EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA THREAT LANDSCAPE: FINANCE SECTOR

JANUARY 2023 TO JUNE 2024

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.

AUTHORS

Marianthi Theocharidou, Ifigeneia Lella, Rossen Naydenov, Apostolos Malatras, ENISA

ACKNOWLEDGEMENTS

Tomislav Vazdar and Adrian Ifrim

The report has been validated and supported by the members of the ENISA advisory group, the National Liaison Officers Network, the ENISA Ad Hoc Working Group on Cybersecurity Threat Landscapes (CTL), and the European Financial Institutes – Information Sharing and Analysis Centre.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-677-4, DOI 10.2824/5410466

TABLE OF CONTENTS

EXECUTIVE SUMMARY

This is the first analysis conducted by the European Union Agency for Cybersecurity (ENISA) of the cyber threat landscape of the European finance sector. From January 2023 to June 2024, the European financial sector faced significant cybersecurity challenges, highlighting threats and vulnerabilities across the sector.

- ENISA analysed 488 publicly reported incidents affecting the finance sector in Europe.
- European banks (credit institutions) were the most frequently affected at a 46% rate, with 301 incidents observed. Public organisations related to finance (13%) followed next. Individuals, such as customers of credit institutions, were also affected (10%), being defrauded through social engineering campaigns with a finance-relevant theme.
- The finance sector saw peaks in distributed denial-of-service activity linked to geopolitical events, particularly Russia's invasion of Ukraine. Hacktivists targeted European credit institutions (58% of incidents) and governmental websites related to finance (21%), notably causing operational disruptions.
- Data breaches and leaks remain prominent issues. Threat actors exploited vulnerabilities for financial gain through fraud, supply chain attacks, and social engineering. European credit institutions were the primary targets (39%), with incidents leading to financial losses, regulatory penalties, and reputational damage.
- Social engineering campaigns, including phishing, smishing and vishing, were prevalent tactics used by cybercrime threat actors. These incidents aimed to steal sensitive information and commit financial fraud, affecting individuals (38%) and credit institutions (36%). The result was financial loss, large-scale financial crimes, and data exposure.
- Fraud accounted for 6% of overall incidents, primarily affecting individuals (40%) and credit institutions (35%). Although reported cases seem low, underreporting and secondary consequences from other cyber incidents suggest a broader issue. Crypto-related cybercrime increased. Related activities include theft, scams, and illicit laundering.
- Ransomware attacks primarily affected service providers (29%) and insurance organisations (17%), with impacts including financial loss (38%), data exposure (35%), and operational disruption (20%).
- Malware incidents (excluding ransomware cases), though fewer in number (21 cases), often affected a large number of citizens. Banking trojans and spyware posed significant threats by enabling device takeovers and fraudulent activities. Credit institutions (36%) and individuals (24%) were affected most.
- Attacks on suppliers, mostly data breaches and ransomware, resulted in the exposure and sale of sensitive data (63%), operational disruption (26%), and financial loss (11%).

Stakeholders in the finance sector must should invest strategically to improve cybersecurity resilience. This involves investing in supply chain management and incident response. Strengthening regulatory compliance with frameworks, like the general data protection regulation, the network and information security directive, and the Digital Operational Resilience Act, is essential, alongside implementing comprehensive employee training programmes and robust incident response plans. Rigorous third-party risk management practices are crucial, as is fostering collaboration and information sharing within the sector. A multifaceted approach is necessary to stay ahead of evolving cyber threats and maintain long-term resilience.

1. INTRODUCTION

This is the first European Union Agency for Cybersecurity (ENISA) threat landscape report which brings insights into cyber threats targeting the European finance sector. The sector was selected due to its criticality and its importance to European citizens. Central banks and financial regulators consider cybersecurity as one of the risks they face. The International Monetary Fund recognises that the financial sector is highly exposed to cyber risks and considers cyber incidents as a rising financial stability concern ([1]). The European Central Bank highlights the need to increase cyber resilience as a priority to be addressed by the ECB Banking Supervision in the period 2024-26 ([2]).

In the *ENISA Threat Landscape 2024* ([3]) report, 9% of the observed incidents targeted finance organisations, with the finance sector being the third-most targeted after public administrations and transport organisations. Moreover, 12 % of the incidents with a significant impact reported under the network and information security (NIS) directive ([4]) in 2023 were incidents in the European finance sector ([5]). Additionally, for 12 consecutive years, the finance industry had the highest average cost of a breach worldwide ([6]).

Reporting period. In this report, we analysed cyber incidents targeting the European finance sector from January 2023 to June 2024. This period is referred to as the 'reporting period' throughout the report.

Scope. Data collection and analysis focused on cyber incidents observed in EU member states and neighbouring countries (Albania, Iceland, Liechtenstein, Moldova, Norway, Switzerland, United Kingdom and Ukraine). These additional countries were included as EU finance institutions operate or offer services to neighbouring countries.

We collected publicly reported cyber incidents affecting various types of organisations related to finance. The collection and analysis focused mostly on organisations in the scope of the NIS directive and of the Digital Operational Resilience Act (DORA) ([7]). We collected incidents related to the following types of organisations:

- credit institutions (banks),
- payment institutions,
- electronic money institutions,
- investment firms,
- crypto-asset service providers,
- central securities depositories,
- central counterparties,
- trading venues,
- insurance organisations (i.e. insurance and reinsurance undertakings, insurance intermediaries, reinsurance intermediaries, ancillary insurance intermediaries),
- credit rating agencies,
- digital service providers (providing services to the financial sector)
- digital infrastructures (providing infrastructures to the financial sector)
- organisations of central or local public administrations, that offer financial services, and

([1]) International Monetary Fund, *Global Financial Stability Report – The last mile: Financial vulnerabilities and risks*, Washington DC, 2024, https://imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024?cid=bl-com-SM2024-GFSREA2024001.
([2]) European Central Bank, Banking Supervision, 'IT and cybersecurity risks – key observations in 2024', ECB Banking supervision website, 2024. https://www.bankingsupervision.europa.eu/ecb/pub/pdf/annex/ssm.nl241113_4_annex.en.pdf.
([3]) ENISA, *ENISA Threat Landscape 2024 – July 2023 to June 2024*, 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
([4]) Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, http://data.europa.eu/eli/dir/2022/2555/oj.
([5]) Data retrieved by the cybersecurity incident reporting and analysis system: https://ciras.enisa.europa.eu/.
([6]) IBM, *Cost of a Data Breach Report 2024*, 2024, https://www.ibm.com/reports/data-breach.
([7]) Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector, http://data.europa.eu/eli/reg/2022/2554/oj.

- organisations offering other financial services such as tax, accounting or consulting services (labelled 'other financial service providers' to distinguish them from digital service providers).

For a limited number of incidents, the type of organisation could not be specified further. These are labelled as 'financial institutions'. We also added a category named 'individuals' as they were often being directly targeted in campaigns with a theme related to the finance sector or were the victims of financial fraud. These were primarily customers of credit institutions (banks).

Methodology. To conduct this study, the *ENISA Cybersecurity Threat Landscape Methodology* ([8]) was applied. This is by no means the complete list of incidents that occurred during the reporting period. ENISA gathered a list of incidents based on open-source intelligence (OSINT) ([9]) and ENISA's own situational awareness capabilities. These incidents serve as the foundation for identifying a list of prime threats and are the source material for statistics in the report. The incidents were analysed by ENISA's threat landscape team and external experts in detail to provide insights to some important inquiries such as how the attacks happened, which systems were targeted, and which finance organisations were most affected and how. Moreover, desk research of available literature from open sources, such as news media articles, expert opinions, intelligence reports, incident analyses and security research reports, was conducted. Within the report, we differentiate between what has been reported by our sources and what is our assessment. When conducting an assessment, we convey likelihood by using estimative language ([10]).

Under the NIS directive, EU credit institutions, operators of trading venues, and central counterparties must notify the national authorities in their Member States of cybersecurity incidents with a significant impact. At the end of each year, the summary reports about these incidents are collected, anonymised, aggregated, and analysed by ENISA. Due to their anonymised character, these reports cannot be combined with the incidents collected by OSINT, as there is a risk that incidents could be duplicated. However, they offer a complementary picture and are presented as additional information throughout the report.

Structure. The report is structured as follows.

- Chapter 1 – **Introduction** – provides an overview of the scope and the methodology used to produce this report.
- Chapter 2 – **Incidents** – analyses the activity observed during the reporting period. It provides insights on the geographical spread of the incidents observed.
- Chapter 3 – **Prime threats** – provides insights on the prime threats and discusses the types of incidents of each threat category.
- Chapter 4 – **Threat actors** – analyses the types of actors that target the finance sector, identifies the top actors, and discusses their potential goals.
- Chapter 5 – **Impact** – analyses how the activity observed affected the sector and discusses which entities were the most targeted, the assets that were affected and the consequences of the incidents.
- Chapter 6 – **Conclusions** – discusses the trends derived from the analysis and some further considerations.

([8]) ENISA, *ENISA Cybersecurity Threat Landscape Methodology – July 2022*, 2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology.
([9]) This is a result of the work done by ENISA in the area of situational awareness in accordance with the EU Cybersecurity Act, Article 7(6): https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN.
([10]) Malware Information Sharing Platform, estimative language: https://www.misp-project.org/taxonomies.html#_estimative_language.

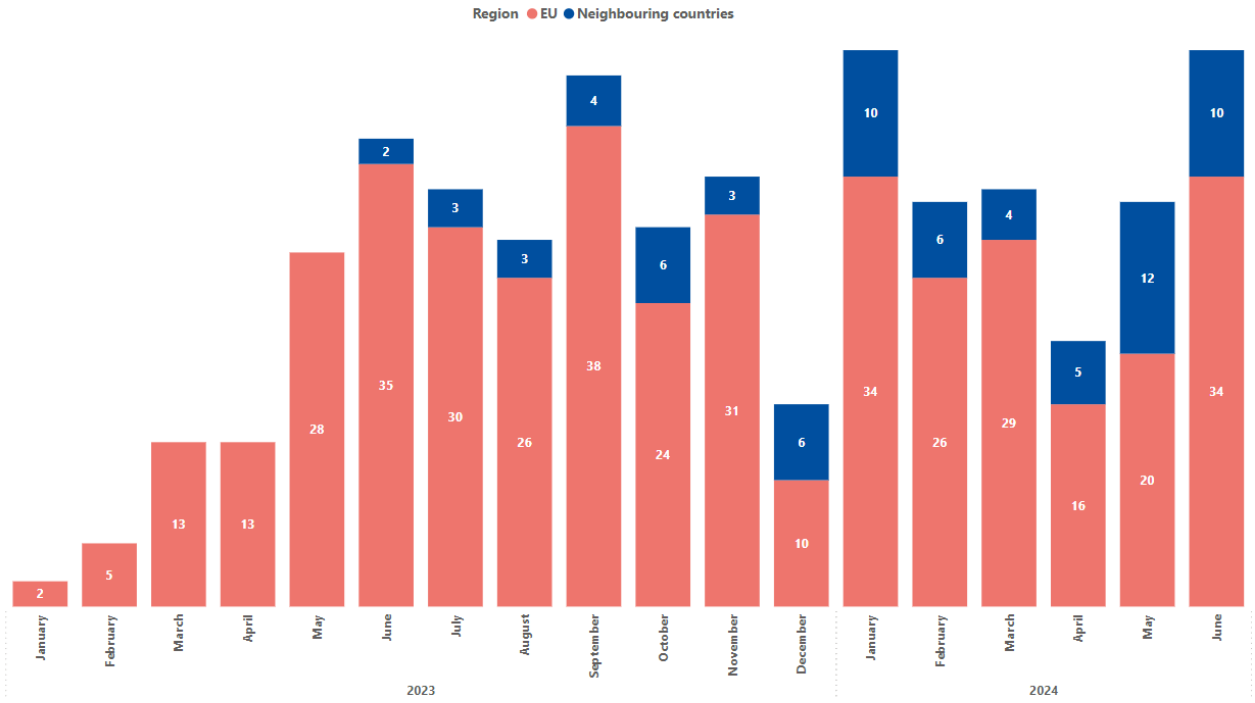
2. INCIDENTS

From January 2023 until June 2024, we analysed a total of 488 publicly reported incidents in the EU and neighbouring countries. There were 414 incidents that affected at least one EU Member State and 74 that affected a neighbouring country. To mark an incident as related to the EU's finance sector, we considered the following criteria.

- The activity is targeting the financial entities (and their customers) being located in the European Union and neighbouring countries (Albania, Iceland, Liechtenstein, Moldova, Norway, Switzerland, United Kingdom and Ukraine).
- The targeted software products or service providers are specifically used by European financial entities, or the incident suggests that European financial institutions were the intended target.
- Large-scale campaigns suggests that financial entities in Europe were the intended target.
- The activity is associated to a well-resourced threat actor known to target financial entities in Europe.

The incidents included 432 cyber attacks on the finance sector, along with 30 campaigns and 26 warnings of potential activity or new vulnerabilities affecting the finance sector.

