the-falsehoods-about-the-ukraine-invasion-and-how-to-stop-them-spre
[602] https://www.euronews.com/my-europe/2022/02/25/the-disinformation-war-the-falsehoods-about-the-ukraine-invasion-and-how-to-stop-them-spre
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

and facts. This approach resembles the traditional DDoS attack aiming to exhaust the resources of physical machines.

Disinformation was used by all actors of the war. Russian disinformation focused on the motivations of the invasion (e.g. denazification, the liberation of Ukraine),[603] [604] [605] Ukrainian and NATO aggression,[606] or the United States providing Ukraine with biological weapons[607] [608] [609]. Ukraine disinformation focused on motivating the troops and highlighting Russian military losses[610] [611]. Other countries also contributed to the spread of disinformation such as the use of chemical weapons in Ukraine or military support by China[612] [613].

In addition, AI-enabled disinformation based on deepfakes took an important role in the war and resulted in videos of Russia's Vladimir Putin and Ukraine's Volodymyr Zelenskyy with messages supporting the views of adversaries. The videos were fake but they spread online[614].

In this perfect storm of disinformation caused by AI, deepfakes and social networks, big companies including Meta, YouTube and Twitter announced waves of new measures in response to growing requests from the Ukrainian government, world leaders and the public[615].

9.1.2 AI-enabled disinformation and deepfakes

The role of AI-enabled disinformation is increasingly becoming central in the creation and spreading of disinformation, and it can make the future supply of disinformation infinite[616] [617]. The proliferation of bots modelling personas can easily disrupt the 'notice-and-comment' rulemaking process, as well as the community interaction, by flooding government agencies with fake comments[618].

In ETL 2021, we already observed that *AI-powered social media is at the basis of the spread of disinformation, causing social chaos*[619]. In this context, *deepfakes technology is evolving quickly. Supporting technology makes the creation of deepfakes simpler, while social media help in spreading them*[620]*. Additionally, misinformation and disinformation campaigns are becoming more credible thanks to deepfakes that cannot yet be fully counteracted*[621] [622].

In particular, content produced or distributed by political leaders has been manipulated or taken out of context for decades but the trend is increasing. However, the advent of deepfakes brought this practice to a different level, providing malicious actors with smart and simple-to-use tools for generating fake content (audio, video, images and text) that is almost impossible to distinguish from real content. The power of AI allows malicious actors (both state

603 https://www.vox.com/2022/2/24/22948944/putin-ukraine-nazi-russia-speech-declare-war
604 https://www.timesofisrael.com/liveblog_entry/putin-calls-on-ukraine-army-to-remove-neo-nazi-leadership-in-kyiv/
605 https://www.factcheck.org/2022/03/the-facts-on-de-nazifying-ukraine/
606 https://www.courthousenews.com/putin-blames-nato-for-pushing-russia-into-invasion/
607 https://www.theguardian.com/media/2022/mar/15/russia-disinformation-social-media-ukraine
608 https://foreignpolicy.com/2022/03/02/ukraine-biolabs-conspiracy-theory-qanon/
609 https://www.bbc.com/news/60711705
610 https://www.bbc.com/news/60528276
611 https://www.businessinsider.com/ukraine-ghost-of-kyiv-died-in-battle-2022-4?r=US&IR=T
612 https://www.nbcnews.com/politics/national-security/us-using-declassified-intel-fight-info-war-russia-even-intel-isnt-rock-rcna23014
613 https://jacobin.com/2022/04/russia-war-ukraine-putin-biden-intelligence-press
614 https://www.dw.com/en/fact-check-the-deepfakes-in-the-disinformation-war-between-russia-and-ukraine/a-61166433
615 https://www.theguardian.com/media/2022/mar/15/russia-disinformation-social-media-ukraine
616 Renée DiResta (20 Sep 2020), 'The supply of disinformation will soon be infinite,' Atlantic, https://www.theatlantic.com/ideas/archive/2020/09/future-propaganda-will-be-computer-generated/616400
617 The_Coming_AI_Hackers.pdf
618 The_Coming_AI_Hackers.pdf
619 The Global Economic Forum, The Global Risks Report 2021 16th Edition, 2021 http://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2021.pdf
620 Avast, 2020: The Year of Fake News, COVID-related Scams and Ransomware, November 2020, https://www.prnewswire.com/news-releases/2020-the-year-of-fake-news-covid-related-scams-and-ransomware-301180568.html
621 Chuck Brooks, Alarming Cybersecurity Stats: What You Need To Know For 2021, March 2021, https://www.forbes.com/sites/chuckbrooks/2021/03/02/alarming-cybersecurity-stats-------what-you-need-to-know-for-2021/
622 Europol, EU SERIOUS AND ORGANISED CRIME THREAT ASSESSMENT (SOCTA 2021), 2021
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

and non-state) to build targeted attacks that mix the profiling of individuals and users, on one side, and personalised disinformation, on the other side[623] [624].

The result of this spread of deepfakes and AI-based disinformation is a loss of credibility in information, media and journalism[625] [626]. This scenario can result in *the liar's dividend,* a major risk described by Chesney and Citron where the goal of a disinformation attack is not fake news, but rather is to deny the truth.

If disinformation has been used to target the community at large, creating ideological conflicts, disrupting elections, and counteracting efforts in limiting the spread of the pandemic, it is also largely used to harm individuals[627] [628]. According to Microsoft, over 96% of deepfake videos concern pornography, while different attacks target the reputations of people. These attacks cause damages that persist after the disinformation has been properly debunked.

9.1.3 Disinformation-as-a-Service (aka disinformation-for-hire)

ETL 2021 observed that professional disinformation is produced on a large scale by major governments, political parties and public relations firms[629]. Since 2019, a growing number of third parties have been offering disinformation services, providing targeted attacks on behalf of clients[630]. Services are provided in numerous countries and an increasing number of non-state and private commercial organisations are using them.[631]

This trend towards disinformation-for-hire is increasing making disinformation campaigns simple to implement and manage[632]. These services coupled with deepfakes are likely to increase mistrust in the entire society[633]. According to the Centre for International Media Assessment (CIMA), *Disinformation-for-hire is a booming industry in which private marketing, communications and public relations firms are paid to sow discord by spreading false information and manipulating content online*[634]. CIMA claims that at least $60 million is the total amount of money spent for propaganda services since 2009.

9.1.4 COVID-19 and the green transition

COVID-19 was a top topic for disinformation attacks in 2021, resulting in what the World Health Organisation (WHO) warned was an infodemic of online disinformation and misinformation[635] [636] [637]. These disinformation campaigns aimed to spread fear, uncertainty and doubt around the effectiveness of coronavirus vaccines. Businesses and individuals were targeted by disinformation campaigns focused on green pass (facilitating border transition based on COVID-19 vaccination), mandatory vaccination, health passports, mass immunity testing and lockdowns. The debate around COVID-19 and disinformation and misinformation continued in 2022, in efforts to find ways to counteract or at least tolerate disinformation and misinformation[638].

The Reuters Institute Digital News Report 2021 reports that COVID-19 disinformation and misinformation was at the top of their survey with 54% of respondents claiming to have seen false and misleading information about COVID-19,

[623] Microsoft FY21 Digital Defense Report
[624] https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
[625] Microsoft FY21 Digital Defense Report
[626] https://lab.cccb.org/en/wolf-wolf-alarm-over-disinformation-and-the-liars-dividend/
[627] Microsoft FY21 Digital Defense Report
[628] https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
[629] Samantha Bradshaw, Hannah Bailey, Philip N. Howard, Industrialised Disinformation 2020 Global Inventory of Organised Social Media Manipulation, 2020, https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/127/2021/01/CyberTroop-Report-2020-v.2.pdf
[630] CTI League, Darknet Report 2021, 2021
[631] Control Risks, Disinformation will affect more than elections in 2021, February 2021, https://www.controlrisks.com/our-thinking/insights/disinformation-will-affect-more-than-elections-in-2021
[632] socta2021_1.pdf
[633] https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
[634] https://www.cima.ned.org/blog/disinformation-for-hire-the-pollution-of-news-ecosystems-and-erosion-of-public-trust/
[635] Managing the COVID-19 infodemic: Promoting healthy behaviors and mitigating the harm from misinformation and disinformation, Joint statement by WHO, UN, UNICEF, UNDP, UNESCO, UNAIDS, ITU, UN Global Pulse, and IFRC, September 2020 , https://www.who.int/news/item/23-09-2020-managing-the-covid-19-infodemic-promoting-healthy-behaviours-and-mitigating-the-harm-from-misinformation-and-disinformation
[636] https://www.who.int/health-topics/infodemic/the-covid-19-infodemic#tab=tab_1
[637] https://unicri.it/sites/default/files/2021-12/11_IF_infodemic.pdf
[638] https://www.theatlantic.com/ideas/archive/2022/03/tolerating-covid-misinformation-better-alternative/626564/
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

with disinformation and misinformation coming from politicians (29%), ordinary people (16%), activists (15%), journalists (11%) and foreign governments (9%) through social networks, search engines and messenger apps[639].

COVID-19 had a strong impact on the energy sector as well as the green transition[640]. During the pandemic we had a reduced consumption of energy but still an impressive consumption of carbon intensive technologies and fossil fuels[641] [642]. Post-COVID-19 recovery measures *mostly neglect the green transition in favour of short-term stability, while loose monetary policies further distort green, market-based solutions or investments*[643]. At the same time, different actors put a lot of effort into slowing the green transition by sharing disinformation and misinformation, and sowing distrust about the climate science community[644].

9.1.5 Additional Facts

- Elections are still a major target of disinformation attacks and a critical concern[645]. Microsoft claims to have shut down many websites used to target elected officials and candidates, organisations that promote democracy, activists and the press. In this context, manipulators of social media platforms tried to distribute disinformation and misinformation.
- According to PwC[646], 19% and 33% of 3,602 respondents replied 'increase significantly' and 'increase', respectively to questions: 'How do you expect a change in reportable incidents for these events in your organisation? How do you expect threats via these vectors/actors to change in 2022 compared to 2021?'
- Disinformation campaigns are increasingly sophisticated, enlarging the scope of disinformation. The mix of modern computing infrastructure, social media, data generation tools, and AI approaches to disinformation are targeting the fundamentals of democracies[647].
- According to Microsoft[648] *threat actors are increasingly using cybersecurity and disinformation attacks in tandem to accomplish their goals.*
- In an analysis made on unmoderated platforms it was found that in a set of 200,000 Telegram posts, those posts with links to sources of misleading information were shared more than the ones with links to professional news content, but only a few channels were targeted[649].
- Australia developed the Australian Code of Practice on Disinformation and Misinformation, which has been adopted by Twitter, Google, Facebook, Microsoft, Redbubble, TikTok, Adobe, and Apple in Australia[650].
- TikTok has been used as a disinformation vector that benefits from its design choice for non-validated and fast video postings[651].
- Generative adversarial networks (GANs) are increasingly used as a vector of disinformation. In 2021, non-expert attackers used GAN to spread disinformation campaigns and spoof social media profiles[652].

[639] https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2021-06/Digital_News_Report_2021_FINAL.pdf
[640] https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
[641] OECD and IEA. 2021. 'Update on recent progress in reform of inefficient fossil-fuel subsidies that encourage wasteful consumption 2021'. Contribution by the Organisation for Economic Co-operation and Development (OECD) and the International Energy Agency (IEA) to G20 Environment, Climate and Energy Ministers, in consultation with the Organization of Petroleum Exporting Countries (OPEC). Climate and Energy Joint Ministerial Meeting. Naples. 23 July 2021. https://www.oecd.org/g20/topics/climate-sustainability-and-energy/OECD-IEA-G20-Fossil-Fuel-Subsidies-Reform-Update-2021.pdf
[642] Clark, A. 2021. 'Energy crisis sets stage for record global carbon emissions'. Bloomberg. 8 October 2021, https://www.bloomberg.com/news/articles/2021-10-08/energy-crisis-setsstage-for-record-global-carbon-emissions
[643] https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
[644] https://edition.cnn.com/2021/10/28/politics/fossil-fuel-oversight-hearing-climate/index.html
[645] Microsoft FY21 Digital Defense Report
[646] PwC, 2022 Global Digital Trust Insights, October 2021
[647] Microsoft FY21 Digital Defense Report
[648] Microsoft FY21 Digital Defense Report
[649] Herasimenka, A., Bright, J., Knuutila, A., Howard, P. N. (2022). Misinformation and professional news on largely unmoderated platforms: the case of Telegram. Journal of Information Technology and Politics. https://doi.org/10.1080/19331681.2022.2076272
[650] https://reutersinstitute.politics.ox.ac.uk/sites/default/files/2021-06/Digital_News_Report_2021_FINAL.pdf
[651] https://www.theguardian.com/media/2022/mar/15/russia-disinformation-social-media-ukraine
[652] Sophos-2022-threat-report.pdf

10. SUPPLY CHAIN ATTACKS

A **supply chain attack** targets the relationship between organisations and their suppliers. For this ETL report we use the definition laid down in the ENISA Threat Landscape for Supply Chain Attacks[653] 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 are 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.

10.1 TRENDS

In 2020, the revelation of SolarWinds already hinted at the potential of supply chain attacks to attackers (and defenders). And as it seems, threat actors continued[654] to further feed on this source to conduct their operations and gain a foothold within organisations. Surveys from the World Economic Forum and Anchore report that between 39%[655] and 62%[656] of organisations were affected by a third-party cyber incident. And according to Mandiant[657] supply chain compromises were the second most prevalent initial infection vector identified in 2021. Furthermore, they also account for 17% of the intrusions in 2021 compared to less than 1% in 2020.

These numbers have raised concerns, rightfully so, with the leaderships of organisations and dribbled down to the attention of governments and policymakers. After all, an increase in cyber defences becomes fruitless if attackers have pathways directly into organisations via compromises of third-party relationships. The European Commission paved the way for the NIS2 Directive[658] which should address the security of supply chains, presented its Cybersecurity Strategy[659] with proposals to strengthen defences and improve responses against malicious activities affecting the supply chain and undertook an in-depth review[660] of strategic areas for Europe's interests. Along the same lines, the Biden administration[661] issued an executive order to improve nationwide cybersecurity in the USA.

While the complexity of the supply chain and dependencies on third parties will only increase, organisations will be required to gain more control and visibility into the web of their supplier relationships and dependencies, possibly by consolidating the number of partners they rely on. Surveys by PWC[662] where only 40% of the respondents said that they understand their third-party cyber and privacy risks and by BlueVoyant[663] where 38% of respondents said that they had no way of knowing when or whether an issue arises with a third-party supplier's cybersecurity underline this need. This complexity of supply chains has affected not only asset and vendor management, the move to the cloud, and the inherent trust needed in these providers, but it has also increased the risk and consequences of supply chain insecurities for many organisations[664]. Furthermore, the lack of clarity in a shared responsibility model can lead to the security of cloud services falling into a sort of digital no-man's land.

