EUROPEAN UNION AGENCY
FOR CYBERSECURITY

ENISA THREAT LANDSCAPE: HEALTH SECTOR

(January 2021 to March 2023)

JULY 2023

ABOUT ENISA

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

CONTACT

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

EDITORS

Marianthi Theocharidou, Ifigeneia Lella, ENISA

CONTRIBUTORS

Albert Haro Abad, Stephen Corbiaux

ACKNOWLEDGEMENTS

We would like to thank the Members and Observers of the ENISA Ad Hoc Working Group on Cyber Threat Landscapes, the members of the Network and Information Systems Cooperation Group (workstream on health), the European Health ISAC and Z-CERT, who reviewed this report, for their valuable feedback and comments.

LEGAL NOTICE

COPYRIGHT NOTICE

ISBN 978-92-9204-638-5 DOI 10.2824/163953 TP-04-23-546-EN-N

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 health sector in the EU. The report aims to bring new insights into the reality of the health sector by mapping and studying cyber incidents from January 2021 to March 2023. It identifies prime threats, actors, impacts and trends based on the analysis of cyberattacks targeting health organisations over a period of more than 2 years.

During this period, the European health sector faced a significant number of incidents. EU healthcare providers (53% of the total incidents), and especially hospitals (42%) were particularly affected. We also observed incidents targeting health authorities, bodies and agencies (14%) and attacks to the pharmaceutical industry (9%).

Ransomware is one of the prime threats in the health sector (54%), both in the number of incidents but also in its impact on health organisations. We expect this trend to continue. In fact, 43% of ransomware incidents are coupled with a data breach or data theft, while disruptions are the other common effect of the attack. Almost half of total incidents (99 incidents, 46%) are a form of threat against the data of health organisations (data breaches, data leaks). Data related threats continue to be one of the main threats in the sector, not only for Europe but also globally.

It is important to note that the reporting period covers a large part of the Covid-19 pandemic era, when the healthcare sector was one of the prime victims of cyber attackers. During the reporting period, cybercriminals had the heaviest impact on the sector, in particular ransomware threat actors driven by financial gain (53%). This is linked to the increase in ransomware attacks in general but also to the value of patient data including electronic health records. In fact, patient data were the most targeted assets (30%) throughout the reporting period.

The pandemic caused data leakage of patient data from Covid-19 related systems or from testing laboratories on multiple occasions and in multiple countries. These leaks were either due to the collaboration of malicious insiders or, in most cases, accidental due to poor security practices and misconfigurations. These incidents offer lessons to be learned on poor cybersecurity practises when there are pressing operational needs, in this case even more pressing due to the pandemic.

Attacks on healthcare supply chain and service providers caused disruptions or losses to organisations in the health sector (7%). We assess that these types of attacks will remain highly relevant for the sector in the future, especially in conjunction with the risks posed by vulnerabilities in healthcare systems and medical devices. In a recent ENISA study, healthcare was the sector that declared the most security incidents related to vulnerabilities in software or hardware. Indeed, 80% of the healthcare organisations interviewed declared that more than 61% of their security incidents were caused by vulnerabilities.

Geopolitical developments and hacktivist activity increased the number of DDoS attacks against hospitals and health authorities in early 2023, reaching 9% of total incidents. This was due to a surge in DDoS attacks by pro-Russian hacktivist groups who aimed to disrupt healthcare providers and health authorities in the EU. We expect this trend to continue; however the actual impact of these attacks remains relatively low.

In terms of impact, the incidents observed caused mainly breaches or theft of data (43%), disrupted healthcare services (22%) and other services not related to healthcare (26%). Data breaches affected healthcare entities in 40% of the total number of incidents, and, in particular, hospitals (27%) and primary care (8%). Disruption of healthcare services took place when healthcare entities (82%) and health authorities (12%) were disrupted.

Other impacts include financial losses but this is an impact which is difficult to assess. The ENISA NIS Investment 2022 study indicates that the median cost of a major security incident in the health sector is 300 000 Euro. We also observed sanctions imposed by data protection authorities as well as reputational harm to healthcare providers after major data breaches.

Patient safety remains a top concern for the health community due to potential delays in the triage and treatment of patients, or due to potential effects on the well-being of patients whose sensitive information is being revealed or who are being subjected to extortion.