Figure 1: Incidents observed per month (January 2023 to June 2024)



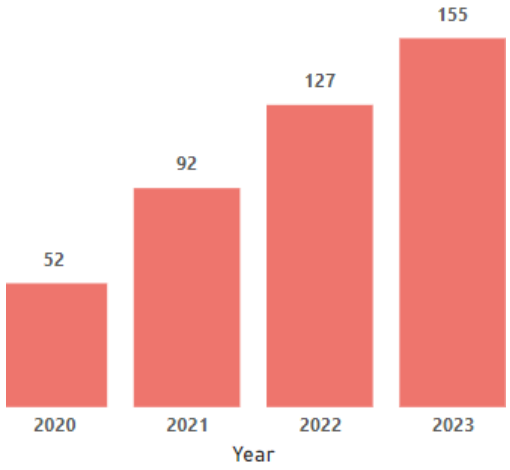
Overall, we observed a stable number of incidents, with an increase in the number of incidents after the third quarter of 2023. The observed monthly incidents fluctuated and were affected by distributed denial-of-service (DDoS) attacks targeting specific Member States at particular periods. These are linked to activity related to Russia's invasion of Ukraine or to events or statements related to support for Ukraine.

However, the number of incidents observed may have been affected by several other factors. An increase in the number of reported cyberattacks does not necessarily mean that the number of attacks actually increased. Such an increase can occur as a sector matures in terms of incident detection and reporting, which may be due to the effect of the legal obligation to report incidents under EU or national law. Alternatively, the attention of the media or the public could have

been focused on a particular sector for a particular period, resulting in more incidents being reported in OSINT. Moreover, ENISA increased its situational awareness capabilities since 2023, providing better visibility.

We also saw an increase since 2020 in the officially reported incidents under the NIS directive ([11]). These were incidents of significant impact officially reported to national authorities by credit institutions, operators of trading venues and central counterparties. We observe an increase in reported incidents, which may be due to the increased use of reporting mechanisms. We expect further reporting to be done under DORA as it covers more types of organisations compared to the NIS directive.

Figure 2: Incidents of significant impact, officially reported under the NIS directive (from 2020 to 2023)

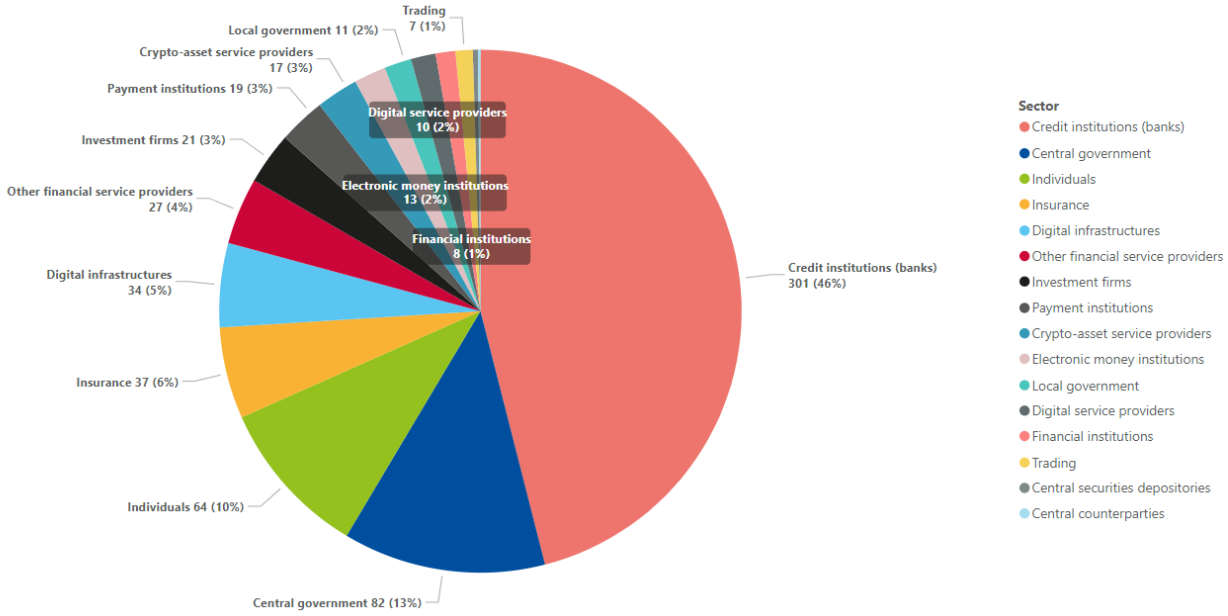


The finance sector is diverse, encompassing a range of institutions and services. Figure 3 shows a breakdown of the types of financial entities that were targeted during the reporting period ([12]).

([11]) In the EU, critical service providers have to notify the national authorities in their Member States of cybersecurity incidents with a significant impact. At the end of each year, the summary reports about these incidents are collected, anonymised, aggregated and analysed by ENISA. The cybersecurity incident reporting and analysis system shows the overall EU statistics: https://ciras.enisa.europa.eu/.

([12]) The types of entities were selected mostly based on Directive (EU) 2022/2555 and Regulation (EU) 2022/2554.

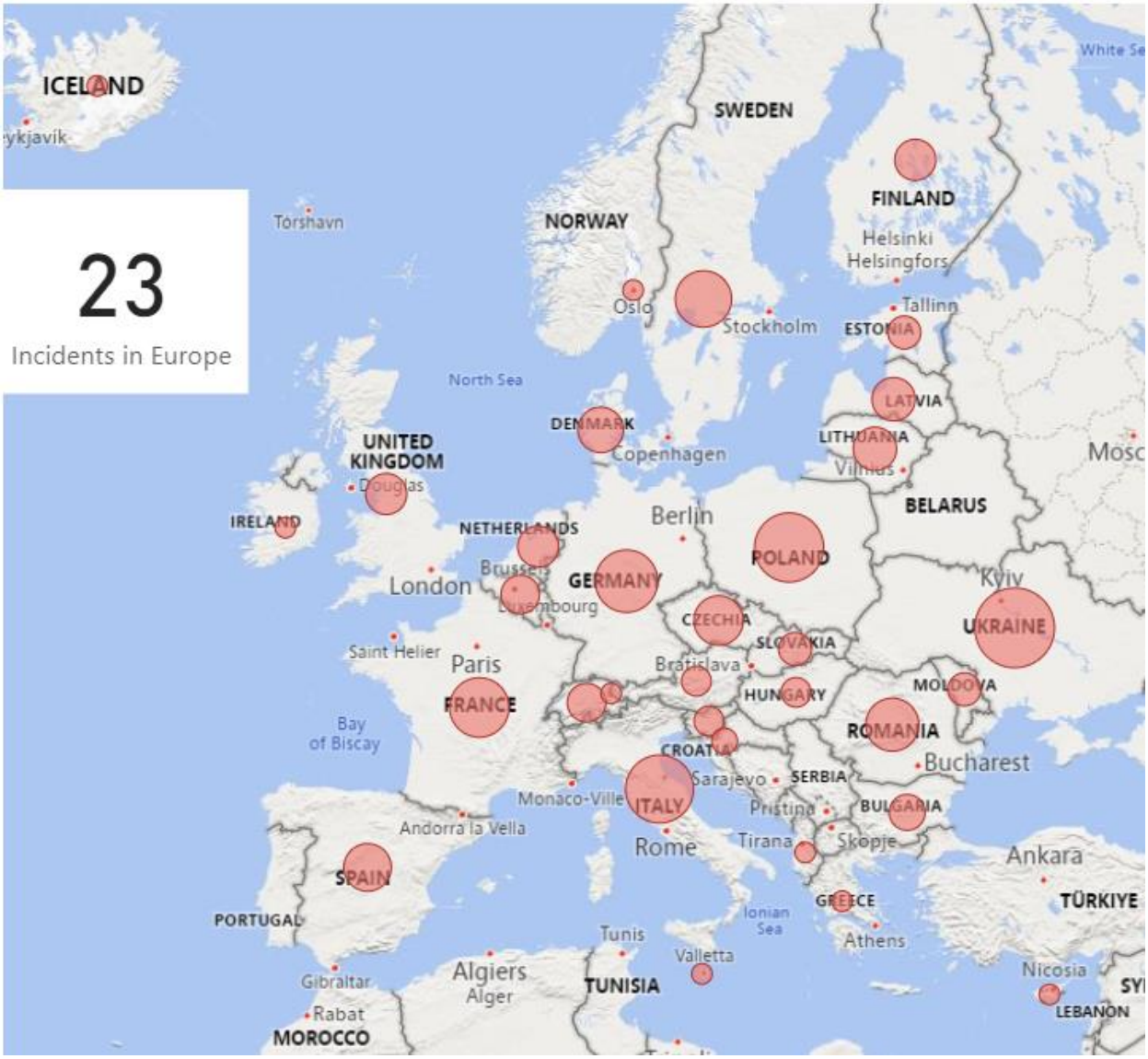
Figure 3: Affected entities (number of incidents per entity type, January 2023 to June 2024)



It is worth noting that one incident may have affected multiple types of organisations. European credit institutions (banks) were the most frequently affected sector (46 %), with 301 incidents reported. Cybercriminals primarily target banks to steal money through fraudulent transactions, access personal customer information, and execute ransomware attacks demanding ransoms for data decryption. The second-most targeted entities were government agencies and public sector organisations related to finance (13 %), followed by individuals (10 %). If we compare this with incidents observed outside of Europe, we see similar trends, with more crypto-asset service providers and digital infrastructures being targeted. This is due to the fact that these types of providers are often located outside Europe, and the effect of their disruption has a global impact.

Figure 4 shows the total incidents observed that targeted European financial organisations during the reporting period. The differences in the number of incidents per country cannot be interpreted as they may be affected by several parameters. These may include the population size, differences in reporting capabilities in specific countries, the use of financial services in a country or limitations of the data collection process itself. Overall, we observe that there were cyber incidents that targeted the European finance sector indiscriminately. All Member States faced cyber incidents affecting the finance sector during the reporting period.

Figure 4: Map of incidents observed in the finance sector in Europe (January 2023 to June 2024)



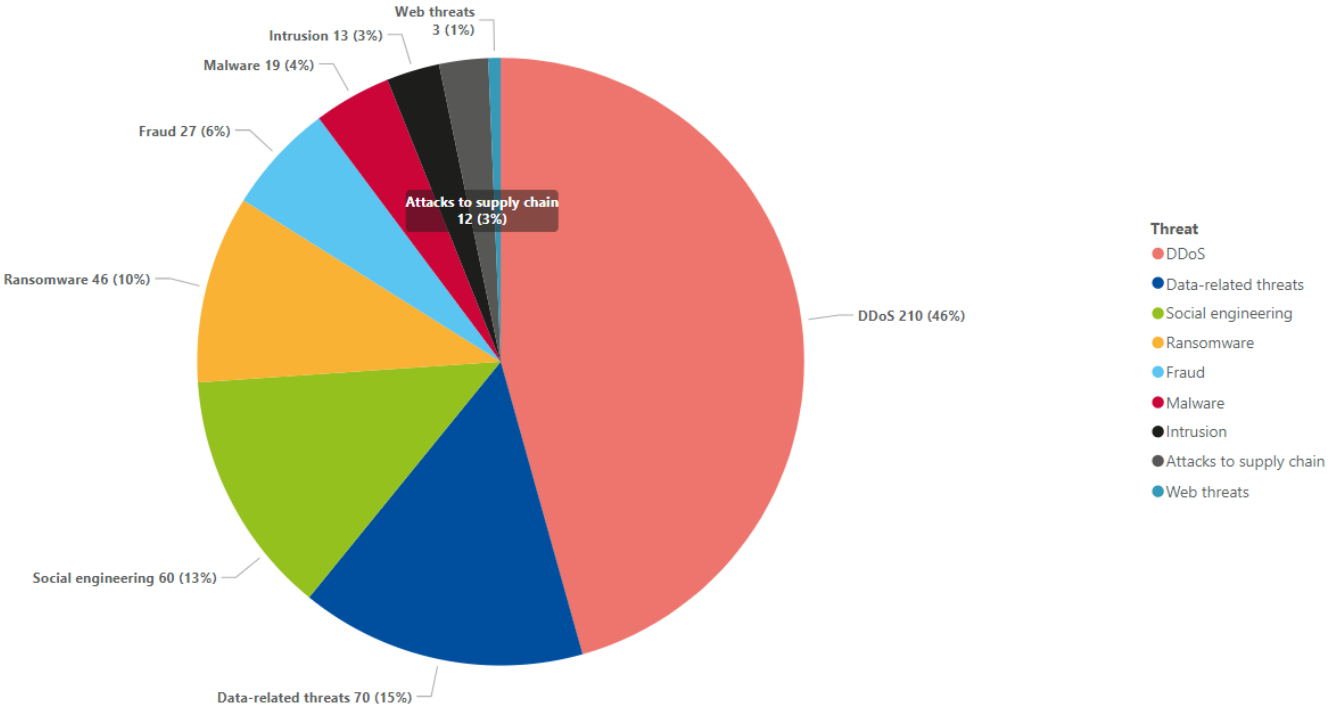
NB: the size of each circle refers to the sum of observed incidents in each country during the reporting period. The 23 incidents labelled as 'Europe' refer to entities that had activity in more than two Member States.

.