[653] ENISA Threat Landscape for Supply Chain Attacks https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
[654] Accenture Cyber Threat Intelligence Report https://www.accenture.com/ae-en/insights/security/cyber-threat-intelligence
[655] WEF Global Cybersecurity Outlook 2022 https://www.weforum.org/reports/global-cybersecurity-outlook-2022/
[656] Anchore 2022 Security Trends: Software Supply Chain Survey https://anchore.com/blog/2022-security-trends-software-supply-chain-survey/
[657] Mandiant M-TRENDS 2022 https://www.mandiant.com/resources/m-trends-2022
[658] EC political agreement on new rules on cybersecurity of network and information systems https://ec.europa.eu/commission/presscorner/detail/en/IP_22_2985
[659] EC Cybersecurity Strategy https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0
[660] EC In-depth reviews of strategic areas for Europe's interests https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/european-industrial-strategy/depth-reviews-strategic-areas-europes-interests_en#cloud-and-edge-computing
[661] The White House https://www.whitehouse.gov/briefing-room/statements-releases/2022/01/19/fact-sheet-president-biden-signs-national-security-memorandum-to-improve-the-cybersecurity-of-national-security-department-of-defense-and-intelligence-community-systems/
[662] PWC 2022 Global Digital Trust Insights Survey https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html
[663] BlueVoyant https://www.bluevoyant.com/news/bluevoyant-research-reveals-rise-in-supply-chain-cybersecurity-breaches-as-firms-struggle-to-effectively-monitor-third-party-cyber-risk/
[664] Accenture Cyber Threat Intelligence Report https://www.accenture.com/ae-en/insights/security/cyber-threat-intelligence

Threat actors already understand fully the critical role suppliers play, both in the digital and physical world. They have realised that one single incident or hiccup can easily ripple down to different industries and sectors, without much additional effort from their end.

Additionally, the logistical challenges organisations experienced during the COVID-19 pandemic as well as the consequences of the war in Ukraine will only further fuel the discussion to find a better balance between self-reliance and the use of supply chain providers, spread geographically across different areas of the world.

10.1.1 Increased abuse of the complexity of systems and lack of visibility

In order to be successful, organisations rely on complex systems to meet the demands of their customers and address the required scale, efficiency and speed of production and delivery. These complex systems rely on a multitude of suppliers and the selection and management of these suppliers is shaped by a host of factors. Many organisations struggle with their vendor or supplier management. An initial assessment of a supplier is often nothing more than a questionnaire (which on its own is sometimes already of questionable value) and, once onboarded, the review cycle consists of annual (or even less frequent) point-in-time reviews[665] [666]. To complicate matters further, different departments within the same organisation onboard suppliers, each with different processes and functions. This makes it nearly impossible for organisations to gain holistic visibility into the web of their third-party relationships, dependencies and risks. And next to these relationships, there is often not always a good oversight of where data resides and which partner has access to this data, either in an online or offline form.

It is almost-certain that adversaries will further abuse this lack of visibility into dependencies, as well as the increased complexity and the trust organisations put into their suppliers, to gain a foothold within organisations. We need to highlight initiatives such as the Software Bill of Materials (SBOM)[667] that aim at making such things more transparent and auditable.

Gaining visibility[668] into the web of third-party relationships and dependencies is a must. Unfortunately, as proactive management of a supplier ecosystem remains difficult, most of the efforts of organisations still limit themselves to a reactive approach. Years ago we witnessed a shift in security monitoring and incident response activities from a reactive to a more proactive approach, and now third-party risk management will have to undergo a similar change. This change should also address the risk of not including suppliers in incident response plans and exercises and not having clear communication pathways with vendors and suppliers for disclosures of vulnerabilities or the coordination of incidents.

Pending this change, it is almost-certain that organisations will continue to struggle with supply chain management, and as a consequence loose valuable resources[669], while trying to grasp whether and how a breach of a third-party vendor affects them.

10.1.2 Use of vulnerabilities in business technologies

One of the ways in which threat actors have begun targeting organisations is by investing in research into vulnerabilities in commonly used business technologies[670], such as e-mail servers[671] [672] or knowledge management software[673] [674]. After all, a vulnerability (or a chain of vulnerabilities) in one technology gives them access to multiple environments at once.

In addition, highly-determined threat actors can scavenge information on the infrastructure of targeted victims in public resources such as tenders, marketing documents or job announcements. This documentation then allows

[665] Microsoft Digital Defense Report https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFli
[666] PWC 2022 Global Digital Trust Insights Survey https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html
[667] CISA, Software Bill of Materials, https://www.cisa.gov/sbom
[668] PWC 2022 Global Digital Trust Insights Survey https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html
[669] Microsoft Digital Defense Report https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFli
[670] PWC Cyber Threats 2021 A Year in Retrospect https://www.pwc.com/gx/en/issues/cybersecurity/cyber-threat-intelligence/cyber-year-in-retrospect/yir-cyber-threats-report-download.pdf
[671] ProxyLogon https://proxylogon.com/
[672] ProxyShell https://news.sophos.com/en-us/2021/08/23/proxyshell-vulnerabilities-in-microsoft-exchange-what-to-do/
[673] Confluence Security Advisory - 2021-08-25 https://confluence.atlassian.com/doc/confluence-security-advisory-2021-08-25-1077906215.html
[674] Confluence Security Advisory - 2022-06-02 https://confluence.atlassian.com/doc/confluence-security-advisory-2022-06-02-1130377146.html
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

these attackers to identify the exact brand and version of technology that they need to target (or investigate) for vulnerabilities.

A side effect of the investment in resources is that the number of 0-days being discovered[675] has increased substantially[676]. And although in a lot of cases the disclosure of such 0-days is done responsibly (with accompanying vendor communication and patches), the mere fact of the publication leads to further attempts at exploitation by opportunistic threat actors seeking an easy win.

It is very likely that we will see an increased investment[677] of resources into vulnerability research in these supply chains in the near future. It is also very likely we will continue to see attempts to exploit the situation by opportunistic threat actors following the disclosure of vulnerabilities in popular business technologies.

10.1.3 Targeting security researchers for gaining access to targets

Vulnerability research is very expensive and requires a lot of investment in resources, partly because of the improved security of such technologies but also because there is always a risk that a freshly discovered vulnerability can be exposed (and patched) before an attacker can make use of it. This is one of the reasons why threat groups also start targeting security researchers directly[678] [679] [680] [681]. After all, instead of doing the hard research yourself, why not let someone else do the heavy lifting and then just steal that information from them? And while the mere abuse of a vulnerability in a business technology does not constitute a supply chain attack according to our ETL definition, targeting specific researchers first and then using the information obtained to gain access to a predetermined victim is certainly considered to be a supply chain attack.

Considering the cost of vulnerability research for threat actors, it is likely we will see increased targeting of those individuals or organisations doing research on security flaws or vulnerabilities with the goal of stealing their findings.

10.1.4 Increased interest of threat groups in supply chain attacks and attacks against MSPs

The notorious SolarWinds compromise from 2020 was attributed to the Russian intelligence services (SVR) affiliated group APT29[682] [683] [684]. This was a first warning of the increased interest of threat groups, and predominantly those coming from Russia and China, and to a lesser extent North Korea, in supply chain attacks. Unfortunately, the SolarWinds attack was only the first of many to come.

Threat actors linked to China

In October 2021 a campaign from the Chinese state-sponsored threat actor, HoneyMyte[685], also referred to as Mustang Panda, that modified an installer package for fingerprint scanner software on a distribution server in Asia. The modified version included changes in the configuration files and the tools needed to deploy the PlugX backdoor. As employees of a central government in South Asia are required to use this software, this gave the actors remote access to key environments. What is interesting to note is that in the ESET report at the end of 2020[686] on operation SignSight[687] [688] there is reference to a modified software installer for a digital signature verification software via the

[675] For example when these vulnerabilities were uncovered during incident investigations in cases where threat actors used such 0-days to gain access to a victim.
[676] Project Zero: A Year in Review of 0-days Used In-the-Wild in 2021 https://googleprojectzero.blogspot.com/2022/04/the-more-you-know-more-you-know-you.html
[677] PWC 2022 Global Digital Trust Insights Survey https://www.pwc.com/gx/en/issues/cybersecurity/global-digital-trust-insights.html
[678] Black Hat Keynote: Supply Chain Infections and the Future of Contactless Deliveries https://www.blackhat.com/us-21/briefings/schedule/#keynote-supply-chain-infections-and-the-future-of-contactless-deliveries-24987
[679] For All Secure https://forallsecure.com/blog/matt-tait-warns-of-stolen-0-days-at-black-hat-usa-2021
[680] Ars Technica https://arstechnica.com/information-technology/2021/01/north-korea-hackers-use-social-media-to-target-security-researchers/
[681] Google TAG New campaign targeting security researchers https://blog.google/threat-analysis-group/new-campaign-targeting-security-researchers/
[682] NCSC UK https://www.ncsc.gov.uk/news/uk-and-us-call-out-russia-for-solarwinds-compromise
[683] The Register https://www.theregister.com/2021/04/15/solarwinds_hack_russia_apt29_positive_technologies_sanctions/
[684] APT29 https://apt.etda.or.th/cgi-bin/showcard.cgi?g=APT%2029%2C%20Cozy%20Bear%2C%20The%20Dukes
[685] HoneyMyte https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Mustang%20Panda%2C%20Bronze%20President
[686] Outside of our reporting period but relevant to include as background
[687] ESET https://www.eset.com/us/about/newsroom/press-releases/eset-discovers-operation-signsight-supply-chain-attack-against-a-certification-authority-in-southea-1/
[688] VinCSS https://blog.vincss.net/2020/12/re018-1-analyzing-new-malware-of-china-panda-hacker-group-used-to-attack-supply-chain-against-vietnam-government-certification-authority.html
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

website of the government of Vietnam. APT10[689], also referred to as Stone Panda, abused vulnerabilities in financial software that is heavily used by Taiwan securities traders[690] to eventually plant the remote access tool Quasar on targeted systems, while using a credential stuffing attack as a smokescreen. And finally to conclude the list of Chinese groups, APT41[691] was likely behind a third-party attack on Air India[692] and the compromise of the Mongolian certification authority (CA) MonPass[693].

Threat actors linked to Russia

Targeting mandatory or popular software used by specific targets is only the beginning for these threat groups. A report on APT29[694] also known as The Dukes and referred to as Nobelium[695] by Microsoft, covers an operation where this Russian group targets organisations in the US and European IT supply chains. In this campaign the actor focussed on specific resellers and technology service providers that customise, deploy and manage cloud services and other technologies. In these attacks the threat actors did not attempt to exploit vulnerabilities but rather used well-known techniques, like password spraying[696] and phishing to steal legitimate credentials from the targeted service and then gain privileged access[697] to one of the downstream customers.

Threat actors linked to North Korea (DPRK)

APTs also directly target suppliers of security software, such as reported by Google in which North Korean hackers targeted South Korean security companies that sell anti-malware software[698]. Apart from security software, attackers also focus[699] on providers of software that give direct access, with extensive permissions, into a broad set of environments. Typical examples of such software include the management tools used by administrators, automation software and remote monitoring and management tools. One of the most covered attacks was the exploitation of a vulnerability in the software of Kaseya. In this incident[700] managed service providers (MSPs) and their customers fell victim to a ransomware incident executed via the remote monitoring and management tool Kaseya Virtual System Administrator (VSA). It is important to note that up to this time, there were no signs that the Kaseya built systems or source code were modified by the attackers. Another attack method was covered by Mandiant[701], where an adversary abused applications that were assigned permissions within multiple Azure tenants, opening the pathway for a supply chain attack.

Long term access by APTs

All this activity is an indicator that certain state-sponsored groups try to get long-term systematic access to these supply chains. The opportunities presented to these actors if they compromise key MSPs are significant, and will potentially allow them to acquire access to key European governments and bodies. A joint warning[702] by the cybersecurity authorities of the United Kingdom (NCSC-UK), Australia (ACSC), Canada (CCCS), New Zealand (NCSC-NZ), and the United States (CISA, NSA, FBI) further strengthens this belief and calls for actions that MSPs, and their customers, can take to reduce the risk of falling victim to such intrusions.

Furthermore the impact of operations, especially those focussed on espionage, by nation-state actors via supply chain attacks might not always be immediately noticeable by victims. And although in general the median dwell time[703] has dropped significantly, these types of threat actors can lurk in the dark for a very long time.

[689] APT10 https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Stone%20Panda%2C%20APT%2010%2C%20menuPass
[690] CyCraft https://medium.com/cycraft/china-implicated-in-prolonged-supply-chain-attack-targeting-taiwan-financial-sector-264b6a1c3525
[691] APT41 https://apt.etda.or.th/cgi-bin/showcard.cgi?g=APT%2041
[692] Group-IB Big airline heist https://blog.group-ib.com/colunmtk_apt41
[693] Venafi https://www.venafi.com/sites/default/files/2021-11/Venafi_WhitePaper_CodeSigningAPT41_2021_f_0.pdf
[694] APT29 https://apt.etda.or.th/cgi-bin/showcard.cgi?g=APT%2029%2C%20Cozy%20Bear%2C%20The%20Dukes
[695] Microsoft New activity from Russian actor Nobelium https://blogs.microsoft.com/on-the-issues/2021/10/24/new-activity-from-russian-actor-nobelium/
[696] MITRE ATT&CK T1110.003 https://attack.mitre.org/techniques/T1110/003/
[697] NOBELIUM targeting delegated administrative privileges to facilitate broader attacks https://www.microsoft.com/security/blog/2021/10/25/nobelium-targeting-delegated-administrative-privileges-to-facilitate-broader-attacks/
[698] Threat Horizons https://services.google.com/fh/files/misc/gcat_threathorizons_full_nov2021.pdf
[699] Acronis Cyberthreats Report 2022 https://dl.acronis.com/u/rc/White-Paper-Acronis-Cyber-Threats-Report-2022-EN-US.pdf
[700] Kaseya https://helpdesk.kaseya.com/hc/en-gb/articles/4403584098961-Incident-Overview-Technical-Details
[701] Mandiant M-TRENDS 2022 https://www.mandiant.com/resources/m-trends-2022
[702] CISA – Alert AA22-131A https://www.cisa.gov/uscert/ncas/alerts/aa22-131a
[703] Mandiant M-TRENDS 2022 https://www.mandiant.com/resources/m-trends-2022

Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

State-sponsored groups are not the only threat actors in this playing field. This was painfully demonstrated by the operators of LockBit (ransomware) when the criminal gang stole and leaked[704] [705] documents from the technology supplier Abiom. Abiom supplies communication technology for the Dutch emergency network C2000, the Dutch Ministry of Defence, the National Police and security services, amongst several other government entities.

Considering this, it is very likely that we will see further interest from APTs in conducting supply chain attacks, very likely by first compromising MSPs before gaining access to their targets.

10.1.5 Log4Shell

Log4Shell is a zero-day vulnerability reported in 2021 in Log4j[706], a Java logging framework, that can lead to the execution of arbitrary code. Although, according to the definition that is used for supply chain attacks in this ETL, Log4Shell is not considered a supply chain attack (there is no combination of two attacks), due to the overwhelming presence of Log4j in IT infrastructure[707] it is worth covering it.

In December 2021 Crowdstrike revealed[708] an operation by Aquatic Panda[709], a China-based threat group that used a modified version of Log4Shell to target a vulnerable VMware Horizon instance at a large academic institution. This was not the only operation linked to instances in which VMware Horizon was abused. In June 2022, both CISA and CGCYBER released an advisory[710] [711] in which they report on multiple threat actor groups that have exploited Log4Shell on unpatched, public-facing VMware Horizon and Unified Access Gateway servers. These threat actors used Log4Shell as an initial access to the environment of their victims, in one case a disaster recovery network, to then exfiltrate sensitive data or enable remote access to these target environments.