3. PRIME THREATS

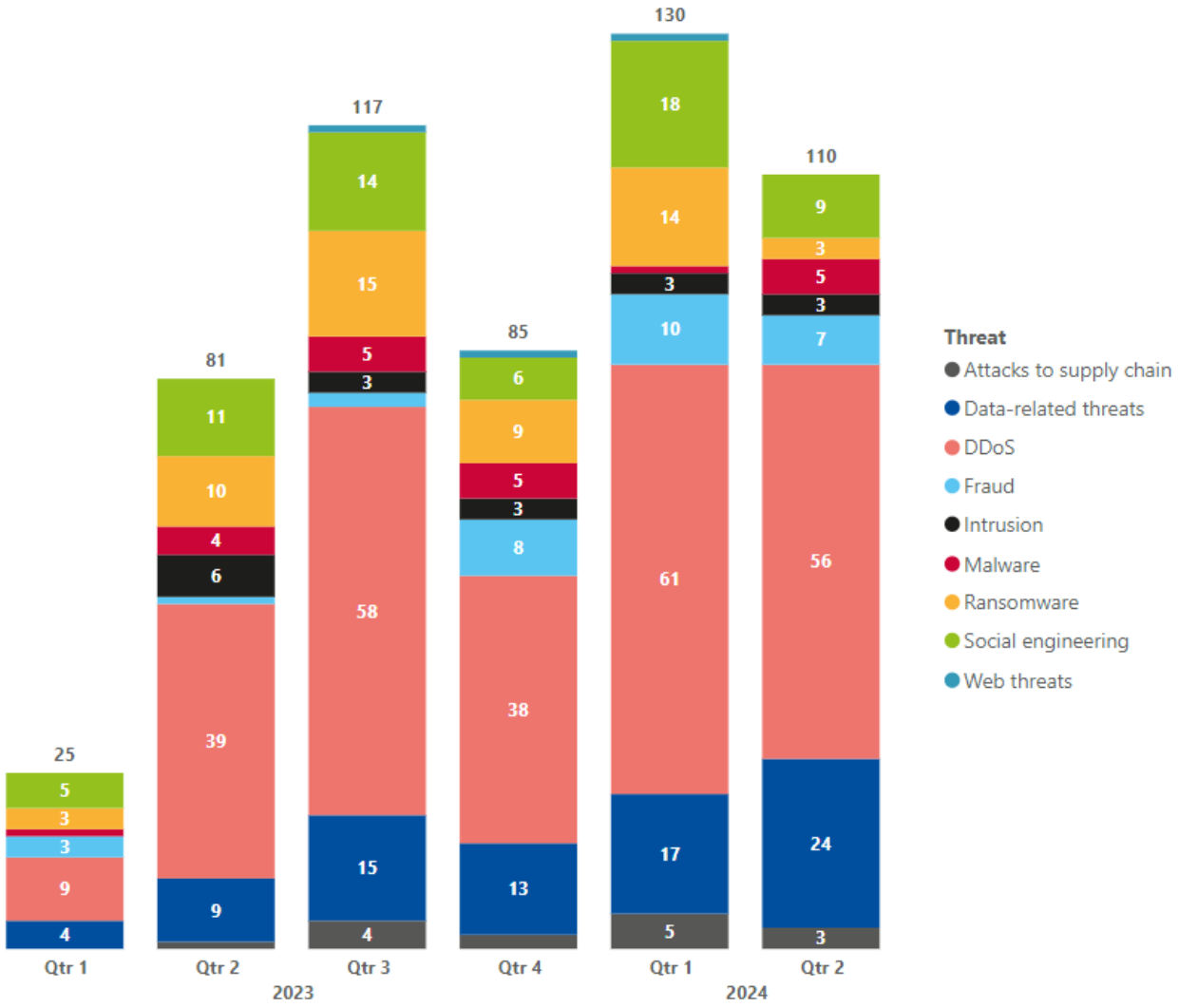
Throughout the reporting period, we observed the following types of threats (Figure 5) targeting the European finance sector. An incident can be categorised into more than one threat category, meaning that the total percentage of the threats shown in Figure 5 exceeds 100%. For example, the attack vector for initial access may include a finance-themed phishing campaign (social engineering), followed by a compromise with ransomware, which may or may not result in data being leaked (data-related threats). Likewise, incidents that included an attack on a supplier or service provider were categorised both as supply-chain attacks and as the type of attack used for the compromise.

Figure 5: Threats observed in the European finance sector (January 2023 to June 2024)



In Figure 6, the differences between the threats observed are depicted on a quarterly basis.

Figure 6: Threats to the European finance sector (in number of incidents per threat, January 2023 to June 2024)



In the following sections, we discuss each type of threat identified in greater detail.

3.1 DISTRIBUTED DENIAL-OF-SERVICE ATTACKS

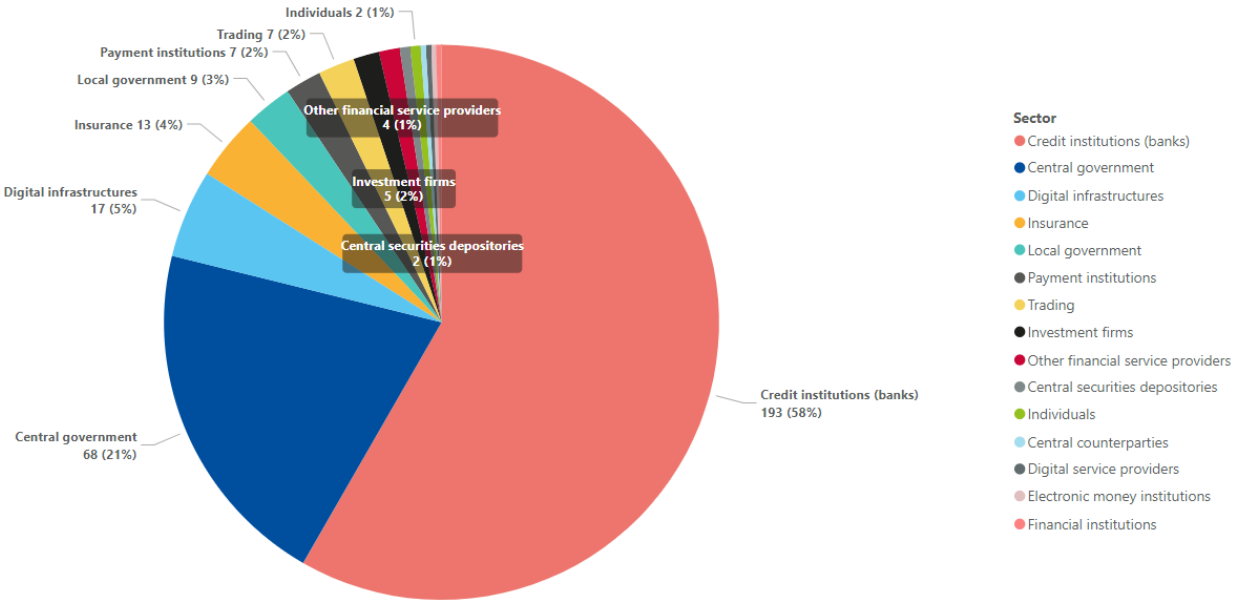
DDoS attacks can be accomplished by exhausting the service and its resources or overloading the components of the network infrastructure. Users of a system or service are then not able to access relevant data, services or other resources.

We observed DDoS attacks targeting finance organisations throughout the reporting period with peaks in specific quarters (the third quarter of 2023 and the first and second quarters of 2024) that were linked to geopolitical developments linked to the Middle east or to Russia's invasion of Ukraine. For example, statements in support of Ukraine by a Member State may have been followed by hacktivist activity targeting the Member state and its financial entities being targeted among other sectors.

The majority of the DDoS attacks we observed (58%) targeted European credit institutions (banks), followed by government websites and services at a 21% rate. The latter referred to attacks on the websites of national ministries related to finance, or the national tax, revenue or custom authorities.

It is worth mentioning that the incidents under analysis were as reported on Telegram channels, thus, it is difficult to confirm the impact of these incidents. After analysing these cases, we assessed that the impact of DDoS attacks was often limited. In 2023, 13 incidents (8%) were officially reported to national competent authorities as DDoS attacks of significant impact. These refer to EU credit institutions, operators of trading venues or central counterparties ([13]). Today, DDoS attacks can often be well mitigated by DDoS mitigation services, but their financial impact to the European financial sector is not negligible, as a lot of resources goes into DDoS mitigation.

Figure 7: DDoS attacks on European financial entities (January 2023 to June 2024)



3.2 DATA-RELATED THREATS

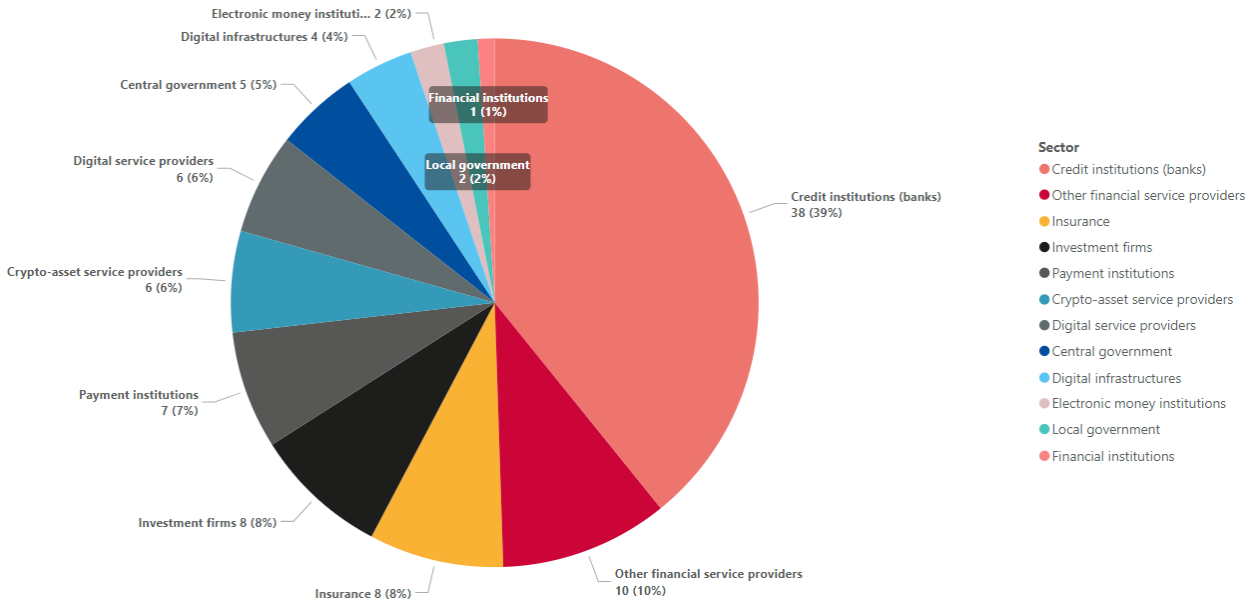
Threats against data can be broadly classified as a data breach or a data leak. A data breach is an intentional cyberattack with the goal of gaining unauthorised access to a system or organisation and stealing sensitive, confidential or protected data. A data leak is an event (such as misconfigurations, vulnerabilities or human errors) that can cause the unintentional loss or exposure of sensitive, confidential or protected data (intentional attacks are sometimes referred to as data exposure).

The finance sector has traditionally suffered from data-related incidents, due to the value of the data that the sector handles which include personal information and corporate information and their potential for financial gain. This is evidently an appealing target for threat actors who would take advantage of the opportunity to monetise their activities based on extortion under the threat of disclosure or to perform financial fraud. We observed that data-related threats often relate to supply chain attacks and social engineering (especially business email compromise).

We observe data breaches or leaks primarily occurring in credit institutions (39% of the data breaches), followed by other financial service providers (10%), insurance organisations (8%), investment firms (8%), payment institutions (7%) and crypto-asset service providers (6%). In most of these incidents, individuals were affected as their personal and financial data were exposed or sold, and in several cases the financial entities faced financial loss, fraud, regulatory and compliance penalties or reputational damage.

([13]) Data retrieved by the cybersecurity incident reporting and analysis system: https://ciras.enisa.europa.eu/.

Figure 8: Data-related threats to European financial entities (January 2023 to June 2024)



3.3 SOCIAL ENGINEERING

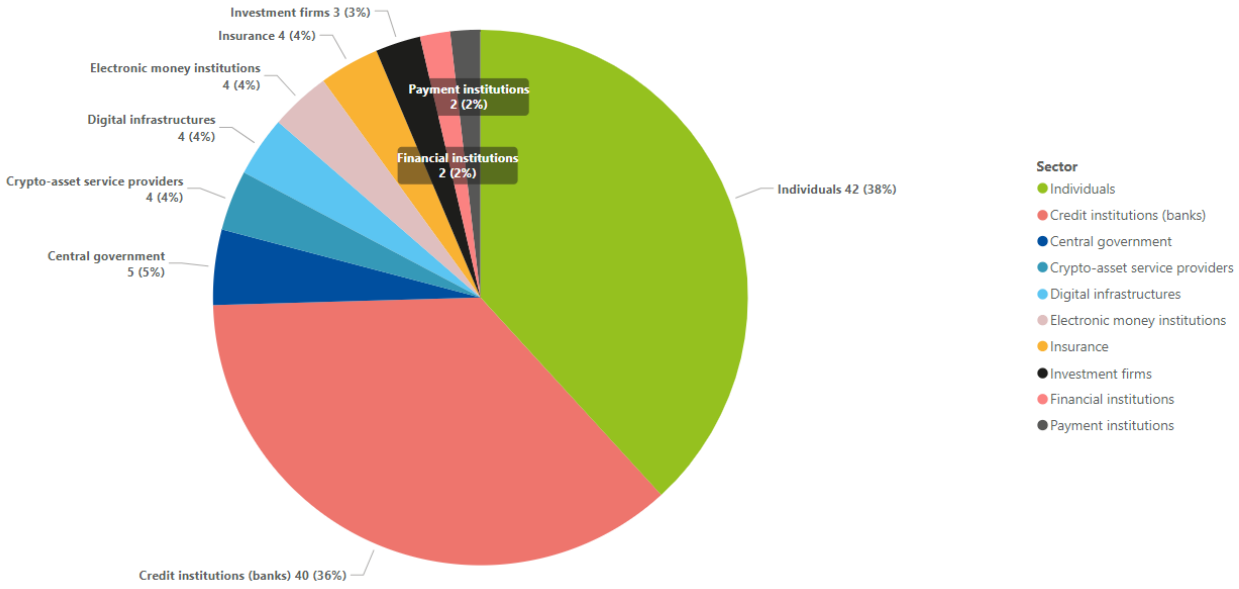
Social engineering encompasses a broad range of activities that attempt to exploit human error or human behaviour with the objective of gaining access to information or services. It uses various forms of manipulation to trick victims into making mistakes or handing over sensitive or secret information. Users may be lured into opening documents, files or e-mails, visiting websites, or granting access to systems or services. This threat canvas consists mainly of the following attack vectors: phishing, spear phishing, whaling, smishing, vishing, watering hole attack, baiting, pretexting, quid pro quo, honeytraps and scareware. While social engineering techniques are often used to gain initial access, they may also be used at later stages in an incident or breach. Notable examples are business e-mail compromise, impersonation, counterfeiting and extortion.