It is expected[712] that many state-operated actors are very likely going to continue to integrate Log4Shell exploits with their arsenal, since this library provides a valuable entry point and organisations are having a hard time identifying which of their assets run a vulnerable version of Log4Shell. From the point of view of these threat actors, Log4Shell is however just a very lucrative access vector among a long list of other vectors.

10.1.6 Targeting build systems, source code and developers

Apart from the vulnerabilities in popular business technologies, there are other vulnerabilities that play a role in supply chain attacks.

According to research by Palo Alto[713], 21% of the security scans that they ran against development environments resulted in misconfigurations or vulnerabilities. The same research from Palo Alto showed that 63% of third-party code templates used in building cloud infrastructure ('infrastructure as code') contained insecure configurations and 96% of third-party container applications deployed in cloud infrastructure contained known vulnerabilities.

Container infrastructure, and the software supply chain on which they rely, is and will very likely remain, an expanding attack[714] [715] [716] surface for supply chain attacks.

Next to targeting container infrastructure, attacks can also directly target the source[717] code or the systems used to build and release software. One of the more stealthier attack methods for changing the source code was revealed by

[704] RedPacket Security https://www.redpacketsecurity.com/lockbit-2-0-ransomware-victim-abiom-nl/
[705] Tweakers https://tweakers.net/nieuws/190358/criminelen-stelen-vertrouwelijke-info-bij-aanval-op-ict-leverancier-van-defensie.html
[706] Log4J https://logging.apache.org/log4j/2.x/
[707] NCSC-NL Log4Shell https://github.com/NCSC-NL/log4shell
[708] OverWatch Exposes AQUATIC PANDA in Possession of Log4Shell Exploit Tools During Hands-on Intrusion Attempt https://www.crowdstrike.com/blog/overwatch-exposes-aquatic-panda-in-possession-of-log-4-shell-exploit-tools/
[709] Aquatic Panda https://apt.etda.or.th/cgi-bin/showcard.cgi?g=Aquatic%20Panda
[710] AA22-174A https://www.cisa.gov/uscert/ncas/alerts/aa22-174a
[711] New Milestones for Deep Panda: Log4Shell and Digitally Signed Fire Chili Rootkits https://www.fortinet.com/blog/threat-research/deep-panda-log4shell-fire-chili-rootkits
[712] Crowdstrike 2022 Global Threat Report https://www.crowdstrike.com/global-threat-report/
[713] Palo Alto Unit 42 Cloud Threat Report https://www.paloaltonetworks.com/prisma/unit42-cloud-threat-research-2h21
[714] Docker – The impacts of an insecure software supply chain https://www.docker.com/blog/the-impacts-of-an-insecure-software-supply-chain/
[715] Container solutions https://blog.container-solutions.com/wtf-can-you-do-about-software-supply-chain-attacks
[716] Aquasec Supply chain attacks using container images https://blog.aquasec.com/supply-chain-threats-using-container-images
[717] Microsoft Supply chain attacks https://docs.microsoft.com/en-us/microsoft-365/security/intelligence/supply-chain-malware?view=o365-worldwide
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

researchers from the University of Cambridge and dubbed Trojan Source[718] [719]. This attack uses Unicode control characters to reorder tokens in source code and makes use of the fact that developers sometimes copy and paste useful snippets of code from online postings directly into their editors. For a human being the attack code is not visible in the source (depending on the developer toolkit that is being used), and thus it can easily find its way into the final released software.

Unfortunately, despite a lot of attention being paid to publications promoting the concept of 'shift left'[720], with the goal of tackling security problems early on during the development phase of software products, there is still a lot of room for improvements to be made.

Changes to source code or build systems can be used to compromise specific targets, possibly for espionage, as we have witnessed with SolarWinds, and will likely continue to occur. Far more likely though is that the objective of attackers is financial gain.

10.1.7 Supply chain cryptojacking for more financial gain

Cryptojacking or hidden cryptomining is a type of cybercrime where a criminal secretly uses a victim's computing power to generate cryptocurrency[721]. This objective is usually attained by criminals by focussing on abusing or mimicking developer libraries[722] and then hiding these libraries in commonly used software development repositories. Examples include malicious packages disguised as legitimate JavaScript libraries[723] or even tampering with popular JavaScript libraries, such as was the case with ua-parser.js[724]. This particular incident happened via the takeover of a developer account and it is very likely that we will continue to see more of this type of activity in the near future. It is important to note is that, based on our definition of a supply chain attack, we do not consider these as 'real' supply chain attacks.

Obviously cryptojacking is just one of many effects of such attacks. Criminals can use the same channels for ransomware, password stealing and even wiper attacks.

[718] Trojan Source paper https://trojansource.codes/trojan-source.pdf
[719] Bleeping Computer https://www.bleepingcomputer.com/news/security/trojan-source-attack-method-can-hide-bugs-into-open-source-code/
[720] Sophos 2022 threat report https://www.sophos.com/en-us/labs/security-threat-report
[721] ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
[722] Accenture Cyber Threat Intelligence Report https://www.accenture.com/ae-en/insights/security/cyber-threat-intelligence
[723] Sonatype - https://blog.sonatype.com/newly-found-npm-malware-mines-cryptocurrency-on-windows-linux-macos-devices
[724] GitHub https://github.com/faisalman/ua-parser-js/issues/536

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[725]. 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. It has been updated to version June 2022.

TA0001: Initial Access	T1190: Exploit Public-Facing Application T1133: External Remote Services T1566: Phishing T1199: Trusted Relationship
TA0002: Execution	T1106: Native API T1047: Windows Management Instrumentation
TA0003: Persistence	T1197: BITS Jobs T1554: Compromise Client Software Binary T1136: Create Account T1133: External Remote Services
TA0004: Privilege Escalation	T1134: Access Token Manipulation T1068: Exploitation for Privilege Escalation T1055: Process Injection
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
TA0006: Credential Access	T1555: Credentials from Password Stores T1539: Steal Web Session Cookie
TA0007: Discovery	T1087: Account Discovery T1217: Browser Bookmark Discovery T1135: Network Share Discovery T1069: Permission Groups Discovery T1057: Process Discovery

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

	T1012: Query Registry T1518: Software Discovery T1614: System Location Discovery T1033: System Owner/User Discovery T1124: System Time Discovery T1497: Virtualisation/Sandbox Evasion
TA0008: Lateral Movement	T1210: Exploitation of Remote Services T1080: Taint Shared Content
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
TA0011: Command and Control	T1568: Dynamic Resolution T1095: Non-Application Layer Protocol T1071: Non-Standard Port T1072: Protocol Tunnelling T1090: Proxy T1102: Web Service
TA0010: Exfiltration	T1041: Exfiltration Over C2 Channel
TA0040: Impact	T1485: Data Destruction T1499: Endpoint Denial of Service T1489: Service Stop

MALWARE (PEGASUS FOR ANDROID)

The current table highlights the techniques in the MITRE ATT&CK® Framework associated with the Pegasus spyware. The 726 Notice Pegasus for Android is the Android version of malware that has reportedly been linked to the NSO Group (Update August 2022). The iOS version is tracked separately under Pegasus for iOS.

Mobile	T1429	Audio Capture
Mobile	T1645	Compromise Client Software Binary
Mobile	T1624 0.001	Event Triggered Execution: Broadcast Receivers
Mobile	T1404	Exploitation for Privilege Escalation
Mobile	T1644	Out of Band Data
Mobile	T1636 0.001	Protected User Data: Calendar Entries
Mobile	T1636 0.002	Protected User Data: Call Log
Mobile	T1636 0.003	Protected User Data: Contact List
Mobile	T1418	Software Discovery
Mobile	T1409	Stored Application Data
Mobile	T1422	System Network Configuration Discovery

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

Mobile	T1512	Video Capture

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.

In addition, we only list those techniques relevant for social engineering. We do not include the techniques commonly used for follow-up activity (including for example the methods showing how malicious documents can execute).

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
TA0042: Resource Development	T1583: Acquire Infrastructure T1586: Compromise Accounts T1584: Compromise Infrastructure T1587: Develop Capabilities T1585: Establish Accounts T1588: Obtain Capabilities T1608: Stage Capabilities
TA0001: Initial Access	T1133: External Remote Services T1566: Phishing T1199: Trusted Relationship T1078: Valid Accounts
TA0002: Execution	T1204: User Execution

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®727 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

TA0003: Persistence	T1197: BITS Jobs

[727] MITRE ATT&CK®, https://attack.mitre.org/

TA0005: Defence Evasion	T1197: BITS Jobs T1599: Network Boundary Bridging
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
TA0010: Exfiltration	T1020: Automated Exfiltration T1048: Exfiltration Over Alternative Protocol T1041: Exfiltration Over C2 Channel 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

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®728 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.

DOS

TA0042: Resource Development	T1583: Acquire Infrastructure T1583.005: Botnet T1584: Compromise Infrastructure T1584.005: Botnet
TA0005: Defence Evasion	T1553: Subvert Trust Controls T1553.003: SIP and Trust Provider Hijacking
TA0040: Impact	T1485: Data Destruction T1489: Service Stop T1499: Endpoint Denial of Service T1499.003: Application Exhaustion Flood T1499.004: Application or System Exploitation T1499.001: OS Exhaustion Flood T1499.002: Service Exhaustion Flood T1498: Network Denial of Service T1498.001: Direct Network Flood T1498.002: Reflection Amplification

[728] MITRE ATT&CK®, https://attack.mitre.org/

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[729]. 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.

TA0001: Initial Access	T1189: Drive-by Compromise
TA0007: Discovery	T1046: Network Service Scanning
TA0009: Collection	T1557: Adversary-in-the-Middle
TA0040: Impact	T1498: Network Denial Of Service

DISINFORMATION - MISINFORMATION

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.

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
TA0042: Resource Development	T1586: Compromise Accounts T1585: Establish Accounts
TA0001: Initial Access	T1566: Phishing
TA0002: Execution	T1203: Exploitation for Client Execution T1204: User Execution
TA0040: Impact	T1565: Data Manipulation T1491: Defacement

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

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' [730] 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.

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
TA0042: Resource Development	T1583: Acquire Infrastructure T1586: Compromise Accounts T1584: Compromise Infrastructure T1587: Develop Capabilities T1585: Establish Accounts T1588: Obtain Capabilities T1608: Stage Capabilities
TA0001: Initial Access	T1195: Supply Chain Compromise T1195.001: Compromise Software Dependencies and Development Tools T1195.002: Compromise Software Supply Chain T1195.003: Compromise Hardware Supply Chain T1200: Hardware Additions T1199: Trusted Relationship

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

B ANNEX: INDICATIVE LIST OF INCIDENTS

This Annex presents a non-exhaustive list of relevant incidents, alongside their geographic spread or proximity and associated time of occurrence. It is important to note that by analysing the incidents presented as well as the full list of incidents related to threats mentioned in the ETL, ENISA determined the trends described in the previous sections.

The incidents that constitute each list were selected based on the following criteria: (a) the geographical spread of the attack, (b) the impact of the incident, (c) an innovative technique used for the attack, and (d) the existence of an unprecedented element (e.g. first incident in which a patient died because of a ransomware attack).

B.1 RANSOMWARE

Table 3: Notable ransomware incidents

Time	Geographical Spread	Description
November 2021	NEAR	**Media Markt,** a German electronic retailer, was hit by Hive ransomware, impacting 49 stores in the Netherlands. The infection caused impacts on retrieving orders and returns in the store. Interestingly, a Dutch reporter got insight into the communication between Hive and the company, revealing they had not paid the ransom[731].
December 2021	NEAR	French IT services company **Inetum Group** [732] suffered a ransomware attack. Although unconfirmed, the attack is attributed to ALPHV. Official statements mention only a limited impact on the business and its customers. This attack follows the BGH trend, with large corporations being targeted, as impact could cause a tickle-down effect on its customers.
December 2021	NEAR	**Nordic Choice Hotels** was impacted by Conti ransomware. The incident impacted the hotel's guest reservation and room key card systems[733]. Guests reported their key cards to be out of service.
January 2022	NEAR	Ministry of Justice in France: threat actors who are using ransomware LockBit 2.0 have posted a message on their Tor-based leak website claiming to have stolen files from the Ministry of Justice's systems[734].
February 2022	MID	Swissport, an Airport management services company: the BlackCat ransomware group, aka ALPHV, claimed responsibility for the recent cyberattack on Swissport that caused flight delays and service disruptions[735].
February 2022	GLOBAL	Nvidia Corp (Lapus$ ransomware gang): 'Lapsus$' took responsibility for the breach on its Telegram channel and claims to have stolen 1 terabyte of information, including 'highly confidential/secret data' and proprietary source code[736].

731 https://www.rtlnieuws.nl/tech/artikel/5289859/mediamarkt-ransomware-hive-cybercriminelen-onderhandelingen-helpdesk
732 https://www.bleepingcomputer.com/news/security/global-it-services-provider-inetum-hit-by-ransomware-attack/
733 https://www.nordicchoicehotels.com/blog/information/virus-attacks
734 https://www.securityweek.com/french-ministry-justice-targeted-ransomware-attack
735 https://www.bleepingcomputer.com/news/security/blackcat-alphv-claims-swissport-ransomware-attack-leaks-data/
736 https://techcrunch.com/2022/03/01/nvidia-hackers-leak-ransomware/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS8&guce_referrer_sig=AQAAABLSW3zgbwSA8dqCyWUEpL5VIsKnzp7GvT5_5Htu8RWj3RvravTSNwfKh5lDoJ7IFaSdbEYkV7r1TpTm9WwclmmsXZP9HBASkWscsSBajOKR6EBjpvf0zGd_tfHo5x16Ly9JDI2qyO1qP3rBPcWllmlKNtE_cdZmyrPO3pluz3Ga

Time	Geographical Spread	Description
March 2022	FAR	Toyota Motor suspended operations in 28 production lines across 14 plants in Japan for at least a day after a key supply chain player was hit by a suspected cyberattack. The incident affected Toyota's plastic parts and electronic components supplier Kojima Industries on February 24. The firm said it discovered a malware infection and a 'threatening message' on rebooting after a file error on its server. The nature of events suggests that Kojima Industries was likely a victim of a ransomware attack.

B.2 MALWARE

Table 4: Notable malware incidents

Time	Geographical Spread	Description
June 2022	GLOBAL	CYBERATTACK AGAINST A DISCORD NFT SERVER: hackers escalate phishing and scamming attacks to exploit popular Discord bot and persuade users to click on the malicious links[737].
July 2022	MID	UAC-0056 target Ukraine in its latest campaign with Cobalt Strike beacon[738].
July 2022	NEAR	EU Commission alarmed by new spyware case against Greek socialist leader. The leader of Greece's socialist opposition PASOK party filed a complaint with the country's top court prosecutors on Tuesday over an attempted bugging of his mobile phone with surveillance software (PREDATOR)[739].