Phishing persisted as the most prevalent attack vector for fraud. We observed phishing campaigns that target individuals (38% of the social engineering incidents) by impersonating primarily credit institutions (36% of the social engineering incidents). In fact, this was the most common attack vector we found in attempts of phishing, smishing and vishing. According to the *Internet Organised Crime Threat Assessment (IOCTA) 2024* report, 'smishing (SMS/text phishing) was the most common type of phishing used by fraudsters in 2023, while quishing (QR code phishing) was considered an on the rise ([14]). A notable example was the Latvian State Police reporting fraud campaigns where attackers impersonated bank officials to steal information, leading to financial loss and compromised personal information ([15]). Another notable change is the increase in business-email compromise incidents during this reporting period ([16]) ([17]). For example, in June 2023, Microsoft uncovered a multi-stage adversary-in-the-middle (AiTM) phishing and business email compromise (BEC) attack against banking and financial services organizations. The attack originated from a compromised trusted vendor and transitioned into a series of AiTM attacks and follow-on BEC activity spanning multiple organizations ([18]).

The social engineering attacks we analysed aimed at stealing personal information or corporate data and resulted in, as a consequence, financial loss (50 %), fraud and large-scale financial crimes (28 %) or the exposure and sale of sensitive data (19 %).

([14]) European Union Agency for Law Enforcement Cooperation (Europol), *Internet Organised Crime Threat Assessment (IOCTA) 2024*, Publications Office of the European Union, Luxembourg, 2024, https://data.europa.eu/doi/10.2813/442713.
([15]) Republic of Latvia State Police, 'Fraudsters ask citizens to return their bank cards', Republic of Latvia State Police press release, 5 January 2024, https://www.vp.gov.lv/lv/jaunums/krapnieki-iedzivotajiem-prasa-atdot-savas-bankas-kartes.
([16]) ENISA, *ENISA Threat Landscape 2024 – July 2023 to June 2024*, 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
([17]) Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2024*, Publications Office of the European Union, Luxembourg, 2024, https://data.europa.eu/doi/10.2813/442713.
([18]) Microsoft Threat Intelligence, *Detecting and mitigating a multi-stage AiTM phishing and BEC campaign*, 8 June, 2023, https://www.microsoft.com/en-us/security/blog/2023/06/08/detecting-and-mitigating-a-multi-stage-aitm-phishing-and-bec-campaign/.

Figure 9: Social engineering attacks to European financial entities and their customers (January 2023 to June 2024)



3.4 FRAUD

Fraud amounted to only 6 % of the overall observed incidents, but it is crucial to understanding the broader context of financial crime as a consequence of cyber incidents. Our analysis showed that incidents resulting in fraud primarily affected individuals (40 %) and credit institutions (35 %). Personal information (77 %) and corporate data (21 %) were targeted as a means to perform fraud, resulting in financial loss (60 %), large-scale financial crimes (24 %) and the exposure and sale of sensitive data (13 %).

One possible reason for the relatively small percentage of fraud in the reported incidents could be under-reporting. Financial institutions might not disclose all fraud incidents due to reputational risks or regulatory pressures. Additionally, fraud is often a secondary consequence of other types of cyber incidents, such as phishing or data breaches, which might be reported under their primary attack vectors rather than as fraud. In our analysis, we observed several fraud cases, such as (a) cases of bank help desk fraud, (b) cases of criminals impersonating bank employees, (c) incidents of investment fraud, especially crypto investment fraud and (d) large-scale theft of credit card data or of customers' personal data, after successful phishing and smishing attacks. Therefore, while fraud appears to be a minor part of the overall threat landscape, it is likely that financial crime resulting from cyber incidents is more prevalent than the statistics suggest ([19]).

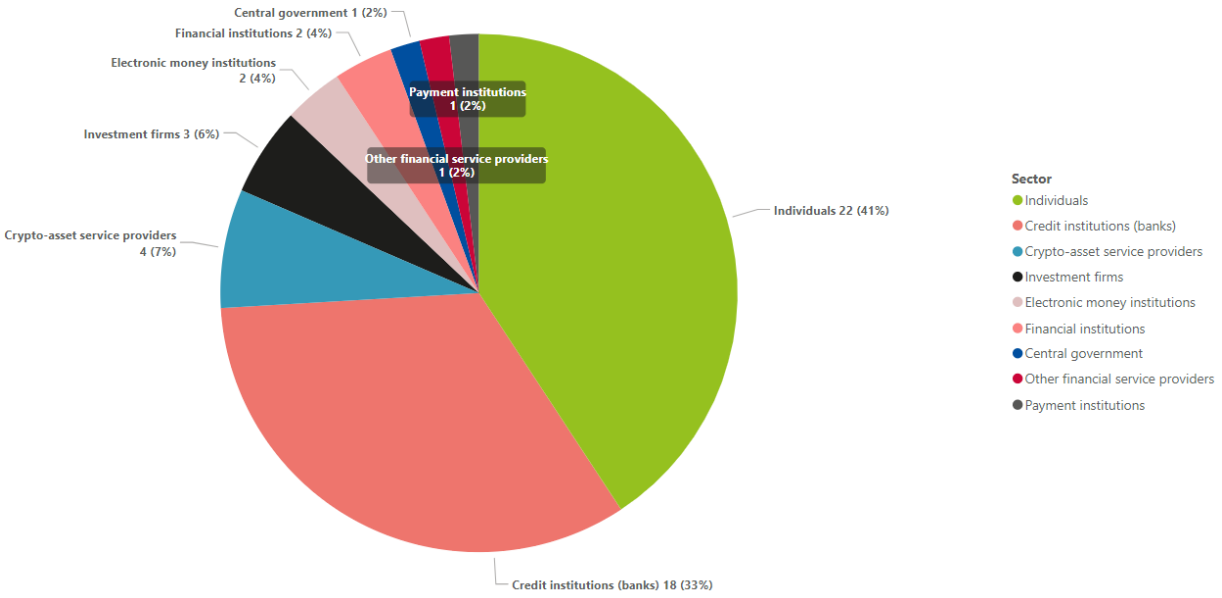
According to the 2024 IOCTA, 'fraud, especially investment-related fraud, is the most frequently identified predicate offence involving the illegal use of cryptocurrencies'. Cybercrime threat actors mostly request Bitcoin for ransom, but the criminal use of altcoins ([20]) seems to be increasing. In 2023, an increase in the usage of swapping services for laundering cryptocurrency was observed. Swapping is mostly done to ensure criminal funds are secure and stable – for security, cryptocurrencies are swapped to privacy coins, while for stability, cryptocurrencies are swapped to stablecoins ([21]).

([19]) Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2024*, Publications Office of the European Union, Luxembourg, 2024, https://data.europa.eu/doi/10.2813/442713.

([20]) 'The term "altcoin" refers to any cryptocurrency other than Bitcoin. Altcoins have the same design and function, and developers can create them for various uses.' Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2024*, Publications Office of the European Union, Luxembourg, 2024, https://data.europa.eu/doi/10.2813/442713.

([21]) 'The term "stablecoin" refers to a type of cryptocurrency where the value of the digital asset is supposed to be linked to a reference asset, which is either fiat money, exchange-traded commodities or another cryptocurrency. This makes it less subject to price volatility than other types of cryptocurrencies'. Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2024*, Publications Office of the European Union, Luxembourg, 2024, https://data.europa.eu/doi/10.2813/442713.

Figure 10: Incidents of fraud to European financial entities (January 2023 to June 2024)

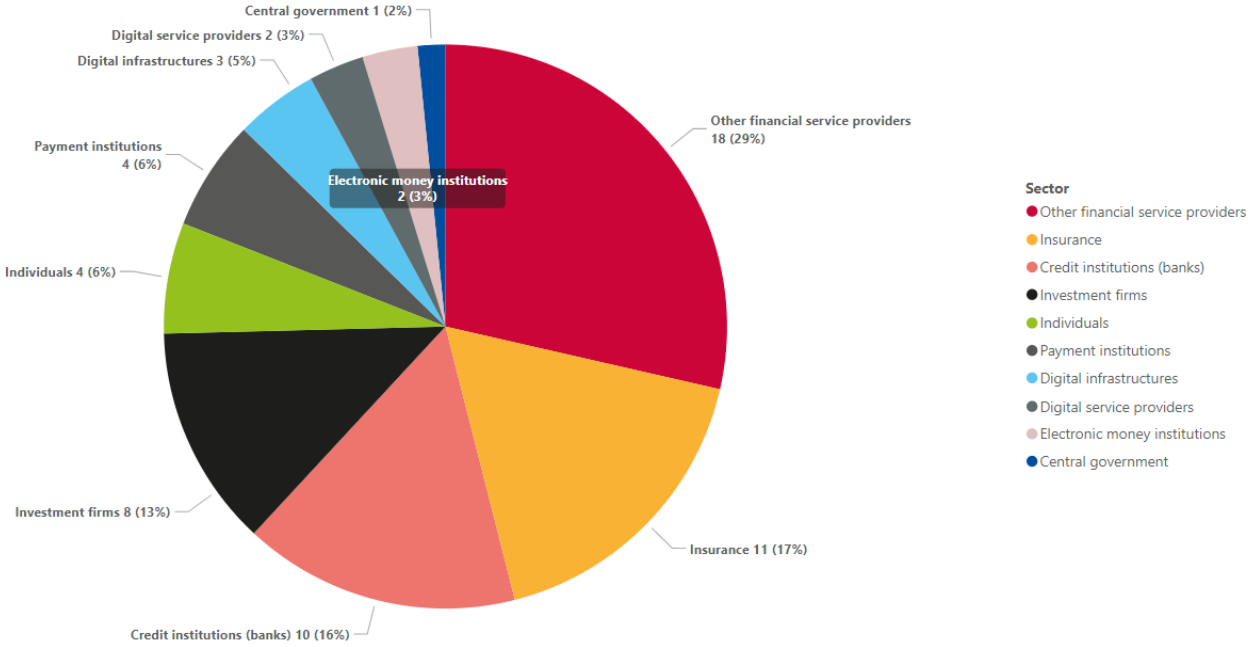


3.5 RANSOMWARE

According to the ENISA's Threat Landscape for Ransomware Attacks ([22]), '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' or in exchange for not publicly exposing the target's data. This 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. While ransomware was one of the prime threats, with several high-profile and highly publicised incidents, we observed fewer ransomware attacks compared to other sectors during the reporting period. It is worth mentioning that the incidents under analysis were reported on data leak sites. Based on our assessment of the impact, this threat remains a concern for the sector and is often coupled with data-related threats.

[22] ENISA, *ENISA Threat Landscape for Ransomware Attacks – July 2022*, 2022. https://data.europa.eu/doi/10.2824/456263.

Figure 11: Ransomware attacks to European financial entities (January 2023 to June 2024)



We observed ransomware mainly targeting other service providers (29 %), insurance organisations (17 %) and credit institutions (16 %). We assessed that companies with lower levels of maturity were more affected in the reporting period, which is why we saw fewer incidents in credit institutions. The impact of ransomware attacks was primarily financial loss (38 % of the cases), the exposure and sale of sensitive data (35 %) and operational disruption (20 %).

3.6 MALWARE

Malware, also referred to as malicious code or malicious logic, is an overarching term used to describe any software or firmware intended to perform an unauthorised process that will have an adverse impact on the confidentiality, integrity or availability of a system. In this report, we observed 21 cases of malware (6 % of the total incidents), including (banking) trojans, spyware and miners. Mobile malware fraud is a significant subset of the broader online fraud landscape, particularly as more people use mobile devices for banking, and is characterised by its specific targeting of mobile devices and methods such as smishing and malicious application distribution. Even though limited in number, these are usually campaigns that target a large number of individuals, primarily the customers of credit institutions. Examples of such banking trojans include [23]:

- Anatsa campaigns targeting Czechia;
- Mispadu targeting users in Italy, Poland and Sweden;
- Godfather targeting EU banking apps;
- Medusa (TangleBot) targeting Spain, Turkey, Italy, and France;
- Hydra targeting Android phones in Poland;
- Copybara used in fraudulent campaigns targeting the UK, Spain, and Italy;
- SpyNote targeting various customers of European banks; and
- Bizarro targeting customers of banks across Europe.