B.3 SOCIAL ENGINEERING

Table 5: Notable social engineering incidents

Time	Geographical Spread	Description
November 2021	NEAR	**IKEA email systems hit by cyberattack:** threat actors targeted employees in internal phishing attacks using stolen reply-chain emails[740].
December 2021	NEAR	**Phishing campaign using QR codes targeting German e-banking users**: the messages that were used in a campaign used QR codes to deceive users of two German financial institutions, Sparkasse and Volksbanken Raiffeisenbanken, and steal digital banking information[741].

[737] https://threatpost.com/scammers-target-nft-discord-channel/179827/
[738] https://www.malwarebytes.com/blog/threat-intelligence/2022/07/cobalt-strikes-again-uac-0056-continues-to-target-ukraine-in-its-latest-campaign
[739] https://www.reuters.com/world/europe/greek-socialist-leader-files-complaint-over-attempted-phone-bugging-2022-07-26/
[740] https://www.bleepingcomputer.com/news/security/ikea-email-systems-hit-by-ongoing-cyberattack/
[741] https://securityaffairs.co/wordpress/125540/cyber-crime/phishing-qr-codes.html
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Time	Geographical Spread	Description
March 2022	NEAR	Chinese phishing actors consistently targeting EU diplomats: TA416 (aka Mustang Panda) has been consistently targeting European diplomats since August 2020, with the most recent activity involving refreshed lures to coincide with the Russian invasion of Ukraine[742].
April 2022	GLOBAL	Multiple Hacker Groups Capitalising on Ukraine Conflict for Distributing Malware: at least three different advanced persistent threat (APT) groups from across the world launched spear-phishing campaigns in mid-March 2022 using the ongoing Russo-Ukrainian war as a lure to distribute malware and steal sensitive information[743].

B.4 THREATS AGAINST DATA

Table 6: Notable incidents against data

Time	Geographical Spread	Description
June-July 2022	FAR	Professional Finance Company (PFC USA) has been the target of a data breach that impacted patients of over 650 healthcare providers across the USA[744].
June 2022	FAR	NFT marketplace OpenSea underwent a mail data breach. An internal attack by an employee of an e-mail vendor contractor was executed to share e-mail addresses of OpenSea users and newsletter subscribers[745].
June 2022	FAR	The data of 1.5 million customers was breached by security incidents at Flagstar Bank[746].
January 2022	FAR	Reports described a possible massive medical data breach in Indonesia. According to Antaranews, 720 GB of medical data were sold on the dark web contained medical information from different hospitals[747].
December 2021	GLOBAL	FlexBooker, an appointment scheduling and calendar service, suffered a data breach of 3.7 million accounts, which was executed after a DDoS attack that targeted the company's Amazon AWS server[748]. The attack was carried by the threat group Uawrongteam and was probably a distraction for implementing the data breach.
November 2021	FAR	Online stock trading platform Robinhood was hit by a cyberattack resulting in the breach of more than five million customer e-mail addresses and two million customer names, including a smaller amount of specific customer data[749] [750] [751]. The attack was caused by a socially engineering attack against a customer service representative to get access to customer support systems.
October 2021	NEAR	The COVID app of Belgium was attacked causing a data breach. The personal data of 39,000 people was exposed[752].

[742] https://www.bleepingcomputer.com/news/security/chinese-phishing-actors-consistently-targeting-eu-diplomats/
[743] https://thehackernews.com/2022/04/multiple-hacker-groups-capitalizing-on.html
[744] https://www.securityweek.com/data-breach-pfc-usa-impacts-patients-650-healthcare-providers
[745] https://techcrunch.com/2022/06/30/nft-opensea-data-breach/
[746] https://www.zdnet.com/article/1-5-million-customers-impacted-in-flagstar-data-breach/
[747] https://en.tempo.co/read/1547439/health-ministry-responds-to-massive-data-leak-of-medical-records
[748] https://www.cpomagazine.com/cyber-security/3-7-million-flexbooker-accounts-leaked-to-hacker-forum-after-ddos-attack/
[749] https://techcrunch.com/2021/11/09/robinhood-data-breach/
[750] https://blog.robinhood.com/news/2021/11/8/data-security-incident
[751] https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf
[752] https://www.bloombergquint.com/onweb/belgium-s-covid-app-reports-data-breach-days-before-pass-rollout
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Time	Geographical Spread	Description
October 2021	FAR	South African banks reported a possible data breach involving more than 1.4 million South African citizens[753].
October 2021	FAR	Security Researcher Jeremiah Fowler in collaboration with the Cooltechzone research team reported finding an unprotected database containing over 82 million records belonging to multiple companies such as, for instance, Whole Foods Market and Skaggs public safety[754].
September 2021	FAR	The cybercriminal group DarkSide launched a DDoS attack against Colonial Pipeline, the largest refined oil pipeline system in the USA[755]. The company lost access to computer systems and suffered a data breach of over 100 GB of corporate data[756].
September 2021	NEAR	A Paris hospital system has been reported as the target of a data breach that resulted in the theft of the COVID test data of 1.4 million people[757].
August 2021	NEAR	T-Mobile has reported being hit by a sophisticated cyberattack against its systems, through an unprotected network access device, which resulted in a massive data breach[758] [759] [760]. According to T-Mobile: *approximately 7.8 million current T-Mobile post-paid customer accounts' information appears to be contained in the stolen files, as well as just over 40 million records of former or prospective customers who had previously applied for credit with T-Mobile.*
July 2021	FAR	Kaseya Virtual Systems Administrator (VSA) has been hit by REvil ransomware to attack Managed Security Service Providers that controlled the infrastructure of thousands of companies[761]. It is not reported how many of the millions of end point systems were encrypted.

B.5 THREATS AGAINST AVAILABILITY (DDOS)

Table 7: Notable incidents against availability

Time	Geographical Spread	Description
April 2022	FAR	One of the largest HTTPS DDoS attacks targeted a Cloudflare customer on the Professional (Pro) plan operating a crypto launchpad[762]. The attack was launched at 15M rps and, according to Cloudfare, mostly came from data centres with a botnet of about 6,000 bots from 112 countries.
March 2022	FAR	The largest ever DDoS cyberattack in Israel targeted the Ministries of Interior, Defence, Health, Justice, Welfare and the Prime Minister's Office[763]. The domain gov.il was under attack, making different websites unavailable during the day[764].

[753] https://portswigger.net/daily-swig/millions-of-south-africans-caught-up-in-security-incident-after-debt-recovery-firm-suffers-significant-data-breach
[754] https://cooltechzone.com/leaks/enterprise-software-developer-exposed-millions-of-logging-records-of-amazon-owned-company
[755] Trend micro - toward a new momentum security predictions for 2022
[756] Trend Micro. (Sept. 14, 2021). Trend Micro. "Attacks From All Angles: 2021 Midyear Cybersecurity Report." Accessed on Nov. 25, 2021, at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/attacks-from-all-angles-2021-midyear-security-roundup.
[757] https://www.rfi.fr/en/france/20210916-hackers-steal-covid-test-data-of-1-4-million-people-from-paris-hospital-system
[758] https://www.t-mobile.com/news/network/additional-information-regarding-2021-cyberattack-investigation
[759] https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf
[760] https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf
[761] https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf
[762] https://blog.cloudflare.com/15m-rps-ddos-attack/
[763] https://www.infosecurity-magazine.com/news/israeli-goverment-websites-offline/
[764] https://portswigger.net/daily-swig/israeli-government-websites-temporarily-knocked-offline-by-massive-cyber-attack
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Time	Geographical Spread	Description
December 2021	NEAR	The largest DDoS attack on mobile network operators in Poland, as well as the largest hitting T-Mobile, was observed[765]. Critical systems were not compromised and the attack was mitigated.
November 2021	FAR	Microsoft mitigated a DDoS attack with a throughput of 3.47 Tbps and a packet rate of 340 million packets per second (pps)[766]. The attack targeted an Azure customer in Asia and originated from about 10,000 sources and multiple countries. UDP reflection on port 80 was used with Simple Service Discovery Protocol (SSDP), Connection-less Lightweight Directory Access Protocol (CLDAP), Domain Name System (DNS), and Network Time Protocol (NTP). The attack duration was about 15 minutes.
November 2021	GLOBAL	Silverline mitigated a huge attack targeting an ISP/hosting customer. The attack duration lasted four minutes with a maximum bandwidth of 1.4 Tbps[767]. The attack combined volumetric (DNS reflection) and application-layer (HTTPS GET floods).
September 2021	MID	Russian company Yandex was hit by a massive volumetric DDoS attack with nearly 22 million requests per second (RPS). The attack started in August and reached its peak on 5 September[768]. Meris botnet was used to execute the attack with an estimated 200,000 bots.[769]
September 2021	FAR	Critical services in New Zealand, including banks, post offices and weather forecasters, were the target of a wave of DDoS attacks[770]. The attacks were claimed to be a continuation of an attack against Vocus, the nation's third-largest ISP, which caused disruption to some of its customers[771].
August 2021	GLOBAL	Cloudfare customers were the target of a HTTP Volumetric DDoS attack that peaked at 17.2 million requests-per-second. According to Cloudfare *this attack reached 68% of our Q2 average rps rate of legitimate HTTP traffic*[772]. The traffic was generated using Meris botnet, including more than 20,000 bots in 125 countries around the world[773].

Table 8: Ukraine-Russia related attacks[774]

Time	Geographical Spread	Description
April 2022	MID	The Ukrainian Postal service Ukrposhta was the target of a DDoS attack just after it released a postal stamp picturing the war between Russia and Ukraine[775]. Online store and other Ukrposhta systems were temporarily not working (for almost 38 hours)[776].

[765] https://blog.mazebolt.com/list-of-ddos-attacks-december-2021?hsCtaTracking=046863b8-4bb8-4660-a086-5aec1133ad6d%7Ccab6a12d-d3ab-4227-9dd0-41bf27d5e5f1
[766] https://azure.microsoft.com/en-us/blog/azure-ddos-protection-2021-q3-and-q4-ddos-attack-trends/
[767] https://www.f5.com/labs/articles/threat-intelligence/2022-application-protection-report-ddos-attack-trends
[768] https://kfgo.com/2021/09/09/russias-yandex-says-it-repelled-biggest-ddos-attack-in-history/
[769] https://www.israeldefense.co.il/en/node/51843
[770] https://www.theregister.com/2021/09/08/new_zealand_ddos_attacks_widespread/
[771] https://www.theregister.com/2021/09/03/nz_outage/
[772] https://blog.cloudflare.com/cloudflare-thwarts-17-2m-rps-ddos-attack-the-largest-ever-reported/
[773] https://blog.cloudflare.com/meris-botnet/
[774] Sophos is monitoring cyberattacks under the Russia-Ukraine war. https://news.sophos.com/en-us/2022/03/21/russia-ukraine-war-related-cyberattack-developments/
[775] https://www.euronews.com/next/2022/04/22/ukraine-s-postal-service-hit-by-cyberattack-after-moskva-warship-stamp-goes-on-sale-online
[776] https://www.cybersecurity-insiders.com/ddos-cyber-attack-on-ukraines-postal-department/
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Time	Geographical Spread	Description
March 2022	MID	Zscaker reported a series of HTTP-based DDoS attacks on the Ukrainian Ministry of Defence's webmail server. The threat actor based its activities on DanaBot, a Malware-as-a-Service platform, to deliver a second-stage malware payload using the download and execute command[777].
March 2022	MID	Triolan, a major Ukrainian Internet provider has been the target of severe DDoS attacks, causing severe internet outages during the Russian invasion. In particular, some internal devices were reset to factory settings. Triolan suspended services for a day, while Ukrtelecom experienced a different internet blackout[778] [779].
February 2022	MID	Different DDoS attacks targeted the website of Ukraine's Ministry of Defence and various financial institutions such as Oschadbank and PrivatBank, as well as the hosting provider Mirohost. The attack was based on flooding with incoming messages, connection requests and malformed packets[780]. Ukraine's public radio was also attacked. Customers of PrivatBank also received a message alerting them that the bank's ATM machines were not working, causing confusion[781]. Additional attacks targeted the websites of Ukraine's Ministry of Foreign Affairs, Ministry of Internal Affairs, the Security Service of Ukraine, and the Cabinet of Ministers.
February 2022	MID	A DDoS attack made Russian state news site RT unavailable for a couple of days. The hacktivist collective Anonymous seems to have claimed responsibility for the attack[782].
February 2022	MID	Rostec, a Russian state-owned aerospace and defence conglomerate, was a target of a DDoS attack that took its website down. The attack was apparently brought by the IT Army, a large group of volunteers that have been targeting Russian state networks and organisations since Russia's invasion[783].

Table 9: Attacks on the web and media

Time	Geographical Spread	Description
April 2022	NEAR	The Romanian national cyber security and incident response team, DNSC, reported an attack from pro-Russian group Killnet, which targeted several public government sites with a high number of requests and a high volume of data. The attack exploited compromised network equipment outside the country and targeted web apps (OSI level 7)[784].
April 2022	NEAR	Estonian government websites were temporarily blocked by DDoS attacks querying them several thousand times the normal traffic flow[785].
December 2021 March 2022	FAR	Philippines media was the target of a wave of DDoS attacks. In March 2022, the online news platform Interaksyon, news and information website PressOne.ph, newspaper Mindanao Gold Star Daily came under malicious DDoS attacks flooding their web sites[786] [787].

[777] https://www.zscaler.com/blogs/security-research/danabot-launches-ddos-attack-against-ukrainian-ministry-defense
[778] https://www.cpomagazine.com/cyber-security/major-ukrainian-internet-provider-triolan-suffers-severe-cyber-attacks-and-infrastructure-destruction-during-russian-invasion/
[779] https://blog.mazebolt.com/list-of-ddos-attacks-march-2022
[780] https://www.computerweekly.com/news/252513489/DDoS-attacks-hit-Ukrainian-defence-ministry-and-banks
[781] https://therecord.media/ddos-attacks-hit-websites-of-ukraines-state-banks-defense-ministry-and-armed-forces/
[782] https://www.wired.com/story/russia-ukraine-ddos-nft-nsa-security-news/
[783] https://www.bleepingcomputer.com/news/security/russian-defense-firm-rostec- shuts-down-website-after-ddos-attack/
[784] https://www.bleepingcomputer.com/news/security/russian-hacktivists-launch-ddos-attacks-on-romanian-govt-sites/
[785] https://news.err.ee/1608575371/ddos-attacks-on-estonian-state-sites-continued-over-weekend
[786] https://blog.mazebolt.com/list-of-ddos-attacks-march-2022
[787] https://newsinfo.inquirer.net/1569602/3-more-news-sites-under-cyberattack-nujp
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Time	Geographical Spread	Description
		In February 2022, a DDoS attack targeted the CNN Philippines website during a presidential debate, causing one of the candidates to remain off debate[788]. In December 2021, ABS-CBN was made unavailable for 6 hours[789], while Rappler web site received a DDoS peaking at 650,000 rps[790], followed by another one peaking at one million rps.
December 2021	GLOBAL	FlexBooker, an appointment scheduling and calendar service, suffered a data breach of 3.7 million accounts, which was executed after a DDoS attack that targeted the company's Amazon AWS servers[791]. The attack was carried out by threat group Uawrongteam and was probably a distraction for implementing the data breach.
September 2021	NEAR	The website of the Federal Returning Officer in Germany was the target of a DDoS attack related to the September elections of the Bundestag. According to Germany, it probably originated in Russia with the goal of gaining access to the private e-mail accounts of federal and regional MPs[792].
July 2021	FAR	BitCoin.org was the target of a RDoS composed of a massive volumetric DDoS attack with a ransom demand of 0.5 Bitcoin (BTC)[793].
July 2021	MID	Infosecurity magazine was the target of a DDoS attack, which made the web site unavailable and caused a switch to a more robust hosting provider[794].

Table 10: Attacks on internet, infrastructure, and telecommunication providers

Time	Geographical Spread	Description
May 2022	NEAR	The Port of London Authority was hit by a DDoS that took its website offline for 24 hours. The attack was launched by Pro-Iran Group Altahrea[795].
May 2022	NEAR	Italian websites of the Senate, the Ministry of Defence and the National Health Institute were targeted by a DDoS attack launched by Russian hackers with the intent of targeting NATO countries[796].
March 2022	FAR	The Israeli ISP Cellcom was the target of a large-scale DDoS attack, which resulted in government resources, that is, ministry websites, being offline for a while.
January 2022	MID	Andorra Telecom was hit by a DDoS attack that temporally stopped communications in the country[797]. According to the media the targets were the participants in the Twitch Rivals Squidcraft Games, a Minecraft tournament based on Squid Game[798]. There are suspicions that the target was not the Andorra government and its citizens (they were just collateral damage) but rather some Andorra streamers who were unable to continue the game to win the top prize of $100,000.

788 https://newsinfo.inquirer.net/1560772/cyber-attack-hits-cnn-philippines-website-during-presidential-debate
789 https://news.abs-cbn.com/news/12/11/21/abs-cbn-news-website-hit-by-cyber-attack
790 https://www.rappler.com/technology/rappler-website-under-cyberattack/
791 https://www.cpomagazine.com/cyber-security/3-7-million-flexbooker-accounts-leaked-to-hacker-forum-after-ddos-attack/
792 https://www.straitstimes.com/world/europe/german-election-authority-confirms-likely-cyber-attack
793 https://decrypt.co/75276/bitcoin-org-reportedly-hit-ddos-attack-ransom-demand
794 https://techgenix.com/infosecurity-magazine-ddos-attack/
795 https://www.hackread.com/pro-iran-altahrea-hit-port-of-london-website-ddos-attack/
796 csis.org/programs/strategic-technologies-program/significant-cyber-incidents
797 https://therecord.media/ddos-attacks-on-andorras-internet-linked-to-squid-game-minecraft-tournament/
798 https://www.tomshardware.com/news/minecraft-ddos-attack-leaves-small-european-country-without-internet
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Time	Geographical Spread	Description
January 2022	FAR	A wave of DDoS attacks targeted North Korea and its infrastructures, taking them out of connectivity for hours and affecting the connectivity of 25 million people[799]. North Korea's core services were unreachable causing North Korea to disappear from the internet[800] [801]. The attacks implemented a flooding approach with unusually high volumes of data traffic[802]. According to Seoul-based NK Pro, *log files and network records showed websites on North Korean web domains were largely unreachable because North Korea's Domain Name System (DNS) stopped communicating the routes that data packets should take*[803].
October 2021	FAR	NITCO ISP received a massive DDoS attack, flooding the network and affecting the operation of NITCO's services[804]. The attack originated from a large botnet[805].
September 2021	FAR	The cybercriminal group DarkSide launched a DDoS attack against Colonial Pipeline, the largest refined oil pipeline system in the USA[806]. The company lost access to computer systems and suffered a data breach of over 100 GB of corporate data[807]. DarkSide offers both DDoS and call centre services, guaranteeing their customers to support quadruple extorsion techniques[808] [809] affecting whole supply chains[810] [811]. According to Trend Micro[812] *malicious actors could deny access to critical data such as manufacturing secrets, withhold access to machines used in production or contact customers and stakeholders to pressure victim organisations to pay up.*
July 2021	FAR	Kaseya Virtual Systems Administrator (VSA) was hit by REvil ransomware to attack Managed Security Service Providers that controlled the infrastructure of thousands of companies[813]. It is not reported how many of the millions of end point systems were encrypted.

B.6 THREATS AGAINST AVAILABILITY (INTERNET THREATS)

Table 11: Notable incidents against availability

Time	Geographical Spread	Description

[799] https://blog.mazebolt.com/list-of-ddos-attacks-january-2022?hsCtaTracking=125a9135-2b30-4f1d-af7a-0385ee0494c7%7C4530f3bc-b5e5-4ce2-9809-5faca26a9780
[800] https://www.nknews.org/2022/01/north-korea-kicked-off-internet-by-suspected-ddos-attack/
[801] https://blog.mazebolt.com/list-of-ddos-attacks-january-2022?hsCtaTracking=125a9135-2b30-4f1d-af7a-0385ee0494c7%7C4530f3bc-b5e5-4ce2-9809-5faca26a9780
[802] https://www.reuters.com/world/asia-pacific/nkorean-internet-downed-by-suspected-cyber-attacks-researchers-2022-01-26/
[803] https://www.reuters.com/world/asia-pacific/nkorean-internet-downed-by-suspected-cyber-attacks-researchers-2022-01-26/
[804] https://blog.mazebolt.com/list-of-ddos-attacks-october-2021?hsCtaTracking=e19be14c-53e4-4c91-8f8a-1d1553eb1d45%7C6454852c-c358-42d7-9f74-a756bade1c8e
[805] https://www.news-gazette.com/news/our_county/ford_county/nitco-recent-outages-due-to-denial-of-service-attacks/article_d911a2b3-a36d-506b-8b43-8bc4488829c8.html
[806] Trend Micro - toward a new momentum security predictions for 2022
[807] Trend Micro. (Sept. 14, 2021). Trend Micro 'Attacks From All Angles: 2021 Midyear Cybersecurity Report' Accessed on Nov. 25, 2021, at https://www.trendmicro.com/vinfo/us/security/research-and-analysis/threat-reports/roundup/attacks-from-all-angles-2021-midyear-security-roundup
[808] Trend Micro - toward a new momentum security predictions for 2022
[809] The Global Economic Forum, The Global Risks Report 2022 17th Edition, 2022 https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2022.pdf
[810] Brian Krebs. (May 11, 2021). Krebs On Security. 'A Closer Look at the DarkSide Ransomware Gang'. Accessed on Nov. 25, 2021, at https://krebsonsecurity.com/2021/05/a-closer-look-at-the-darkside-ransomware-gang/
[811] Janus Agcaoili et al. (June 15, 2021). Trend Micro Security News. 'Ransomware Double Extortion and Beyond: REvil, Clop, and Conti'. Accessed on Nov. 5, 2021, at https://www.trendmicro.com/vinfo/us/security/news/cybercrime-and-digital-threats/ransomware-double-extortion-and-beyond-revil-clop-and-conti
[812] Trend Micro - toward a new momentum security predictions for 2022
[813] https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf

February 2022	FAR	KlaySwap crypto users lose funds after BGP hijack: hackers have stolen roughly $1.9 million from South Korean cryptocurrency platform KLAYswap after they pulled off a rare and clever BGP hijack against the server infrastructure of one of the platform's providers.
March 2022	FAR	BGP Hijacking of Twitter Prefix by RTComm.ru RTComm.ru started to advertise 104.244.42.0/24, a prefix used by Twitter. RTComm.ru is a sizeable Russian telecom provider. Russian ISPs have started restricting access to Twitter after Russia's invasion of Ukraine led to many Twitter posts critical of Russia's war.

B.7 DISINFORMATION - MISINFORMATION

Table 12: Notable disinformation - misinformation incidents

Time	Geographical Spread	Description
January 2022	NEAR	COVID-related disinformation increased attacks on health structures and personnel. This problem existed before the pandemic and was strengthened by disinformation attacks during the pandemic. Vaccination teams were attacked by anti-vaxxers and the president of the Czech Medical Chamber received protection by the police[814].
November 2021	NEAR	Mateusz Morawiecki, President of Poland, on a visit to Latvia discussed various disinformation attacks and fake news targeting the eastern part of NATO regarding migration, COVID vaccines, energy and international relations between the EU and NATO[815].
October 2021	GLOBAL	Fossil fuel companies have been accused of disinformation activities around climate crisis. This includes activities in social media (e.g. ads)[816].
September 2021	NEAR	The French elections and all candidates were the target of mass disinformation and misinformation attacks[817] [818] [819]. For instance, false claims were reported about a mass immigration statement attributed to President Macron and BBC news. Other claims targeted voting machines as a means to ensure a Macron victory. Nicolas Dupont-Aignan was falsely associated with a claim on the fact that *If there is no participation, this election will not be valid*. Marine Le Pen was falsely associated with a claim on the fact that she intended to withdraw France from the 2015 Paris Agreement on climate change.
September 2021	NEAR	Security Company Mandiant observed that UNC1151 and ghostwriter activities could be linked to Belarus and its interests with high confidence. The disinformation campaigns shared anti-NATO narratives with the goal of reducing support and cooperation in Lithuania, Latvia and Poland. The narratives targeted the cost of NATO membership and the possible threats due to the presence of foreign troops in the countries[820] [821]. This continued into the following months and the beginning of 2022.

[814] https://www.bbc.com/news/world-europe-60111142
[815] https://www.polskieradio.pl/395/7989/Artykul/2853213,Polish-PM-warns-of-fake-news-hacker-attacks-by-Belarus-Russia
[816] https://edition.cnn.com/2021/10/28/politics/fossil-fuel-oversight-hearing-climate/index.html
[817] https://www.bbc.com/news/61179620
[818] https://www.euronews.com/my-europe/2022/04/22/french-election-2022-misinformation-spreads-online-ahead-of-runoff-vote
[819] https://www.newsguardtech.com/special-reports/french-election-misinformation-tracker/
[820] https://www.mandiant.com/resources/unc1151-linked-to-belarus-government
[821] https://www.mandiant.com/resources/unc1151-linked-to-belarus-government

Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Time	Geographical Spread	Description
September 2021	NEAR	In the German elections all candidates for the chancellorship have been the target of mass disinformation attacks and fake news on social media[822] [823]. According to Deutsche Welle, *Traditional media also play a role in spreading falsehoods*[824].
September 2021	NEAR	The continuation of the second COVID infection wave was followed by continuous disinformation around the efficacy of COVID vaccines and the reliability of pharmaceutical companies. This has been surrounded by continuous political themes and anti-West messages.
July 2021	NEAR	Disinformation and misinformation targeting COVID vaccines continue, showing that 12 individuals were responsible for more than 65% of the misinformation posts on social media.[825]

Table 13: War-related disinformation/misinformation incidents

Time	Geographical Spread	Description
June 2022	NEAR	The mayors of Berlin, Madrid and Vienna were the targets of a deepfake disinformation attack. The three mayors had been involved in a video call with a deepfake of their counterpart in Kyiv, Vitali Klitschko[826].
May 2022	MID	According to Meduza, Yandex, the 'Google of Russia', supported Russian propaganda. In particular, censorship activities were observed in the Yandex News Feed used by up to 50 million users to promote the Kremlin's agenda before and after the war in Ukraine began[827].
May 2022	MID	TikTok has been used as a disinformation vector during the Russia-Ukraine war, benefiting from its design choice for quick and non-validated posts[828] [829]. According to the BBC, false TikTok videos and live streams collected millions of views about the war[830]. Also, according to Media Matters, a pro-Russia disinformation campaign used over 180 TikTok influencers to support the war against Ukraine.
May 2022	MID	The largest social networks (e.g. Twitter, YouTube) have been used to spread disinformation around the war[831]. Social media providers put a lot of effort into counteracting the spread of fake information.
April 2022	MID	Russian diplomats, as well as reporting on Ukraine by Chinese, Iranian and Russian state-backed media in English, saw a peak of engagements in social media[832].

[822] https://www.bbc.com/news/world-europe-58655702
[823] https://www.institutmontaigne.org/en/blog/disinformation-2021-german-federal-elections-what-did-and-did-not-occur
[824] https://www.dw.com/en/disinformation-fake-news-plague-german-election-campaign/a-59104314
[825] Center for Countering Digital Hate (CCDH), The Disinformation Dozen, 2021
[826] https://www.theguardian.com/world/2022/jun/25/european-leaders-deepfake-video-calls-mayor-of-kyiv-vitali-klitschko
[827] https://demtech.oii.ox.ac.uk/war-in-ukraine-and-disinformation-newsletter-12-may-2022/
[828] https://demtech.oii.ox.ac.uk/war-in-ukraine-and-disinformation-newsletter-12-may-2022/
[829] https://www.mediamatters.org/tiktok/pro-russia-propaganda-campaign-using-over-180-tiktok-influencers-promote-invasion-ukraine
[830] https://www.bbc.com/news/60867414
[831] https://demtech.oii.ox.ac.uk/war-in-ukraine-and-disinformation-newsletter-26-may-2022/
[832] https://demtech.oii.ox.ac.uk/war-in-ukraine-and-disinformation-newsletter-26-april-2022/

Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Time	Geographical Spread	Description
March 2022	NEAR	A substantial wave of fake news and disinformation on Ukraine targeted Serbia, Bosnia, and Hungary. Religion and nationalism pushed online attacks and hate speech in Bosnia and North Macedonia[833].
March 2022	FAR	A conspiracy theory built on the narrative of 'secret' US research laboratories in Ukraine to develop biological weapons has been distributed by China and QAnon[834].
March 2022	MID	AI-enabled disinformation based on deepfakes took an important role in the war and resulted in videos of Russia's Vladimir Putin and Ukraine's Volodymyr Zelenskyy with messages supporting the points of view of adversaries[835] [836].
July 2021	MID	According to Ukraine's Defence Ministry, Russian government hackers targeted the Ukrainian Navy website to spread disinformation about the multinational Sea Breeze military exercises in the Black Sea[837].

B. 8 SUPPLY CHAIN ATTACKS

Table 14: Notable supply chain Incidents

Time	Geographical Spread	Description
December 2021	GLOBAL	Log4j CVE: a vulnerability was found in Log4j, an open-source logging library commonly used by apps and services across the internet. If left unfixed, attackers can break into systems, steal passwords and logins, extract data, and infect networks with malicious software.
March 2022	GLOBAL	A threat actor dubbed RED-LILI has been linked to an ongoing large-scale supply chain attack campaign targeting the NPM package repository by publishing nearly 800 malicious modules.

[833] https://balkaninsight.com/2022/03/04/ukraine-war-prompts-flood-of-misinformation-fake-news/
[834] https://www.france24.com/en/europe/20220312-china-and-qanon-embrace-russian-disinformation-justifying-war-in-ukraine
[835] https://www.dw.com/en/fact-check-the-deepfakes-in-the-disinformation-war-between-russia-and-ukraine/a-61166433
[836] https://securityaffairs.co/wordpress/129124/intelligence/russia-deepfake-video-zelenskyy.html
[837] https://www.rferl.org/a/ukraine-hack-russia-navy-sea-breeze/31351045.html


CVE

C ANNEX: CVE LANDSCAPE

The analysis of the vulnerability landscape is intended to identify trends and help stakeholders improve their patch prioritisation practices by tracking the most popular vulnerabilities that are commonly used in cyberattacks and also aid developers in fixing common root causes for vulnerabilities by observing the main weaknesses behind these vulnerabilities. Moreover, this work is meant to complement the ETL by giving a glimpse into the vulnerabilities that are often leveraged in cyberattacks.