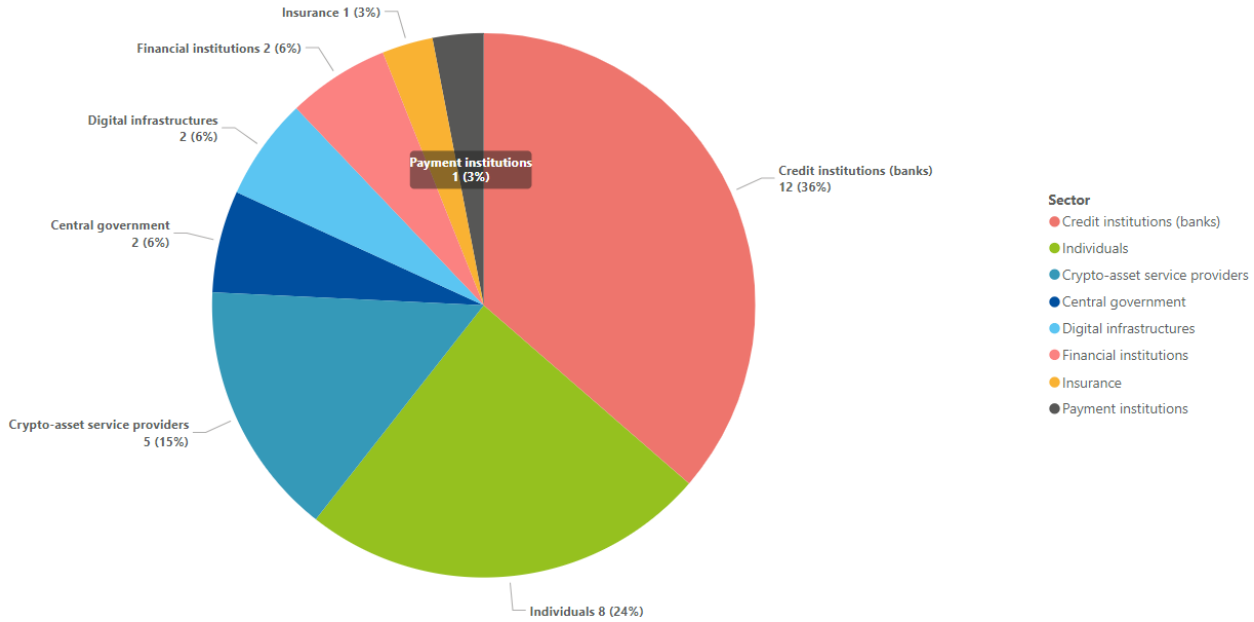
During the reporting period, a surge in mobile banking trojans was reported ([24]), with an increase in the complexity of their attack vectors. Research indicated a 200 % year-on-year growth in malware families targeting banking applications, expanding from 10 to 29 distinct families and from 600 to 1 800 affected applications globally ([25]). The rise of device-takeover-capable malware families highlights the increasing advancement of threats targeting banks.

([23]) These were banking trojans included in the observed incidents of the reporting period.
([24]) ENISA, *ENISA Threat Landscape 2024 – July 2023 to June 2024*, September 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.
([25]) Help Net Security, '29 malware families target 1 800 banking apps worldwide', Help Net Security website, 3 January 2024, https://www.helpnetsecurity.com/2024/01/03/banking-trojans-mobile-devices/.

These malware families grant attackers full control over infected devices, enabling them to perform a wide range of malicious activities, from stealing login credentials to executing fraudulent transactions. The resurgence of Anatsa in 2023, marked by a series of six distribution waves, underscores the persistent and evolving nature of this threat ([26]). By releasing non-malicious versions of applications that later perform updates with malicious code, Anatsa bypasses initial security checks and builds credibility with users. This approach, combined with the malware's technical advancement, allows it to evade detection and maintain a persistent presence on infected devices. Emerging threats, such as GoldPickaxe ([27]), capable of synthesising deepfake videos using stolen facial recognition data, and Brokewell ([28]), a Trojan with extensive device-takeover capabilities, underscore the evolving nature of the global threat landscape in mobile banking.

In fact, 36 % of the observed incidents affected credit institutions (36 %), individuals (24 %) and crypto-asset service providers (15 %). The impact of these incidents included fraud and large-scale financial crimes (59 % of the cases), financial losses (21 %), the exposure and sale of sensitive information (14 %) and operational disruptions (7 %).

Figure 12: Malware targeting European financial entities (January 2023 to June 2024)



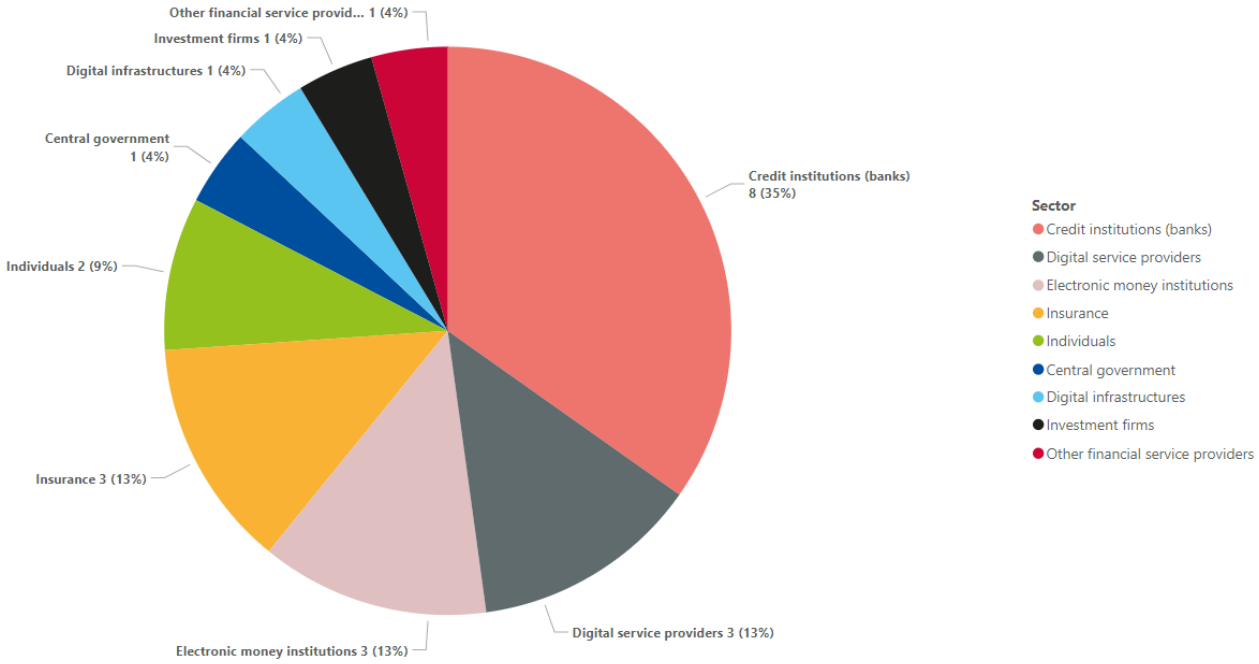
3.7 ATTACKS TO THE SUPPLY CHAIN

Supply chain attacks target service providers to gain access to multiple financial institutions through trusted relationships. By compromising a service provider, attackers *can* bypass direct defences and spread malware or gather intelligence across a wide range of targets, exploiting the interconnected nature of the financial sector. We have to highlight that during the reporting period we observed attacks on providers that affected financial institutions, most often including digital service providers, cloud service providers and payment services providers. However, financial organisations were affected only as a consequence, and a secondary attack on these organisations was not observed.

Although just 29 incidents involved attacks on a supplier, these were, in most cases, data breaches and ransomware attacks on the supplier side. Their impact was the exposure and sale of sensitive data in 63 % of the cases, along with operational disruption (26 %) and financial loss (11 %).

([26]) Threat Fabric, 'Anatsa trojan returns: targeting Europe and expanding its reach', Threat Fabric website, 19 February 2024, https://www.threatfabric.com/blogs/anatsa-trojan-returns-targeting-europe-and-expanding-its-reach.
([27]) WeLive Security, 'ESET threat report H1 2024', WeLiveSecurity website, 27 June 2024, https://www.welivesecurity.com/en/eset-research/eset-threat-report-h1-2024/.
([28]) Threat Fabric, 'Brokewell: do not go broke from new banking malware!', Threat Fabric website, 25 April 2024, https://www.threatfabric.com/blogs/brokewell-do-not-go-broke-by-new-banking-malware.

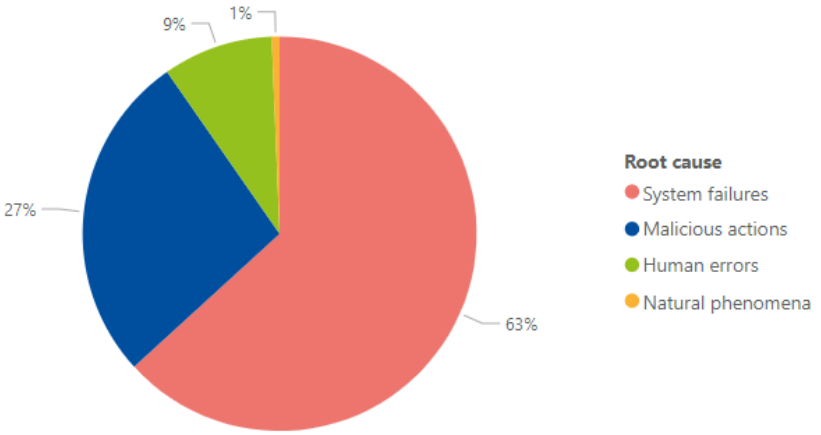
Figure 13: Attacks on providers of European financial entities (January 2023 to June 2024)



3.8 OTHER THREATS

Concerning other threats, 73 % of the officially reported incidents from financial entities under the NIS directive were considered non-malicious ([29]). These are usually not found within the incidents collected by open sources by ENISA, but they provide valuable insight on what causes significant impacts on European financial entities. Reported incidents were caused by system failures (64 % of the total reported incidents) and user errors (9 %). System failures were caused by software bugs (43 % of the reported system failures), faulty software changes and updates (18 %), hardware failures (10 %), faulty hardware changes and updates (6 %), or power cuts (2 %). User errors related to errors in software changes and updates (35 %), software bugs (7 %) or policy and procedure flaws (7 %).

Figure 14: Incidents of significant impact reported in 2023 under the NIS directive



([29]) Data retrieved by the cybersecurity incident reporting and analysis system: https://ciras.enisa.europa.eu/.

4. THREAT ACTORS

As in the *ENISA Threat Landscape* 2024 (30), we considered three main categories of cybersecurity threat actors: state-nexus actors, cybercrime actors and hacktivists.

- **State-nexus actors**' objective is primarily espionage and, although the techniques they employ might not always be that novel, their goals and planning allow them to execute advanced, large-scale or targeted and long-term operations. State-nexus actors often spend considerable time investigating their targets to identify weaknesses and entry points and they focus on avoiding operational mistakes. State-nexus actors do not only target other states. They can as well target other organisations for sensitive data or conduct operations to obtain funding for their country.
- **Cybercrime actors'** primary motive is financial gain. Cybercrime actors perform attacks which are opportunistic and indiscriminate as they target the data or infrastructure that has the highest impact on the operations of victims. They can either steal directly from victims, can extort the victim or can monetise the information stolen from victims.
- **Hacktivists'** objectives often involve disruption, and they use hacking to affect some form of political or social change. Hacktivist groups are very diverse and vary heavily in skillsets and capabilities. Hacktivist threat actors are sometimes also leveraged by state-nexus actors for influence operations or other forms of intrusion campaigns.

In addition, for this report, we considered **insider** actors, both those with malicious intent and those with non-malicious intent. We were able to identify only two cases attributed to human errors or misconfigurations and poor security practices. For the cases in which one of the above types of actors was not identified, we categorised the incident as **unknown**.