C.1 SUMMARY

A total of 21,920[838] vulnerabilities were identified during the period of this report.

Also, within the given timeframe, 134 out of 21,920 published vulnerabilities are referenced in the 'CISA Known Exploited Vulnerabilities catalogue', later referred to as KEV.

In future editions of the ETL we are aiming to include information on the vulnerabilities associated with the recorded incidents.

C.2 ANALYSIS

A CVE Numbering authority is an organisation responsible for the regular assignment of CVE IDs to vulnerabilities and for creating and publishing information about the vulnerability in the associated CVE Record. Each CNA has a specific scope of responsibility for vulnerability identification and publishing.

For better context, Figure 16 below details the percentage of the CVE numbers assigned by each CVE numbering organisation (CNA) for the given period:

[838] Not all vulnerabilities are relevant as some of them are Rejected/Disputed

Figure 16 Percentage of CVE numbers assigned by each CNA

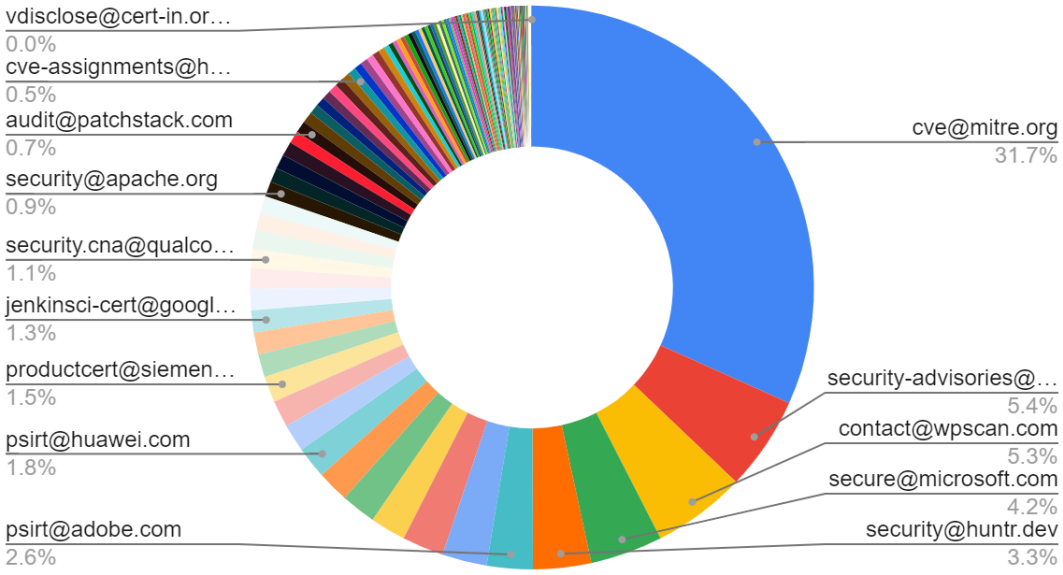
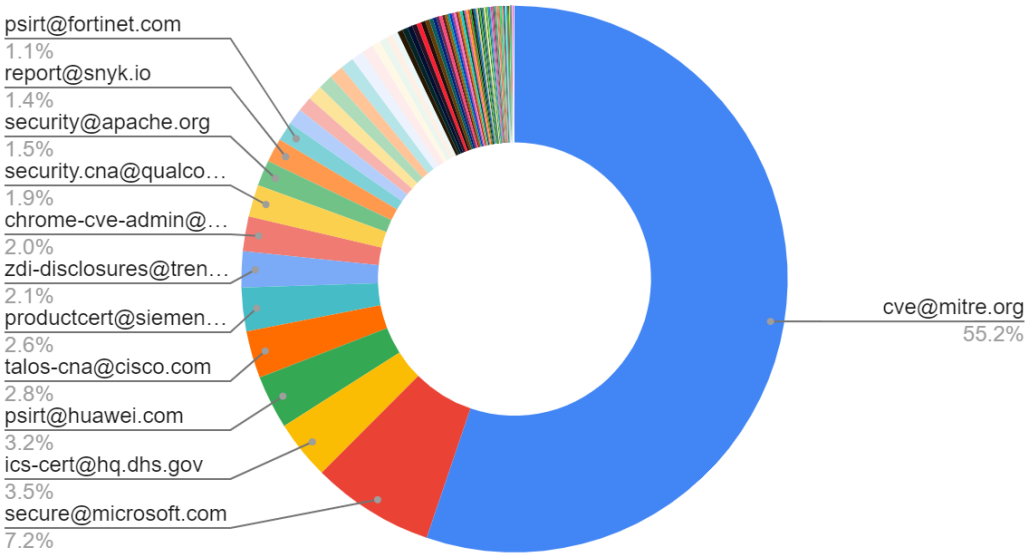


Figure 17 ranks the percentage of CVE numbers assigned by CNAs that have an average CVSS score greater than 7 for each CNA:

Figure 17 Percentage of CVEs with an average CVSS greater than 7 by CNA



In Figure 18 below, we highlight the CNAs allocating CVEs that appear as part of CISA's known exploit vulnerability catalogue.

Figure 18 Allocation of CVEs that appear in CISA's known exploit vulnerability catalogue

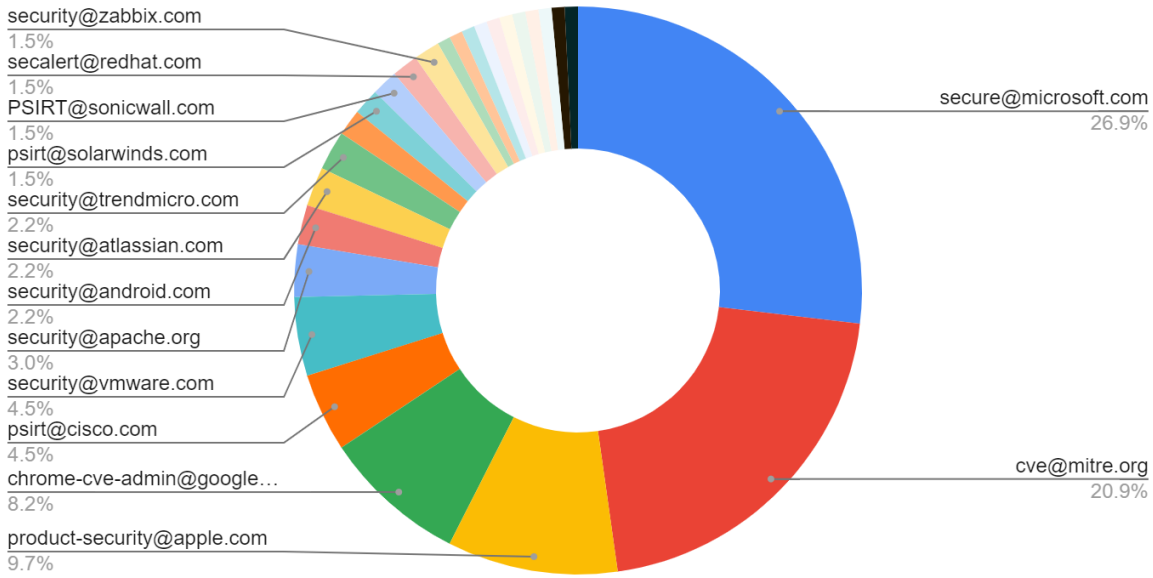
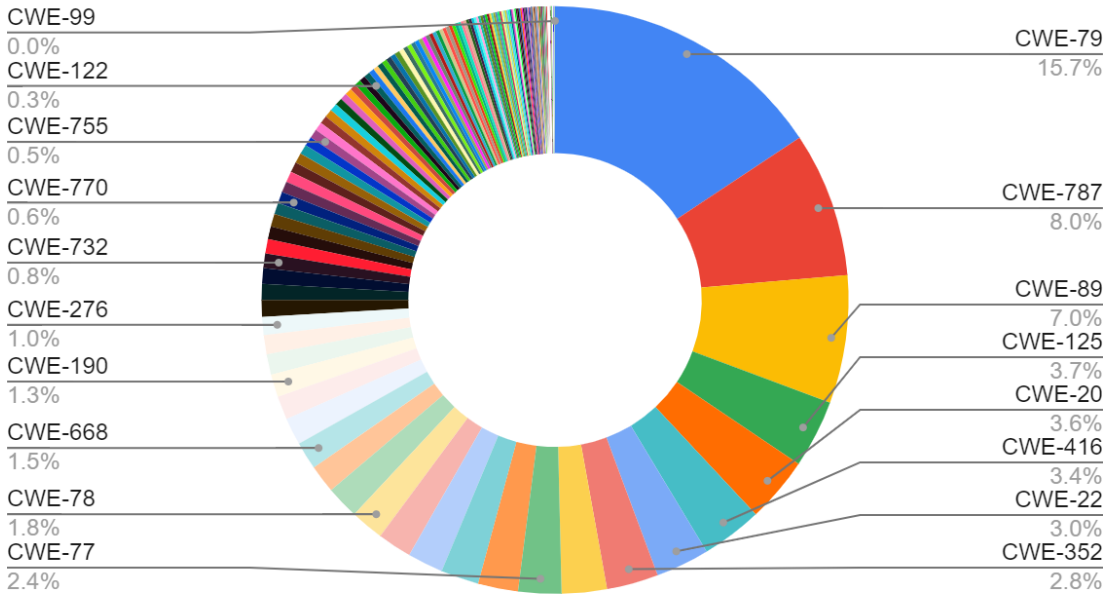


Figure 19 ranks the top weaknesses by count for the entire NVD data set (Total of 21,290 vulnerabilities) during the given timeframe.

Figure 19 Top weaknesses by count



The following table covers the same data as above, but this time together with a description to give a better understanding of the context.

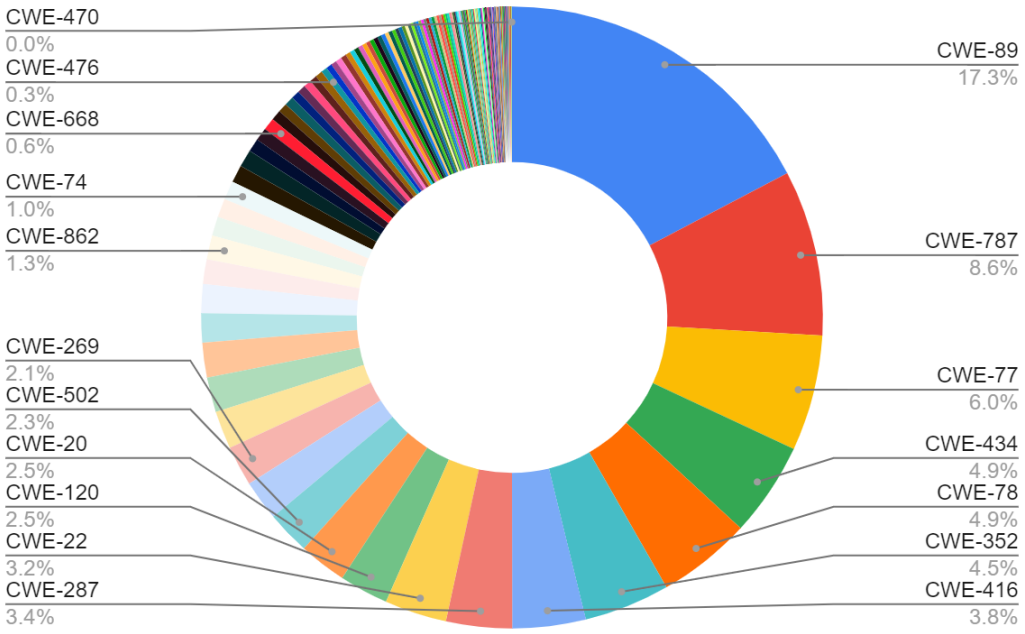
Table 15: Top weaknesses' description

CWE	Description	Count
CWE-79	Improper Neutralisation of Input During Web Page Generation ('Cross-site Scripting')	2868
CWE-787	Out-of-bounds Write	1458
CWE-89	Improper Neutralisation of Special Elements used in an SQL Command ('SQL Injection')	1287
CWE-125	Out-of-bounds Read	683
CWE-20	Improper Input Validation	658
CWE-416	Use After Free	613
CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	541
CWE-352	Cross-Site Request Forgery (CSRF)	521
CWE-269	Improper Privilege Management	454
CWE-77	Improper Neutralisation of Special Elements used in a Command ('Command Injection')	433
CWE-476	NULL Pointer Dereference	403
CWE-863	Incorrect Authorisation	383
CWE-287	Improper Authentication	360
CWE-434	Unrestricted Upload of File with Dangerous Type	344

The list shows that well known web related weakness such as Cross-site scripting, SQL Injection, Improper input validation, and Cross-Site Request Forgery are still responsible for many of the reported vulnerabilities. This is very interesting when considering the increased usage of cloud based services.

In Figure 20 below we can see the most important weaknesses (CWEs) that correlate to vulnerabilities having an average CVSS score higher than 8.

Figure 20 Weaknesses that correlate to a CVSS score higher than 8



The following table lists the same data as above but includes the matching description (the data was filtered to include just the vulnerabilities with CVSS score higher than 8).

Table 16 CWE description

CWE Count	CWE ID	CWE description	Average of base Score
871	CWE-89	Improper Neutralisation of Special Elements used in an SQL Command ('SQL Injection')	9.529161883
433	CWE-787	Out-of-bounds Write	9.350115473
303	CWE-77	Improper Neutralisation of Special Elements used in a Command ('Command Injection')	9.50990099
247	CWE-434	Unrestricted Upload of File with Dangerous Type	9.401214575
245	CWE-78	Improper Neutralisation of Special Elements used in an OS Command ('OS Command Injection')	9.360408163
224	CWE-352	Cross-Site Request Forgery (CSRF)	8.7625
192	CWE-416	Use After Free	8.9515625
172	CWE-287	Improper Authentication	9.487790698

CWE Count	CWE ID	CWE description	Average of base Score
163	CWE-22	Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	9.082208589
128	CWE-120	Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	9.46953125
125	CWE-20	Improper Input Validation	9.2296
114	CWE-502	Deserialisation of Untrusted Data	9.334210526
105	CWE-94	Improper Control of Generation of Code ('Code Injection')	9.316190476
105	CWE-269	Improper Privilege Management	9.000952381

Further on we will look into CISA's known exploited vulnerabilities catalogue for the given time span. At this point we will also introduce the corresponding EPSS (exploit prediction score) for all the vulnerabilities of the data set.

In Figure 21 below it is noticeable that most of the vulnerabilities that appear in the KEV catalogue correlate with a high EPSS score. The bigger the square, the higher the score (indicating the popularity of the vulnerability). Nevertheless the smaller squares from the lower right corner confirm that there are many other vulnerabilities confirmed to be used in cyberattacks however lacking in online popularity.