4.1 THREAT ACTOR GOALS

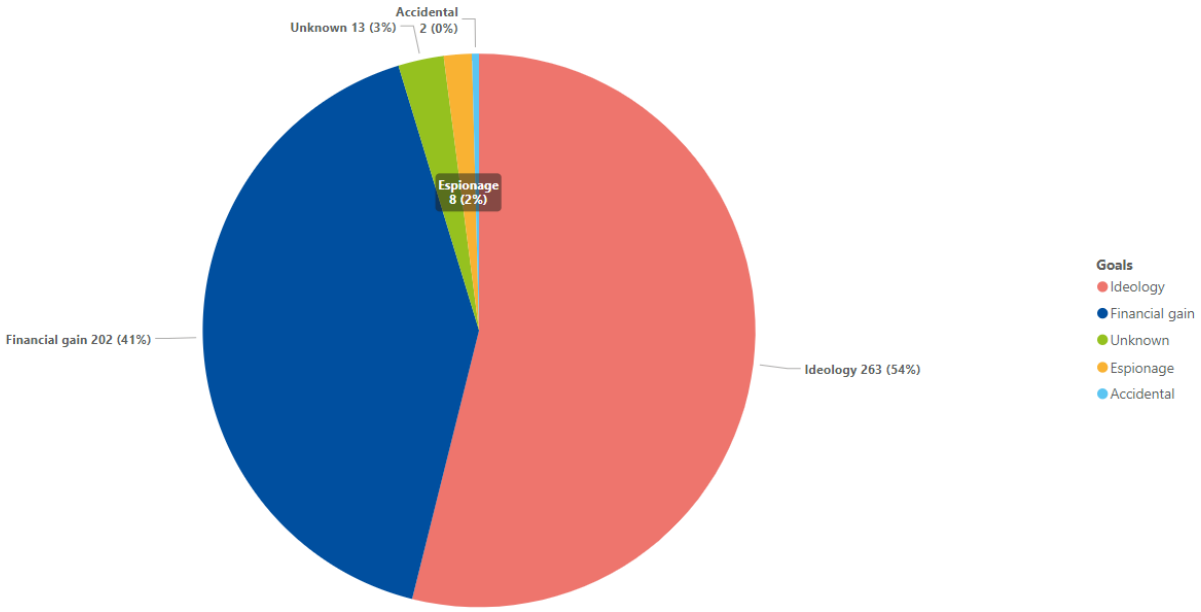
For the analysis of the incidents, we have considered the following goals.

- **Accidental**: when the incident was unintentional. These are often user errors or system failures.
- **Espionage**: when the aim of the attack is information collection (intellectual property or strategic information).
- **Financial gain**: when there is a clear monetary gain underlying the attack, such as extortion, selling stolen data, or stealing proprietary information, trade secrets or other valuable intellectual assets. The stolen data may be used for competitive advantage, to replicate products or services or to undermine the target's market position.
- **Ideological**: when the attack is linked to hacktivist activity, and there are clear declarations about the aim of the attack by the actor.
- **Unknown**: when we can make no clear conclusions on the goals.

The overall statistics are depicted in Figure 15. Ideological goals and financial gain were the primary goals of threat actors (at 54% and 41%, respectively) during the reporting period regarding the relevant incidents collected. Only 2% of the incidents were linked with espionage, while in another 3% of incidents (13 incidents), the motivations could not be determined with certainty by ENISA (these are marked as 'unknown'). This lack of clarity is attributed to a shortage of sufficient data to enable ENISA to conduct a comprehensive assessment and reach a conclusive determination regarding the motives behind these incidents.

Figure 15: Threat actor goals against European financial entities (January 2023 to June 2024)

(30) ENISA, *ENISA Threat Landscape 2024 – July 2023 to June 2024*, September 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.



We were able to identify two accidental cases, which were not malicious in nature. In one instance, the financial data of 52 000 clients were leaked due to user error, and in another one, the trading activity of over 300 000 users spanning the past 6 years was leaked due to a misconfigured web server. Even though such cases are not often publicly disclosed, we have additional information stemming from the incident reporting taking place under the NIS directive. In 2023, out of the 155 incidents of significant impact officially reported to national competent authorities ([31]), 9 % (14 incidents) were caused by human errors and 64 % by system failures (98 incidents).

We will discuss in more detail the goals of specific threat actor groups in the following sections.

4.2 THREAT ACTOR ANALYSIS

In the next section, we explore the trends related to each threat actor. 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 threat actors' goals, impact and targeting along with tactics, techniques, and procedures.

During the reporting period, we noticed an increased number of threat actors active in the European financial sector ([32]). Over the course of the reporting period, we pinpointed the 10 most active threat actors overall for our collected data. It is worth highlighting that a significant majority of the events (290 incidents) could not be associated to any specific threat actor.

([31]) Entities in the finance and banking sectors of the NIS directive.
([32]) Cipollone, P., 'One step ahead: Protecting the cyber resilience of financial infrastructures', introductory remarks at the ninth meeting of the Euro Cyber Resilience Board for pan-European Financial Infrastructures, Frankfurt am Main, 17 January 2024, https://www.ecb.europa.eu/press/key/date/2024/html/ecb.sp240117~3e839b396f.en.html.

Figure 16: Top 10 threat actors during the reporting period of January 2023 to June 2024

4.2.1 State-nexus actors

In the period analysed, state-nexus actors continued to pose a significant threat to the European Financial Sector. Even though they were not highly represented in our sample, we analysed incidents and official warnings about such groups and their targeting of the finance sector worldwide.

4.2.1.1 Trends

State-nexus actors are engaging in cybercrime. State-nexus actors appear to be targeting crypto-asset service providers to steal large sums of money through fraudulent transactions ([33]). For instance, North Korean advanced persistent threats (APTs), such as those attributed to the Lazarus Group, are involved in extensive cybercrime activities, including cryptocurrency theft and ransomware attacks ([34]) ([35]) ([36]) ([37]). The US Federal Bureau of Investigation recently linked the Lazarus Group to a USD 41 million cybertheft from Stake.com on 4 September 2023, highlighting their ongoing criminal activity ([38]).

Importance of espionage for state-nexus actors. Intelligence gathering remained a critical objective for many state-nexus actors, according to cyber espionage observed overseas ([39]). These campaigns aimed to collect sensitive information that could be used to gain economic advantages and strategic insights. By compromising financial

([33]) Insikt Group, 'Crypto country: North Korea's targeting of cryptocurrency', Recorded Future website, 30 November 2023, https://go.recordedfuture.com/hubfs/reports/cta-2023-1130.pdf.
([34]) Baran, G., 'Lazarus Group attacking crypto users via Telegram to deploy malware', Cyber Security News website, 8 December 2023, https://cybersecuritynews.com/lazarus-group-attacking-crypto/.
([35]) Lakshmanan, R., 'N. Korean hackers "mixing" macOS malware tactics to evade detection', The Hacker News website, 28 November 2023, https://thehackernews.com/2023/11/n-korean-hackers-mixing-and-matching.html.
([36]) Lakshmanan, R., 'North Korea's Lazarus Group launders $900 million in cryptocurrency', The Hacker News website, 6 October 2023, https://thehackernews.com/2023/10/north-koreas-lazarus-group-launders-900.html.
([37]) Elliptic Research, 'How the Lazarus Group is stepping up crypto hacks and changing its tactics', Elliptic website, 15 September 2023, https://www.elliptic.co/blog/how-the-lazarus-group-is-stepping-up-crypto-hacks-and-changing-its-tactics.
([38]) Federal Bureau of Investigation, 'FBI identifies Lazarus Group cyber actors as responsible for theft of $41 million from Stake.com', Federal Bureau of Investigation News website, 6 September 2023, https://www.fbi.gov/news/press-releases/fbi-identifies-lazarus-group-cyber-actors-as-responsible-for-theft-of-41-million-from-stakecom.
([39]) Centre for Cyber Security, 'The cyber threat against the Danish financial sector – Threat assessment', November 2024, https://www.cfcs.dk/globalassets/cfcs/dokumenter/trusselsvurderinger/en/cyber-threat-assessment-financial-sector-2024.pdf.

institutions, these actors could access proprietary data and other valuable information, which is crucial for both economic and political strategies.

Use of known vulnerabilities or leveraging zero-day vulnerabilities. State-nexus actors have increasingly exploited vulnerabilities to gain access to financial systems in Europe throughout 2024. These groups use advanced persistent threats (APTs) to conduct cyber espionage, sabotage, and financial theft. For example, APT29, which is linked to Russian intelligence, has targeted European financial institutions ([40]). Similarly, Chinese APT groups such as APT10, also known as Stone Panda, have focused on stealing sensitive data and intellectual property from Taiwanese financial institutions, leveraging zero-day supply chain attacks ([41]).

4.2.2 Cybercrime groups

Cybercrime groups face increasing challenges in breaching the defences of major financial institutions. Shifting tactics towards exploiting the human factor – customers who lack proficiency with digital technologies – is likely to increase in the following years. During our analysis, we observed multiple social engineering attacks that trick victims into revealing sensitive information or granting access to financial resources.

4.2.2.1 Trends

Use of zero-day vulnerabilities. Exploiting zero-day vulnerabilities was another strategy employed by cybercrime groups. These attacks involved taking advantage of previously unknown security flaws that had not yet been patched. The financial sector was also heavily impacted by a zero-day vulnerability in MOVEit software, a file transfer program. This vulnerability, codenamed CVE-2023-34362, allowed the ransomware group Cl0p (also known as FIN11 or Lace Tempest) to gain unauthorised remote access to MOVEit transfer databases ([42]) ([43]), which facilitated further attacks ([44]). In a notable case, four major European banks – Deutsche Bank, ING Bank, Postbank and Comdirect – reported data leaks, which were a result of the same third-party business vendor being breached in the Cl0p MOVEit hacks ([45]). This further highlights the reliance of financial organisations on third-party providers and that cybercrime actors are targeting their supply chains.

The prevalence of fraud and scams in cybercrime. Fraud and scam operations are also prevalent among cybercriminals. These can include various types of online scams, such as fake investment schemes, fraudulent online auctions and other deceptions designed to trick victims. Operation Magalenha, targeting Portuguese banks ([46]), suggests a concerning trend of cybercriminals tailoring their attacks to specific financial institutions. This necessitates continuous threat intelligence gathering and scenario planning to address potential sector-specific attacks. Financial institutions should consider collaborating with industry peers to share threat intelligence and develop collective defences against specialised financial fraud.

Use of artificial intelligence (AI). These operations often rely on sophisticated social engineering techniques to deceive victims and can be highly profitable for the perpetrators. The use of AI-powered phishing scripts and social engineering tactics with fake invoices showcases a shift towards more sophisticated attacks designed to bypass traditional security measures. Groups are increasingly using AI ([47]) to reach more potential victims and to have more convincing messages, and sometimes these techniques are so successful that users refuse to listen to warning messages from banks that detect attempted payments to platforms known to be fraudulent ([48]). AI capabilities are

([40]) Cybersecurity and Infrastructure Security Agency, 'Russian Foreign Intelligence Service (SVR) exploiting JetBrains TeamCity CVE globally', Alert code AA23-347A, 13 December 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-347a.
([41]) CyCraft Technology Corp, 'Smokescreen supply chain attack targets Taiwan financial sector, a deeper look', Medium website, 1 March 2022, https://medium.com/cycraft/smokescreen-supply-chain-attack-targets-taiwan-financial-sector-a-deeper-look-8acf290ddb96.
([42]) Anwalt.de, 'Data leak at Deutsche Bank and ING larger than previously known', Anwalt.de website, 29 September 2023, https://www.anwalt.de/rechtstipps/datenleck-bei-deutscher-bank-und-ing-groesser-als-bislang-bekannt-216908.html.
([43]) Kovacs, E., 'Evidence suggests ransomware group knew about MOVEit zero-day since 2021', Securityweek website, 9 June 2023, https://www.securityweek.com/evidence-suggests-ransomware-group-knew-about-moveit-zero-day-since-2021/.
([44]) Bracken, B., 'Cl0p's MOVEit campaign represents a new era in cyberattacks', Dark Reading website, 5 July 2023, https://www.darkreading.com/cyberattacks-data-breaches/c10p-moveit-campaign-new-era-cyberattacks.
([45]) Schappert, S., 'Deutsche Bank, ING and Postbank impacted by MOVEit hack', Cybernews website, 13 July 2023. https://cybernews.com/security/deutsche-ing-postbank-impacted-moveit-hack-clop/.
([46]) Toulas, B., '"Operation Magalenha" targets credentials of 30 Portuguese banks', Bleeping Computer website, 25 May 2023, https://www.bleepingcomputer.com/news/security/operation-magalenha-targets-credentials-of-30-portuguese-banks/.
([47]) Cepăreanu, A., 'ZF cybersecurity trends 2023. Bogdan Costea, Head of information security, ING Bank România: cybersecurity specialists are very important, especially since many phishing attacks have started to rely on artificial intelligence', Ziarul Financiar website, 27 September 2023, https://www.zf.ro/business-hi-tech/zf-cybersecurity-trends-2023-bogdan-costea-head-of-information-22137755.
([48]) 'The Year of email and WhatsApp fraud. Alin Becheanu (ING) on how to protect yourself', YouTube website, 5 January 2024, https://www.youtube.com/watch?v=nO7DTqJGtFc.

being leveraged to make social engineering campaigns more realistic, personalised, deceptive and psychologically manipulative. AI-powered cryptocurrency scams are on the rise, with perpetrators using platforms like YouTube to trap unsuspecting victims ([49]).

4.2.2.2 Ransomware

During the analysis period, threat actors utilized various ransomware variants, either through different Ransomware-as-a-Service (RaaS) programs as affiliates or independently. By monitoring multiple data leak sites, we were able to gather relevant statistics.

Akira ([50]) is a ransomware-as-a-service group, first observed in late March 2023, operating as a ransomware-as-a-service (RaaS) scheme for personal gain. Since its emergence, Akira has targeted a wide range of businesses and critical infrastructure organisations across Australia, Europe and North America. Initially designed to attack Windows systems, the ransomware expanded in April 2023 to include a Linux variant, specifically targeting VMware ESXi virtual machines. By 1 January 2024, Akira had impacted over 250 organisations and reportedly generated approximately USD 42 million in ransom payments ([51]) ([52]).

TA505 (or FIN11 subset of TA505 as tracked by Mandiant) financially motivated threat actor leveraging **Cl0p** ransomware have been active since at least February 2019. The group operate under the RaaS model, recruiting affiliates to expand its operations. Cl0p ransomware have primarily targeted the industrial, financial and technology sectors. The group operated its own data leak site accessible via Tor and issues high ransom demands, which can reach tens of millions of dollars ([53]) ([54]).

LockBit was the most deployed ransomware variant in 2022 being leveraged both by the group and affiliates. It was first observed in 2019 and is suspected to have originated from Eastern Europe. The group operates under a RaaS model, recruiting affiliates in return for a fraction of the ransom obtained from each attack. The group targets a wide range of industry sectors, including financial services, communications, and commercial and retail sectors globally. LockBit's tactics include T1486 – Data Encrypted for Impact and T1005 – Data from Local System. These tactics require high technical ability to search local system sources for files of interest and sensitive data prior to exfiltration. LockBit also possesses the skill to encrypt data on target systems, interrupting the availability of those systems and network resources ([55]). On 24 February 2024, they were disrupted by a law enforcement operation, Operation Chronos ([56]), and have since remained mostly inactive.

NoEscape is a ransomware-as-a-service group that surfaced in May 2023 and is speculated to be using a possible rebranding of the Avaddon ransomware, although this has not been confirmed. NoEscape also operates on a RaaS model. However, unlike some other RaaS schemes, NoEscape's developers claim to have independently created the ransomware and its entire supporting infrastructure, positioning it as a unique offering within the ransomware landscape ([57]).

4.2.3 Hacktivists

The emergence of crowd-sourced distributed denial-of-service (DDoS) attacks represents an escalation in cybercriminal activities with geopolitical tensions serving as a catalyst. Volunteers with limited resources and minimal technical expertise are now able to contribute to significant DDoS attacks by downloading and running client software on their devices or cloud-hosted hosts. Crowd hacktivists are compensated in cryptocurrency, based on their contribution to

([49]) Avast, 'Avast Q1/2024 threat report', Avast website, 14 May 2024, https://decoded.avast.io/threatresearch/avast-q1-2024-threat-report/.
([50]) Cybersecurity and Infrastructure Security Agency, '#StopRansomware: Akira ransomware', Alert code: AA24-109A, 18 April 2024, https://www.cisa.gov/news-events/cybersecurity-advisories/aa24-109a.
([51]) SOCRadar, 'Dark web profile: Akira ransomware', SOCRadar website, 19 April 2024, updated 1 October 2024, https://socradar.io/dark-web-profile-akira-ransomware/.
([52]) Antoniuk, D., 'Akira ransomware compromised at least 63 victims since March, report says', The Record website, 26 July 2023, https://therecord.media/akira-ransomware-early-victims-conti-links.
([53]) National Cyber Security Centre, 'MOVEit vulnerability and data extortion incident', National Cyber Security Centre website, 7 June 2023, updated 27 June 2023, https://www.ncsc.gov.uk/information/moveit-vulnerability.
([54]) Jones, C., 'The GoAnywhere data breach explained', ITPro website, 25 August 2023, https://www.itpro.com/security/data-breaches/370409/the-goanywhere-data-breach-explained.
([55]) Cybersecurity and Infrastructure Security Agency, 'Understanding ransomware threat actors: LockBit', Alert code: AA23-165A, 14 June 2023, https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a.
([56]) Europol, 'Law enforcement disrupt world's biggest ransomware operation', Europol website, 20 February 2024, https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation.
([57]) SOCRadar, 'Dark web profile: NoEscape ransomware', SOCRadar website, 20 September 2023, https://socradar.io/dark-web-profile-noescape-ransomware/.

DDoS attacks against digital assets. This type of approach is attracting both ideologically motivated individuals and those seeking to profit from cybercrime. Besides implementing ranking systems and financial incentives for the most productive attacks, the groups have also developed a systematic approach to stage attacks. The most resource-intensive components of the targeted resources are identified and analysed, the attack is developed centrally to simulate real user interaction and is then distributed by the crowd-sourced platform ([58]).

Hacktivists are targeting financial institutions ([59]) ([60]), such as payment processing systems and ATMs ([61]), aimed to cause significant operational disruption. The ENISA threat landscape report of 2024 shows the finance sector as the 3rd more targeted sector. Such attacks could potentially result in financial losses and undermine customer trust in the financial system, amplifying the overall impact of the cyber operation. We assess that the groups' current capabilities are limited, having a low impact on the overall financial European eco-system stability. Future geo-pollical conflicts and state sponsorship may amplify the effectiveness and capabilities of these groups.

4.2.3.1 Trends

DDoS attacks disrupt operations. European financial organisations are being increasingly targeted by hacktivists through numerous DDoS attacks. Geopolitical developments related to Ukraine and the Middle east have underscored the use of cyberattacks as tools for political retaliation and disruption ([62]). These attacks overwhelm systems, hindering customer access to online and mobile banking services. We observed DDoS attacks claimed by hacktivists in almost all Member States and in Ukraine throughout the reporting period. In some of the cases, longer outages were observed.

Beyond banks: broader infrastructure targeted. Often, the focus of the attacks was not only on financial institutions themselves. We observed such attacks happening as part of larger campaigns that targeted other sectors of a Member State, such as public administration, energy or transport. By targeting infrastructure that supports financial services, attackers can create a domino effect, inflicting a widespread effect. The landscape is further complicated by the involvement of state-backed actors, as these groups often target institutions based on geopolitical tensions or political developments.

The *ENISA Threat Landscape 2024* reports that DDoS can be used as a smokescreen from other attacks, stating, 'Akamai claim[ed] that attacks on the banking and financial industries were aimed mainly at hitting reputations or distracting security experts while ransomware, data theft and cyber espionage attacks were being launched'.

Evolving capabilities of hacktivist groups. The fact that operational disruption is taking place demonstrates that the ability of these groups is increasing. Hacktivists further mimic cybercrime actors/tactics, such as using ransomware payloads to disrupt targets and draw attention to their political causes. Alongside the blending of hacktivism with state-nexus activity, it is likely hacktivists will increasingly adopt cybercrime tactics, sometimes with direct or indirect support from these state-nexus actors ([63]).

4.2.3.2 Threat Actors Profiles

When it comes to hacktivist activity, the reporting period saw a number of prominent threat actor groups emerging as the most active.

NoName057(16), a pro-Russia hacktivist group, has become a major player in the cyberwarfare surrounding Russia's invasion of Ukraine. While they target various sectors, their focus on the financial industry deserves particular attention. These DDoS attacks aim to overwhelm financial services in Ukraine and NATO-aligned countries. This deliberate

([58]) SOCRadar, 'Dark Web Profile: NoName057(16)', SOCRadar website, 6 March 2023, https://socradar.io/dark-web-profile-noname05716/.
([59]) The Wall street journal, 'Banks Face 'Hacktivist' Cyberattacks', WSJ website, 6 March 2024, https://www.wsj.com/articles/banks-face-hacktivist-cyberattacks-f23d3ec8.
([60]) NBC News, 'Russian-aligned cyber groups are seeking to target Western infrastructure, U.K. says', NBC News website, 19 April 2023, https://www.nbcnews.com/news/russian-aligned-cyber-groups-are-seeking-target-western-infrastructure-rcna80310.
([61]) Financial services top target for DDOS attacks, March 2024, https://www.finextra.com/pressarticle/99976/financial-services-top-target-for-ddos-attacks.
([62]) Europol, *Internet Organised Crime Threat Assessment (IOCTA) 2023*, Publications Office of the European Union, Luxembourg, 2023, p. 5, https://data.europa.eu/doi/10.2813/587536.
([63]) ENISA, *ENISA Threat Landscape 2024 – July 2023 to June 2024*, September 2024, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024.

disruption of financial stability aligns with Russia's strategic objectives, potentially hindering economic activity or causing public distrust.

NoName057(16)'s targeting patterns mirror Russia's interests, suggesting a level of coordination beyond mere hacktivism. Additionally, the group exhibits a high degree of organisation and operational consistency, hallmarks of state-backed APT groups ([64]). This level of structure, coupled with their boasts about attacks on Telegram channels, points towards a broader strategic agenda, possibly supported by Russian intelligence. Furthermore, potential connections between NoName057(16) and other Russian state-backed groups like Sandworm bolster the case for state sponsorship. These affiliations might grant them access to advanced cyberwarfare capabilities, escalating the threat beyond simple hacktivism**.**

Turk Hack Team (THT), a Turkish nationalist hacker group, emerged as a significant threat in the financial sector during the reporting period. Known for launching DDoS attacks, THT has targeted critical financial institutions like the Central Bank of Malta and Crédit Agricole Group. Their attacks are often politically motivated, aligning with tensions between Turkey and other nations. This targeted disruption of financial services highlights the vulnerability of the sector to cyberwarfare tactics employed by hacktivist groups. THT's actions underscore the need for robust cybersecurity measures within the financial industry to protect against increasingly sophisticated attacks.

ZulikGroup ([65]) targets various sectors in Eastern Europe, with their activities often involving unauthorised access to critical financial systems. This includes hacking the websites of banks and institutions in Estonia, Lithuania, Poland and Ukraine and potentially compromising sensitive financial data. Their diverse toolkit includes phishing emails, malware deployment, network infiltration attempts and social engineering tactics to manipulate individuals. Despite a brief hiatus in November 2023, ZulikGroup's resurgence highlights the ongoing threat posed by cybercriminals targeting the financial sector's vulnerabilities.

UserSec ([66]) is a pro-Russia cyber group known for targeting NATO countries and organisations backing Ukraine, driven by political motives. The group emerged as a prominent force during the invasion, leveraging Telegram for recruitment and communication. Although no official links to the Russian government have been established, UserSec's actions align closely with Russia's geopolitical aims, especially in destabilising Western nations and promoting pro-Russian narratives. In regard to UserSec's activity in the financial sector, they claimed to allegedly carry out DDoS attacks on the Latvian and Polish central banks (December 2023).

Anonymous Russia is another active hacking group often associated with Russian interests, targeting various Western entities as part of ongoing cyber confrontations. The group emerged as a counterpart to the global hacktivist collective Anonymous, which has generally supported Ukraine and opposed Russian activities during recent military aggression. Similarly, they use platforms like Telegram and other social media to share their attacks, make statements and rally support. Anonymous Russia operates alongside other pro-Russian groups in the cybersphere, like Killnet and NoName057(16), often focusing on amplifying Russia's geopolitical messaging ([67]). In regard to the financial sector, among their claimed victims were banks from Belgium, Czechia, France, Italy and Slovakia.

Anonymous Sudan has been responsible for numerous high-profile cyberattacks, particularly since its emergence in early 2023 ([68]). The group has targeted various sectors, including transportation, government and healthcare, but notably, it has also attacked major financial institutions ([69]). One such target was the European Investment Bank, which faced a DDoS attack in June 2023. In addition to financial services, Anonymous Sudan has also joined forces with other

([64]) Arghire, I., 'Canadian government targeted with DDoS attacks by pro-Russia group', SecurityWeek website, 18 September 2023, https://www.securityweek.com/canadian-government-targeted-with-ddos-attacks-by-pro-russia-group/.
([65]) 'Pro-Russia hacktivist group's latest activities', BE4SEC website, 8 September 2023, https://be4sec.com/2023/09/08/pro-russia-hacktivist-groups-latest-activities/.
([66]) SOCRadar, 'Dark web profile: UserSec, SOCRadar website, 30 September 2024, https://socradar.io/dark-web-profile-usersec/.
([67]) ThreatMon, 'In-depth analysis on the roles of threat actors and attacks in the Ukraine–Russia war – Anonymous Russia', https://threatmon.io/storage/anonymous-russia-in-depth-analysis-on-the-roles-of-threat-actors.pdf.
([68]) Sekoia, 'Anonymous Sudan', Sekoia website, https://www.sekoia.io/en/glossary/anonymous-sudan/.
([69]) Cyberint, 'Behind the mask of Anonymous Sudan: an analysis', Cyberint website, 9 August 2023, updated 19 December 2023, https://cyberint.com/blog/research/anonymous-sudan-an-analysis/.