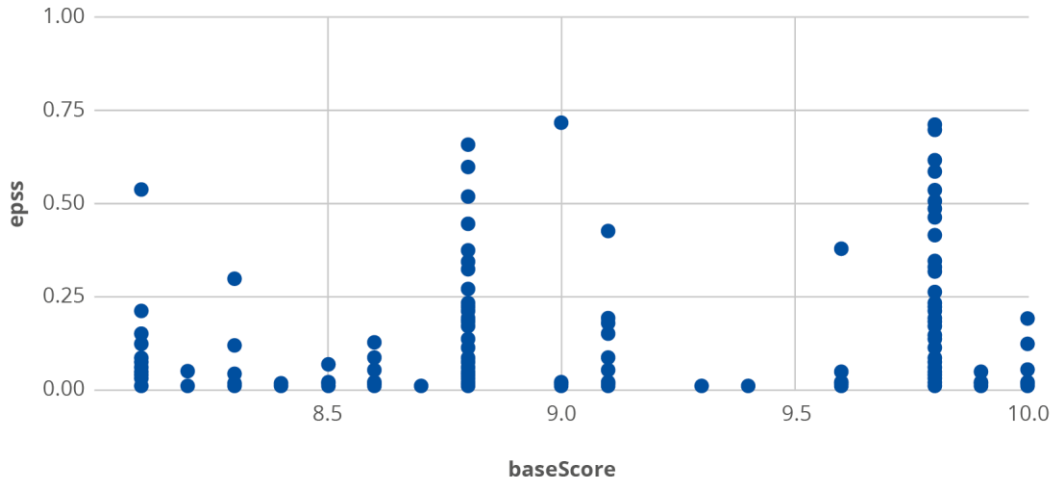
The focus of the defenders in terms of patching prioritisation should not be only on the 'popular' vulnerabilities that get a lot of attention (e.g. due to the wide usage of a product), but also on the less common vulnerabilities from CISA's KEV catalogue.

Figure 21 Tree map visualisation of the KEV together with their EPSS score

In Figure 22 below you can see a plot of the exploit prediction scores over the BaseScore (severity) of the NVD vulnerabilities. Extra attention should be given to the high CVSS score vulnerabilities that correlate to a lower EPSS score.

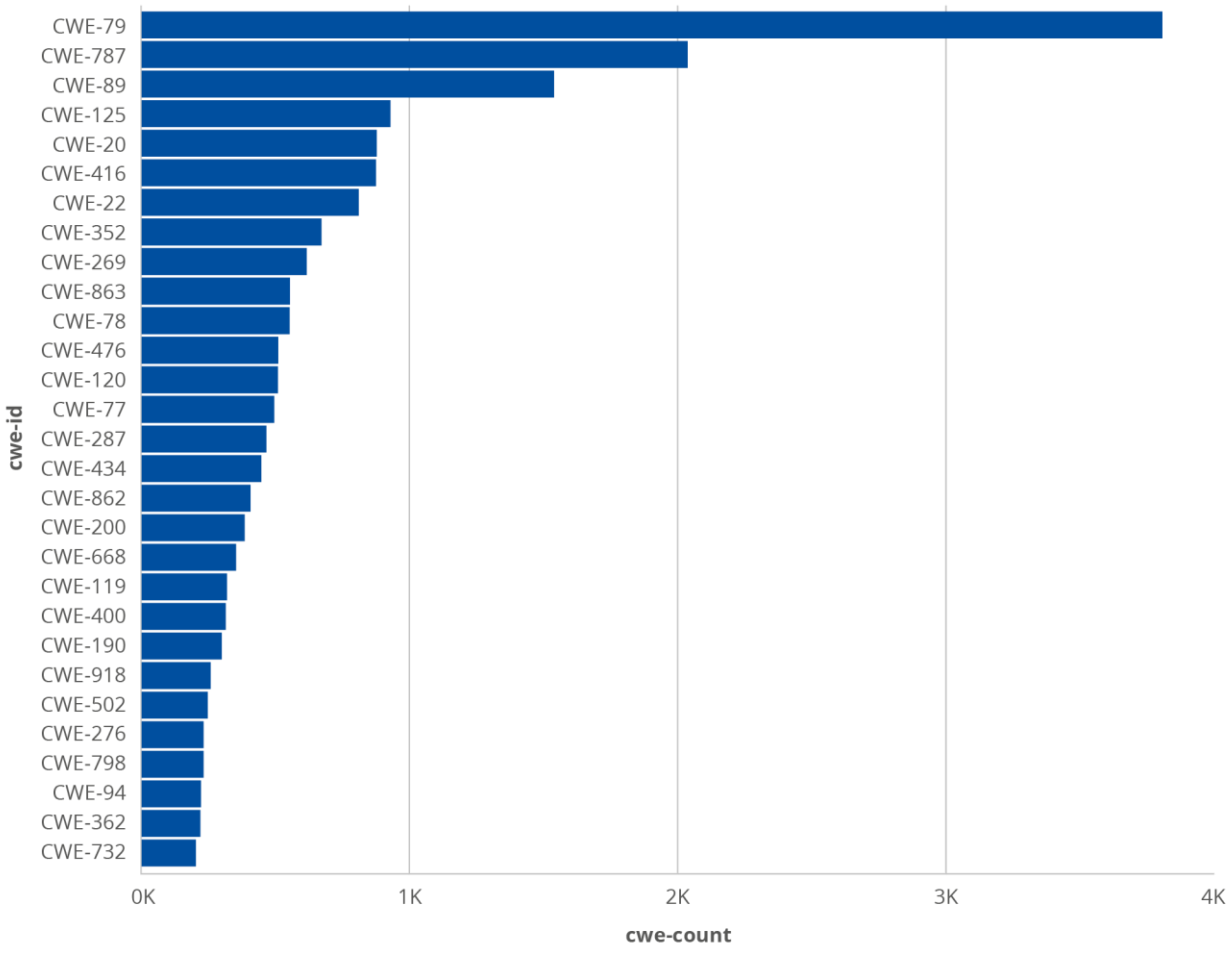
It is noticeable that roughly 2919 high severity vulnerabilities (CVSS above 9.5) are associated with a low Exploit Prediction Scoring System (EPSS). The patching prioritisation process should account also for these high severity vulnerabilities and not rely solely on the ones with high EPSS scores.

Figure 22 Exploit Prediction Scoring System (EPSS) with BaseScore (severity score)



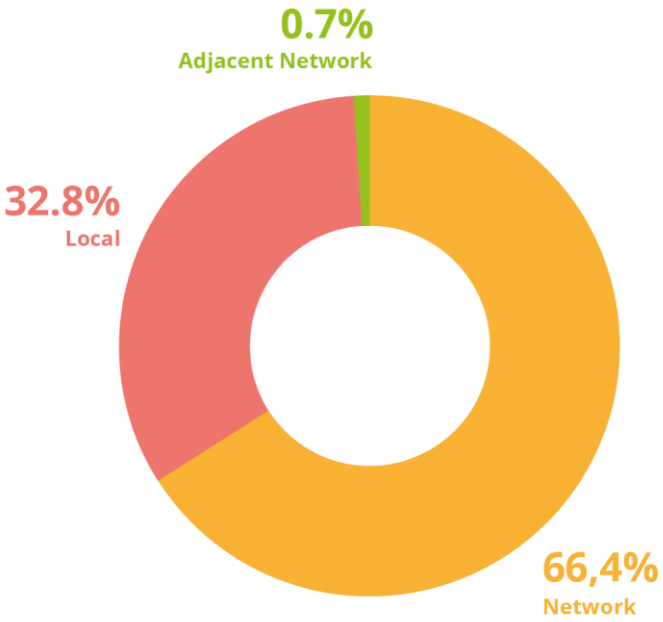
In Figure 23 below you can see the main weaknesses associated with KEV vulnerabilities from the given timeframe:

Figure 23 Top count of CWEs for KEV



Another important observation for the KEV data set is the fact that 66.4% of the 134 vulnerabilities are network exploitable, probably associated with remote exploits, and 32.8% are local exploitable which means they are likely used in privilege escalation tactics. Threats actors could leverage a combination of the two types in order to compromise organisations, as shown in Figure 24 below.

Figure 24 Network exploitation



C.3 BACKGROUND

For the analysis of the CVE landscape, the following data sources were utilised:

- NIST NVD (National Vulnerability Database): https://nvd.nist.gov/vuln/full-listing
- CISA known exploited vulnerability catalogue (KEV[839]) snapshot as of 12 August 2022: https://www.cisa.gov/known-exploited-vulnerabilities-catalog
- FIRST Exploit prediction scoring system (EPSS)[840]: more details regarding EPSS available at https://www.first.org/epss/ and here https://www.first.org/epss/data_stats

[839] 'CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild, i.e. the Known Exploited Vulnerability (KEV) catalogue. CISA strongly recommends all organisations review and monitor the KEV catalogue and prioritise remediation of the listed vulnerabilities to reduce the likelihood of compromise by known threat actors.'
[840] The Exploit Prediction Scoring System (EPSS) is a community-driven effort to combine descriptive information about vulnerabilities (CVEs) with evidence of actual exploitation in-the-wild. The higher the score, the greater the probability that a vulnerability will be exploited (in the next 30 days).

D ANNEX: RECOMMENDATIONS

Our recommendations are mapped[841] to the security measures that are part of international standards used by operators in the business sectors as documented[842] by ENISA.

SOCIAL ENGINEERING

Review and update the incident response plans to adapt to the new trends identified for social engineering attacks.	
ISO/IEC 27001:2013 A16.1 Management of information security incidents & improvements	**NIST Cybersecurity Framework (CSF)** 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 organization 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 4.1 Understanding the organization 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	**NIST Cybersecurity Framework (CSF)** 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 organization 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)**

[841] 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.
[842] Minimum Security Measures for Operators of Essentials Services https://www.enisa.europa.eu/topics/nis-directive/minimum-security-measures-for-operators-of-essentials-services

5.3 Organizational 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 framework[843].** **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 organizational 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.** **Utilize e-mail security features that notify a user when an e-mail is being sent from a user they have not interacted with before.**	

[843] AIL Framework https://github.com/CIRCL/AIL-framework

ISO/IEC 27001:2013	NIST Cybersecurity Framework (CSF)
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	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)**
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 organizational stakeholders ID.GV-1: Organizational cybersecurity policy is established and communicated

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 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	**NIST Cybersecurity Framework (CSF)** Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized 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 organization'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 centralize 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 organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization'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.**	

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	NIST Cybersecurity Framework (CSF)
A.12.4.1 Event Logging A.14.2.7 Outsourced Development A.15.2.1 Monitoring and review of supplier services	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.

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 Organizational 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 organizational 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.844

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 organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. PR.MA-1: Maintenance and repair of organizational 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.

[844] 2022 Thales Data Threat Report
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Support for compliance and certification:845	
ISO/IEC 27001:2013 A.5.1.1 Policies for information security A.12.7.1 Information systems audit controls 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	**NIST Cybersecurity Framework (CSF)** Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, 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
Authorization Management: Human errors and misconfigurations are at the basis of many data breaches. A proper authorization management that reviews access privileges according to changing rights of the users, users leaving an organization is key to reduce possible insider threat attacks. 846 **Zero trust architectures: Zero trust architectures can increase the security posture of a system by implementing "never trust, always verify" paradigm. 847 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. 848 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 organizations. 849** **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 properly trained and know the most recent cybersecurity trends. The first should increase their knowledge to implement security controls and properly manage data; the latter should undergo basic training in database security. 850 The need of a security awareness program stands out when social attacks are executed and result in malware installation and stolen credentials. 851**	
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 organization'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 authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions. PR.PT-3: The principle of least functionality is incorporated by configuring systems to provide only essential capabilities

845 https://artificialintelligenceact.eu/
846 EU H2020 CONCORDIA, D4.3
847 https://www.wsav.com/wp-content/uploads/sites/75/2022/01/20220124_ITRC-2021-Data-Breach-Report.pdf
848 https://blog.f-secure.com/data-breach-and-data-leak-whats-the-difference/
849 EU H2020 CONCORDIA, D4.3
850 EU H2020 CONCORDIA, D4.3
851 https://www.verizon.com/business/resources/reports/2022/dbir/2022-data-breach-investigations-report-dbir.pdf
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

Data security auditing: The support of security auditing is key to identify organizational gaps and vulnerabilities, as well as data misuse. 852 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. 853	
ISO/IEC 27001:2013 A.12.7.1 Information systems audit controls A.18.2 Information security reviews	**NIST Cybersecurity Framework (CSF)** 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 sanitization: Data sanitization enables end-users to protect their data by decreasing the quality of data according to different techniques including anonymization, generalization, encryption, masking, filtering. Manipulated data can then be used for testing, training, processing. 854 855 **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,856 replacement and healing.857 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. 858 859** **Adversarial training: Adversarial training is important to protect a ML model against inference-time attacks. It builds on training set augmentation (adversarial training),860 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

[852] EU H2020 CONCORDIA, D4.3
[853] EU H2020 CONCORDIA, D4.3
[854] EU H2020 CONCORDIA, D4.3
[855] 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.
[856] N. Peri, N. Gupta, W. R. Huang, L. Fowl, C. Zhu, S. Feizi, T. Goldstein, and J. P. Dickerson, “Deep k-NN Defense Against Clean-Label Data Poisoning Attacks,” in Proc. of ECCV 2020, August 2020.
[857] E. Rosenfeld, E. Winston, P. Ravikumar, and Z. Kolter, “Certified Robustness to Label-Flipping Attacks via Randomized Smoothing,” in Proc. of
ICML 2020, Virtual, June 2020.
[858] 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.
[859] W. Wang, A. Levine, and S. Feizi, “Improved Certified Defenses against Data Poisoning with (Deterministic) Finite Aggregation,” arXiv preprint arXiv:2202.02628, 2022.
[860] A. Kurakin, D. Boneh, F. Tramèr, I. Goodfellow, N. Papernot, and P. McDaniel, “Ensemble Adversarial Training: Attacks and Defenses,” in Proc. of ICLR 2018, Vancouver, BC, Canada, April, May 2018.
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

	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: Organizational communication and data flows are mapped
Data backups: Data backups are fundamental to support prompt recovery from attacks. 861 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 organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational 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 organizational 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): Organizational 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 centers, 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	**NIST Cybersecurity Framework (CSF)**

[861] EU H2020 CONCORDIA, D4.3

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 A.16.1.4 Assessment of and decisions on information security events A.16.1.7 Collection of evidence	ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value Risk Management Strategy (ID.RM): The organization'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 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, analyze and respond to vulnerabilities disclosed to the organization 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 organization'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 organizational 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): Organizational 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 centers, 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[862]. All critical elements (e.g. servers, services and applications) should be protected and included in recurrent tests of a DDoS mitigation plan[863].	

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

ISO/IEC 27001:2013	NIST Cybersecurity Framework (CSF)
6 Planning 7.5.3 Control of documented information 8 Operation 8.1 Operational planning and control 9.3 Management review 10 Improvement 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	ID.GV-4: Governance and risk management processes address cybersecurity risks Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. Risk Management Strategy (ID.RM): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. Improvements (RS.IM): Organizational response activities are improved by incorporating lessons learned from current and previous detection/response activities. Supply Chain Risk Management (ID.SC): The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization has established and implemented the processes to identify, assess and manage supply chain risks. Improvements (RS.IM): Organizational 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 organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization'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, analyze and respond to vulnerabilities disclosed to the organization 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 organizational 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[864]. **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[865]. For instance, Mozi botnet continues to rely on the same set of older vulnerabilities, even those that are eight years old[866].**	
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	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

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

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 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	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 DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events DE.CM-7: Monitoring for unauthorized 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)[867]. For instance, the higher the bandwidth of a system or service, the more difficult or expensive a successful attack will be for a cybercriminal[868].	
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 organizational 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[869] [870].	
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 organizational stakeholders

[867] Neustar, Pay Or Else: DDoS Ransom Attacks
[868] https://hacked.com/will-2022-be-the-year-of-the-ddos-attack/
[869] David Warburton, F5Labs, DDoS Attack Trends for 2020, May 2021, https://www.f5.com/labs/articles/threat-intelligence/ddos-attack-trends-for-2020
[870] 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

	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
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[871]. The remediations for these threats depend on correct and complete training and education in cybersecurity[872].	
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 organization'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.