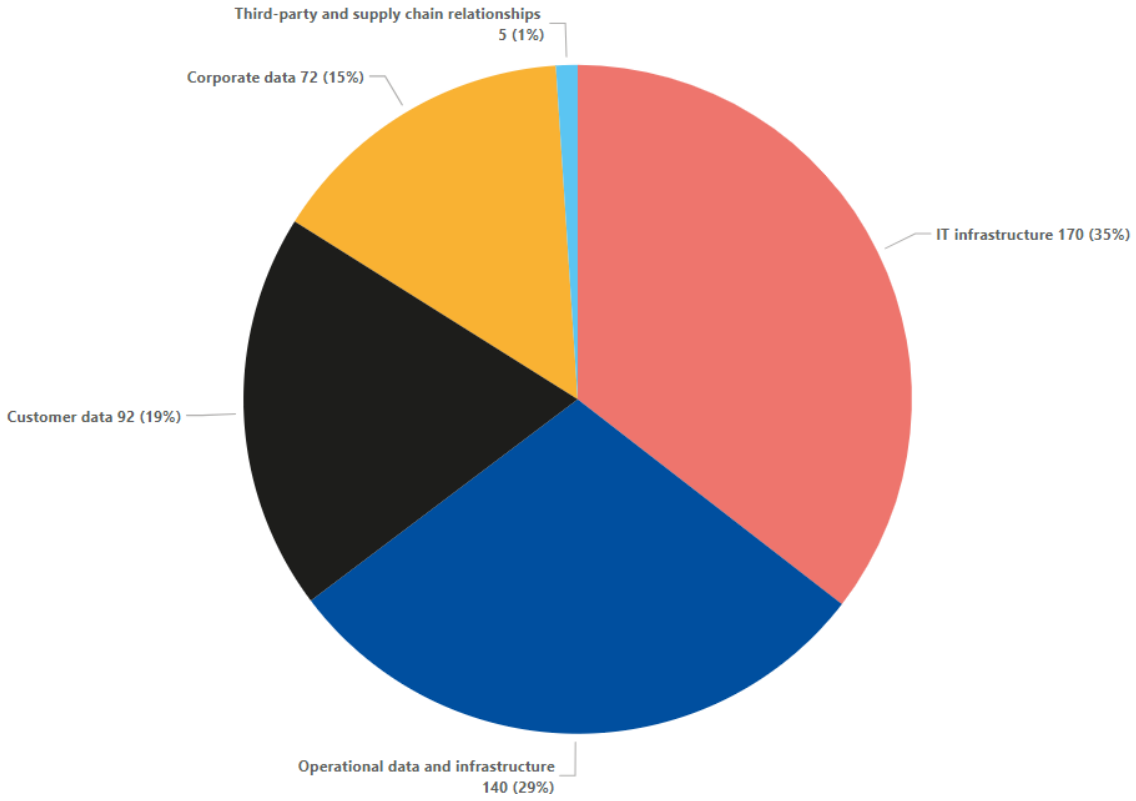
pro-Russian cyber groups, such as Killnet, to target organisations linked to Russia's invasion of Ukraine ([70]). Two Sudanese nationals were indicted for their alleged role in Anonymous Sudan in October 2024 ([71]).

([70]) Cloudflare, 'What is Anonymous Sudan?', Cloudflare website, https://www.cloudflare.com/learning/ddos/glossary/anonymous-sudan/.
([71]) United States Attorney's Office, Central District of California, 'Two Sudanese Nationals Indicted for Alleged Role in Anonymous Sudan Cyberattacks on Hospitals, Government Facilities, and Other Critical Infrastructure in Los Angeles and Around the World', US Department of Justice website, 16 October 2024, https://www.justice.gov/usao-cdca/pr/two-sudanese-nationals-indicted-alleged-role-anonymous-sudan-cyberattacks-hospitals.

5. IMPACT

In this chapter we analyse the effect of cyber threats on the European finance sector during the reporting period. We analysed which assets were affected by the incidents observed (Figure 17). The observed incidents resulted in impacts on various asset categories in the finance sector, with significant implications for operational continuity, data integrity and organisational trust. These cyber incidents primarily targeted IT infrastructure (31 % of the cases), operational data and infrastructure (28 %), personal information (25 %) and corporate data (15 %).

Figure 17: Impacted assets in European financial entities (January 2023 to June 2024)



The most often targeted asset type in the European finance sector is **IT infrastructure**, with 170 instances documented. The attacks often targeted key IT systems like servers, routers, firewalls and other network components. Financial organisations rely heavily on the integrity and availability of their IT infrastructure. Cyberattacks on this asset can cause extensive service interruptions, impacting anything from online banking platforms to transaction processing systems.

The second-most targeted asset type, **operational data and infrastructure**, saw 140 incidents. This category contains critical components that enable financial institutions' daily operations, such as trading data, payment systems and automated teller machine infrastructure. Attacks on operational data can disrupt the flow of financial transactions, cause settlement delays and interfere with real-time trading activity. These disruptions not only create immediate operational issues, but they can also have long-term consequences for market stability and public trust.

Customer data, including customer financial data, personal data and authentication data, was compromised in 92 cases. The exposure of customer data can have serious effects, such as identity theft, financial fraud and a loss of

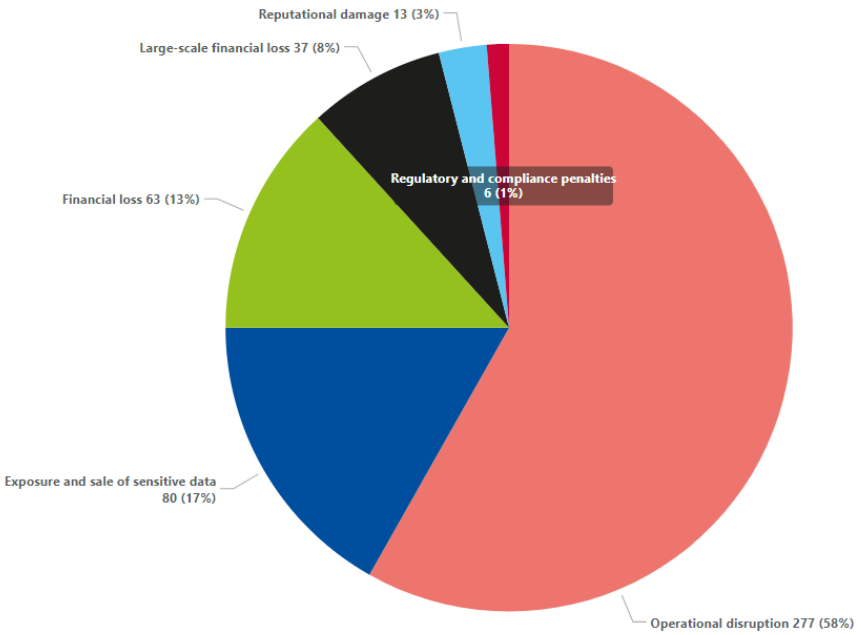
customer trust. Financial organisations handle massive volumes of sensitive information, making them prime candidates for data breaches.

There were 72 incidents involving **corporate data**. These assets include internal records, strategic plans, intellectual property and access credentials. Cyberattacks on company assets can result in the theft of valuable information, causing competitive disadvantages and financial losses. Such breaches frequently employ sophisticated strategies, such as spear phishing and social engineering, to get access to critical corporate information.

Although just 5 cases involving **third-party and supply-chain relationships** were documented, they constitute a substantial vulnerability. Financial institutions increasingly rely on third-party vendors and service providers for a variety of functions, including IT services and customer assistance. Cyberattacks on third-party businesses can pose dangers to the financial institution's environment, compromising sensitive data and disrupting services.

Cyber incidents in the finance sector can have far-reaching and multifaceted consequences, compromising operational efficiency, financial stability, regulatory compliance and customer trust. The main consequences observed include operational disruption (58 %), the exposure and sale of sensitive data (17 %), financial loss (13 %) and fraud and large-scale financial crimes (8 %), as depicted in Figure 18.

Figure 18: Impact (consequences) to European financial entities (January 2023 to June 2024)



The most common impact was **operational disruption**, with 277 cases reported. Cyberattacks that affect the functioning of financial institutions can have both immediate and far-reaching consequences. These disruptions can cause transaction processing to be halted, key financial activities to be delayed and individuals to lose access to banking services. Operational disruptions can cause considerable financial losses, reputational damage and a loss of customer trust. To solve this, financial institutions must engage in business continuity planning, disaster recovery solutions and resilient IT infrastructure to mitigate the effects of such disruptions.

The **exposure and sale of sensitive data** were reported in 80 cases. This results in the unlawful access and subsequent publication of confidential information, such as personal data and corporate data. The selling of such data on the dark web can lead to additional criminal activity, such as identity theft and financial fraud. Protecting sensitive data requires implementing robust encryption, access controls and continuous monitoring for data breaches. Additionally, timely incident response and communication strategies are vital to mitigate the effects of data exposure and maintain customer confidence.

Financial loss was a key outcome in 63 occurrences. Cyberattacks can cause direct financial losses by stealing funds, demanding ransom payments and incurring incident response and clean-up costs. Furthermore, financial organisations may face indirect costs such as higher insurance premiums, regulatory fines and long-term reputational damage. Implementing comprehensive risk management frameworks, increasing cybersecurity insurance coverage and maintaining a strong security posture are essential tactics for reducing financial losses caused by cyberattacks.

Large-scale financial loss (due to fraud and financial crime) was reported in 37 incidents. Cybercriminals target financial institutions to facilitate large-scale fraud, exploiting vulnerabilities in transaction systems and financial networks. These sophisticated attacks often involve state-sponsored actors and organised crime groups aiming to steal substantial amounts of money or manipulate financial markets. Strengthening fraud detection systems, conducting regular security audits and collaborating with law enforcement agencies are essential measures to combat large-scale financial crimes.

Reputational damage from cyber incidents is severe and long-lasting, as financial institutions rely significantly on client trust, and major data breaches or service outages can seriously harm their brand. In our analysis, only 13 cases were found with reputational damage being directly evidenced. However, we assessed that this is a consequence that is harder to quantify and is more of a secondary consequence. The theft of consumer data, in particular, can cause widespread distrust and a shift in customer loyalty towards competitors.

6. CONCLUSIONS

The analysis of cybersecurity incidents from January 2023 to June 2024 reveals several critical findings and concerns for the European financial sector. The finance industry remains a prime target for cyber threats due to the high value of financial data and the potential for significant financial gain.

The key findings include the following.

- **European banks** (credit institutions) were the most frequently targeted at a 46 % rate. **Government agencies and public sector organisations in finance** (13 %) followed next. **Individuals** (10 %) were lured into and defrauded by social engineering campaigns with a finance-relevant theme.
- The finance sector saw peaks in **DDoS activity linked to geopolitical events**, particularly Russia's invasion of Ukraine. Hacktivists frequently targeted European credit institutions (58 % of incidents) and government websites related to finance (21 %), causing operational disruptions and raising cybersecurity concerns.
- Financial institutions frequently suffered **significant losses** as a result of cyber incidents such as fraud, ransomware and data breaches. These losses were exacerbated by costs associated with remediation, legal fees and regulatory penalties.
    - **Data breaches and leaks** remained critical issues. Threat actors exploited vulnerabilities for financial gain through **fraud, supply chain attacks and social engineering**. European credit institutions (39 %) were the primary targets, with incidents leading to financial losses, regulatory penalties and reputational damage.
    - **Social engineering campaigns**, including phishing, smishing and vishing, were prevalent tactics used by cybercrime threat actors. These incidents aimed to steal sensitive information and commit financial fraud, affecting Individuals (38 %) and credit institutions (36 %). The results were financial loss, large-scale financial crimes and data exposure.
    - **Fraud** accounted for 6 % of overall incidents, primarily impacting Individuals (40 %) and credit institutions (35 %). Although reported cases seem low, under-reporting and secondary consequences from other cyberattacks suggest a broader issue. **Crypto-related cybercrime** saw a rise in thefts, scams and illicit laundering.
    - **Ransomware attacks** primarily targeted less mature financial entities, such as service providers (29 %) and insurance organisations (17 %), with impacts including financial loss (38 %), data exposure (35 %) and operational disruption (20 %).
- The **mobile threat landscape** remained dynamic and challenging, with increasing sophistication of mobile malware. Banking trojans and spyware posed significant threats by enabling device takeovers and fraudulent activities. Credit institutions (36 %) and Individuals (24 %) were impacted most.
- **Attacks on suppliers**, mostly data breaches and ransomware, resulted in the exposure and sale of sensitive data (63 %), operational disruption (26 %) and financial loss (11 %).

Stakeholders in the finance sector should invest strategically to improve cybersecurity resilience. Key measures include the following.

- **Investing in advanced technologies.** Financial entities must invest in advanced threat detection and response systems. Tools such as intrusion detection systems, intrusion prevention systems, and security information and event management solutions can detect anomalies and respond in real time. Integrating AI and machine learning enhances these capabilities through predictive analytics and automated responses to new risks.
- **Strengthening regulatory compliance.** Adherence to regulatory frameworks like the general data protection regulation, the NIS directive and DORA is crucial for maintaining cybersecurity resilience. Financial institutions must have robust policies and procedures to meet these regulatory requirements and conduct regular compliance audits.

- **Implementing comprehensive training programmes.** Employee training and awareness programmes are essential to reducing the risk of social engineering attacks and improving overall security hygiene. Financial institutions should invest in ongoing cybersecurity training, simulated phishing exercises and public awareness campaigns.
- **Creating strong incident response plans.** Financial institutions must have well-defined incident response plans detailing steps to be taken during a cyberattack. These plans should be regularly updated and tested through drills and tabletop exercises to ensure preparedness and effective incident management. Effective plans include precise action for detecting, containing, eradicating, recovering and communicating during a cyber incident.
- **Implementing multi-factor authentication (MFA).** Implementing MFA is crucial for preventing unauthorised access. MFA requires users to provide multiple forms of authentication, reducing the risk of credential theft and illegal access to critical data. Financial organisations should require MFA for both employee and customer access to vital systems and data.
- **Robust third-party risk management.** Financial institutions must assess the cybersecurity posture of their vendors and partners throughout the financial ecosystem. This includes requiring security audits from third parties, implementing stricter data-sharing protocols and conducting penetration testing to identify and mitigate potential weaknesses in the supply chain. Moreover, hardening system and cloud configurations and secure software and hardware development should be prioritised.
- **Collaboration and information sharing.** Collaboration and information sharing among financial institutions enhance overall cybersecurity resilience. Participation in industry forums, threat intelligence sharing platforms and public–private partnerships help institutions stay current on emerging threats and best practices.

TP-01-24-002-EN-N

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

Brussels Office
Rue de la Loi 107
1049 Brussels, Belgium

enisa.europa.eu

ISBN 978-92-9204-677-4
doi: 10.2824/5410466