DISINFORMATION – MISINFORMATION

Regulations and laws need to be adapted to govern disinformation and deepfakes873. Attackers must be made accountable for their activities (e.g., deepfake revenge pornography, fraud) and for the consequences on the target of disinformation. This aspect is particularly critical because regulations and laws must preserve freedom of expression and speech as well.	
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 A.16.1.2 Reporting Information Security Events	**NIST Cybersecurity Framework (CSF)** RS.CO-2: Incidents are reported consistent with established criteria RS.CO-3: Information is shared consistent with response plans RS.CO-4: Coordination with stakeholders occurs consistent with response plans RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness DE.DP-4: Event detection information is communicated

[871] D4.2 concordia
[872] 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
[873] Microsoft FY21 Digital Defense Report

Training and awareness is key to understand disinformation and its working, and prepare proper countermeasures avoiding information fraudsters874. Training employees in managing disinformation attacks, and also in assessing any e-mail and report becomes increasingly important875 876.

High-quality information: Supporting high-quality media information and journalism is key to debunk fake news and disinformation. A chain of trust should be grounded on trusted news organizations, reporting the reputation of the source at the center of the discussion.877

Modern Media Literacy: Modern media literacy is key to promote a culture of trustworthy and reliable information. People must be trained on how to understand, expect, and recognize disinformation and misinformation to reduce unintentional spreading of misinformation.878 Work on media literacy should provide tools to support people in debunking fake news through source identification and news and information checking.879 Media literacy improves individuals resilience to disinformation, supporting the evaluation of accessed information and verification of the content source.

Fact Check and Debunking False Stories: Many efforts by both non-profit organisations and government agencies have been undertaken to reduce the impact of disinformation and misinformation.880 881 These actors aim to debunk publications and content carrying false information and fake news.882

AI pattern recognition: Pattern recognition based on AI can support the detection of manipulated communications and content, to identify malicious multimedia content.883

ISO/IEC 27001:2013	**NIST Cybersecurity Framework (CSF)**
4.1 Understanding the organization and its context	ID.AM-6: Cybersecurity roles and responsibilities for the entire workforce and third-party stakeholders (e.g., suppliers, customers, partners) are established
4.2 Understanding the needs and expectations of interested parties	ID.GV-2: Cybersecurity roles and responsibilities are coordinated and aligned with internal roles and external partners
5.3 Organizational roles, responsibilities, and authorities	ID.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed
6.2 Information security objectives and planning to achieve them	RS.CO-1: Personnel know their roles and order of operations when a response is needed
7 Support	PR.IP-7: Protection processes are improved
9.1 Monitoring, measurement, analysis and evaluation	PR.IP-11: Cybersecurity is included in human resources practices (e.g., deprovisioning, personnel screening)
A.6.1.1 Information security roles and responsibilities	PR.AT: The organization'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.6.1.2 Segregation of duties	PR.DS-6: Integrity checking mechanisms are used to verify software, firmware, and information integrity
A.7 Human resource security	PR.DS-8: Integrity checking mechanisms are used to verify hardware integrity
A.9.3 User responsibilities	DE.AE-1: A baseline of network operations and expected data flows for users and systems is established and managed
A.12.2 Protection from malware	DE.AE-5: Incident alert thresholds are established
A.12.4 Logging and monitoring	DE.CM: The information system and assets are monitored to identify cybersecurity events and verify the effectiveness of protective measures
A.12.6.1 Management of technical vulnerabilities	
A.15.2.1 Monitoring and review of supplier services	

874 D4.3 CONCORDIA
875 Paul McEvatt, Fujitsu, 2021 Prediction: The Age of Disinformation Attacks, January 2021, https://blog.global.fujitsu.com/fgb/2021-01-12/2021-prediction-the-age-of-disinformation-attacks/
876 Fujitsu, Top 10 Cyber Security Predictions for 2021, 2021, https://www.fujitsu.com/global/services/security/insights/predictions-2021/
877 D4.3 CONCORDIA
878 Microsoft FY21 Digital Defense Report
879 Microsoft FY21 Digital Defense Report
880 Trend Micro, Fake News and Cyber Propaganda: The Use and Abuse of Social Media, June 2017, https://www.trendmicro.com/vinfo/it/security/news/cybercrime-and-digital-threats/fake-news-cyber-propaganda-the-abuse-of-social-media
881 Tanveer Khan, Antonis Michalas, Adnan Akhunzada, Fake news outbreak 2021: Can we stop the viral spread?, Journal of Network and Computer Applications, Volume 190, 2021
882 Lion Gu, Vladimir Kropotov, and Fyodor Yarochkin, Trend Micro, The Fake News Machine: How Propagandists Abuse the Internet and Manipulate the Public, 2017, https://documents.trendmicro.com/assets/white_papers/wp-fake-news-machine-how-propagandists-abuse-the-internet.pdf
883 Microsoft FY21 Digital Defense Report
Please use footnotes for providing additional or explanatory information and/or relevant links. References should be listed in a dedicated section. Use only the function References/Insert Footnote

	DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability DE.DP-2: Detection activities comply with all applicable requirements DE.DP-3: Detection processes are tested PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy
It is important for enterprises to establish more resilient practices to clearly identify critical information gathering and distribution processes that should be strengthened to limit disinformation spread. According to identified processes, controls and validations must be employed to mitigate the impact of polluted data and mischaracterized information.884 885	
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)** PR.MA: Maintenance and repairs of industrial control and information system components are performed consistent with policies and procedures 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 PR.IP-4: Backups of information are conducted, maintained, and tested PR.IP-7: Protection processes are improved 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
External sources of intelligence can be manipulated before ingestion in the target enterprise system. Source validation and intelligence checking is key to reduce the risk and impact of data manipulation on the system. 886 887 Deeply inquire and research, on different sources (especially institutional ones) are fundamental to avoid scams.888	
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 10.1 Nonconformity and corrective action A.8.1.1 Inventory of assets 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	**NIST Cybersecurity Framework (CSF)** PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access 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 PR.IP-4: Backups of information are conducted, maintained, and tested PR.IP-7: Protection processes are improved PR.IP-12: A vulnerability management plan is developed and implemented

884 Microsoft FY21 Digital Defense Report
885 https://www.ofcom.org.uk/news-centre/2022/one-in-three-internet-users-fail-to-question-misinformation
886 Microsoft FY21 Digital Defense Report
887 https://www.ofcom.org.uk/news-centre/2022/one-in-three-internet-users-fail-to-question-misinformation
888 CONCORDIA D4.3

A.15.2.2 Managing changes to supplier services A.18.2.1 Independent review of information security	PR.DS-3: Assets are formally managed throughout removal, transfers, and disposition PR.DS-4: Adequate capacity to ensure availability is maintained ID.GV-4: Governance and risk management processes address cybersecurity risks ID.RA-1: Asset vulnerabilities are identified and documented ID.RA-3: Threats, both internal and external, 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.RA-6: Risk responses are identified and prioritized ID.RM: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions. RS.IM-1: Response plans incorporate lessons learned RS.IM-2: Response strategies are updated ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process 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 RC.IM-1: Recovery plans incorporate lessons learned RC.IM-2: Recovery strategies are updated ID.AM-1: Physical devices and systems within the organization are inventoried ID.AM-2: Software platforms and applications within the organization are inventoried ID.AM-4: External information systems are catalogued ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value 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, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers)
Network monitoring: Being able to identify the source location and organization of disinformation is critically important for implementing filtering functionalities.889	
ISO/IEC 27001:2013	**NIST Cybersecurity Framework (CSF)**
8.1 Operational planning and control 9.1 Monitoring, measurement, analysis and evaluation A.12.4 Logging and monitoring A.13.1 Network security management A.13.2.1 Information transfer policies and procedures A.13.2.2 Agreements on information transfer 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	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 organizational stakeholders PR.MA-1: Maintenance and repair of organizational assets are performed and logged, with approved and controlled tools PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized access DE.CM-1: The network is monitored to detect potential cybersecurity events

[889] Microsoft FY21 Digital Defense Report

	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 DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed DE.AE-3: Event data are collected and correlated from multiple sources and sensors RS.MI-3: Newly identified vulnerabilities are mitigated or documented as accepted risks PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy 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
Content verification and certification: Traditional cryptographic and security solutions can be employed to guarantee authenticity and provenance of collected information. Cross-organization collaborations can help in strengthening content certification.890 Content verification and certification is at the basis of deepfakes detection.	
ISO/IEC 27001:2013 6 Planning 6.2 Information security objectives and planning to achieve them 7.1 Resources 7.2 Competence 8 Operation 9 Performance evaluation 9.2 Internal audit 9.3 Management review 10 Improvement A.5.1.2 Review of the policies for information security A.12.1.3.Capacity Management A.12.7.1 Information systems audit controls A.18.2 Information security reviews	**NIST Cybersecurity Framework (CSF)** ID.AM-5: Resources (e.g., hardware, devices, data, time, personnel, and software) are prioritized based on their classification, criticality, and business value PR.IP-7: Protection processes are improved PR.IP-8: Effectiveness of protection technologies is shared PR.IP-12: A vulnerability management plan is developed and implemented 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.GV-3: Legal and regulatory requirements regarding cybersecurity, including privacy and civil liberties obligations, are understood and managed ID.GV-4: Governance and risk management processes address cybersecurity risks ID.RA-1: Asset vulnerabilities are identified and documented ID.RA-3: Threats, both internal and external, 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.RA-6: Risk responses are identified and prioritized ID.RM: The organization's priorities, constraints, risk tolerances, and assumptions are established and used to support operational risk decisions DE.CM-8: Vulnerability scans are performed DE.DP-5: Detection processes are continuously improved 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 authorized devices, users and processes

[890] Microsoft FY21 Digital Defense Report

	PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy RS.IM-1: Response plans incorporate lessons learned RS.IM-2: Response strategies are updated RC.IM-1: Recovery plans incorporate lessons learned RC.IM-2: Recovery strategies are updated
Social network detection and mitigation are still among the most important technical approaches for disinformation management. Countermeasures 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 users891.	
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 A.16.1.1 Responsibilities and procedures A.16.1.4Assessment of and decision 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)** 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 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 DE.CM-1: The network is monitored to detect potential cybersecurity events 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-4: Malicious code is detected DE.CM-5: Unauthorized mobile code is detected DE.CM-6: External service provider activity is monitored to detect potential cybersecurity events DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed DE.DP-1: Roles and responsibilities for detection are well defined to ensure accountability DE.DP-2: Detection activities comply with all applicable requirements DE.DP-3: Detection processes are tested PR.PT-1: Audit/log records are determined, documented, implemented, and reviewed in accordance with policy ID.RA-3: Threats, both internal and external, 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.RA-6: Risk responses are identified and prioritized 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.AN: Analysis is conducted to ensure effective response and support recovery activities RS.IM-1: Response plans incorporate lessons learned RS.IM-2: Incidents are mitigated

[891] https://www.apa.org/monitor/2022/06/news-misinformation-attack

	RS.CO-1: Personnel know their roles and order of operations when a response is needed RS.CO-3: Information is shared consistent with response plans RS.CO-4: Coordination with stakeholders occurs consistent with response plans RS.CO-5: Voluntary information sharing occurs with external stakeholders to achieve broader cybersecurity situational awareness 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 RC.CO-2: Reputation is repaired after an incident

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	**NIST Cybersecurity Framework (CSF)** Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized activities and transactions.

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	PR.MA-2: Remote maintenance of organizational assets is approved, logged, and performed in a manner that prevents unauthorized 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 organization's personnel and partners are provided cybersecurity awareness education and are trained to perform their cybersecurityrelated 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 communicate
Monitor and centralize 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 organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization'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.

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 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	ID.RM-1: Risk management processes are established, managed, and agreed to by organizational 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 organization's priorities, constraints, risk tolerances, and assumptions are established and used to support risk decisions associated with managing supply chain risk. The organization 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).

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[892]) and coordinate security communications with customers via this PSIRT.

ISO/IEC 27001:2013	NIST Cybersecurity Framework (CSF)
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	Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational 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): Organizational 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	NIST Cybersecurity Framework (CSF)
A.9.1 Business requirements of access control A.9.3 User responsibilities	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices,

[892] FIRST PSIRT Services Framework https://www.first.org/standards/frameworks/psirts/psirt_services_framework_v1.1

A.9.4.1 Information access restriction A.9.4.2 Secure log-on procedures A.9.4.3 Password management system	and is managed consistent with the assessed risk of unauthorized access to authorized 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 organizational 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 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, analyze and respond to vulnerabilities disclosed to the organization 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 organization are inventoried ID.AM-4: External information systems are catalogued PR.IP-5: Policy and regulations regarding the physical operating environment for organizational 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 FIRST893 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 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	**NIST Cybersecurity Framework (CSF)** ID.GV-4: Governance and risk management processes address cybersecurity risks Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. Risk Management Strategy (ID.RM): The organization'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 organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy. ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; 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, analyze and respond to vulnerabilities disclosed to the organization from internal and external sources (e.g. internal testing, security bulletins, or security researchers) Improvements (RS.IM): Organizational 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.**	

[893] FIRST SIG: https://www.first.org/global/sigs/vulnerability-coordination/multiparty/guidelines-v1.1

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 A.18.1.2 Intellectual property rights A.18.2.2 Compliance with security policies and standards	**NIST Cybersecurity Framework (CSF)** Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. Business Environment (ID.BE): The organization's mission, objectives, stakeholders, and activities are understood and prioritized; 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 organization'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. 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 prioritized 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 authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized 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	NIST Cybersecurity Framework (CSF)
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	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[894].	
ISO/IEC 27001:2013	**NIST Cybersecurity Framework (CSF)**
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	Identity Management, Authentication and Access Control (PR.AC): Access to physical and logical assets and associated facilities is limited to authorized users, processes, and devices, and is managed consistent with the assessed risk of unauthorized access to authorized 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.**	
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 organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk. Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals. Risk Management Strategy (ID.RM): The organization'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 authorized 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): Organizational 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)

[894] https://github.blog/2022-03-28-how-to-secure-your-end-to-end-supply-chain-on-github/

	PR.AC-6: Identities are proofed and bound to credentials and asserted in interactions
Use container image signing.	
ISO/IEC 27001:2013 A.10.1 Cryptographic controls A.18.1.5 Regulation of cryptographic controls	**NIST Cybersecurity Framework (CSF)** 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 organization'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
Agamemnonos 14, Chalandri 15231, Attiki, Greece

Heraklion Office
95 Nikolaou Plastira
700 13 Vassilika Vouton, Heraklion, Greece

enisa.europa.eu

ISBN 978-92-9204-588-3
DOI: 10.2824/764318