According to a recent study by ENISA, only 27% of organisations surveyed in the health sector have a dedicated ransomware defence programme and 40% of the organisations have no security awareness programme for non-IT staff. In another recent survey by the NIS cooperation group, 95% of the health organisations surveyed face challenges when performing risk assessments, while 46% have never performed a risk analysis. These findings highlight the pressing need for health organisations to apply cyber hygiene practices. These may include offline encrypted backups of critical data, awareness raising and training programmes for healthcare professionals, vulnerability handling and patching, stronger authentication methods, cyber incident response plans and contingency plans, and more. The commitment of senior management is key, especially now that the NIS2 directive introduces liabilities for top management.

1. INTRODUCTION

This is the first ENISA threat landscape report which brings insights into cyber threats targeting the European health sector. The sector was selected due to its criticality and its importance to European citizens and their well-being. In the ENISA Threat Landscape 2022[1], around 7% of the observed incidents targeted health organisations. Moreover, 32% of the incidents with a significant impact reported under the Network and Information Security Directive[2] in 2022[3] were incidents in the EU health sector. Additionally, during 12 consecutive years the healthcare industry had the highest average cost of a breach worldwide[4].

In this report, we have analysed cyber incidents targeting the health sector from January 2021 to March 2023. This period is referred to as the 'reporting period' throughout the report. We collected publicly reported cyber incidents affecting various types of organisations related to health. These include:

- **healthcare providers**[5], such as hospitals, primary care providers, sociosanitary care providers, dental care providers, emergency services, mental health institutions, etc.,
- EU reference **laboratories**[6], entities carrying out **research and development** activities for medicinal products[7] and, more generally, **organisations conducting health related research**,
- entities manufacturing basic pharmaceutical products and pharmaceutical preparations[8], and the **pharmaceutical industry** in general,
- entities **manufacturing medical devices**[9] and **biotechnology manufacturers**,
- **health authorities, bodies and agencies** nationally and in the EU,
- **health insurance organisations**,
- **residential treatment facilities** and **social services providers**.

To conduct this study, the ENISA Cybersecurity Threat Landscape Methodology[10] was applied. Data collection and analysis focused on cyber incidents observed in EU member states and neighbouring countries (Norway, Switzerland and the United Kingdom). This is by no means the complete list of incidents that occurred during the reporting period. ENISA gathered a list of major incidents based on open-source intelligence (OSINT)[11] and ENISA's own cyber threat intelligence capabilities. The data collected were further analysed by ENISA's threat landscape team and external experts.

These incidents serve as the foundation for identifying a list of prime threats and the source material for several trends and statistics in the report. The incidents were analysed in detail to identify their core elements, providing answers to some important questions such as how the attacks happen, which systems are being targeted, and which health organisations are most affected and how. An in-depth 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 by ENISA and external experts. 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[12]. The report has been validated and supported by the ENISA Ad Hoc Working

[1] ENISA Threat Landscape 2022, November 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
[2] 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, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive)
[3] Data retrieved by the Cybersecurity Incident Reporting and Analysis System (CIRAS). https://ciras.enisa.europa.eu/
[4] IBM Cost of a Data Breach Report 2022. https://www.ibm.com/reports/data-breach
[5] 'Healthcare provider' means any natural or legal person or any other entity legally providing healthcare on the territory of a Member State. Article 3, point (g) of Directive 2011/24/EU of the European Parliament and of the Council (OJ L 88, 4.4.2011, p. 45).
[6] Article 15 of Regulation (EU) 2022/2371 of the European Parliament and of the Council (OJ L 314, 6.12.2022, p. 26).
[7] Article 1, point (2), of Directive 2001/83/EC of the European Parliament and of the Council (OJ L 311, 28.11.2001, p. 67).
[8] Referred to in section C division 21 of NACE Rev. 2.
[9] Article 22 of Regulation (EU) 2022/123 of the European Parliament and of the Council (OJ L 20, 31.1.2022, p. 1).
[10] ENISA Cybersecurity Threat Landscape Methodology, July 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-methodology
[11] This is a result of work by ENISA in the area of situational awareness in accordance with the EU Cybersecurity Act Article 7, Paragraph 6 https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0881&from=EN
[12] Malware Information Sharing Platform estimative language. https://www.misp-project.org/taxonomies.html#_estimative_language

Group on Cybersecurity Threat Landscapes (CTL) and the NIS Cooperation Group (workstream 12 on the health sector).

Moreover, EU health organisations must notify cybersecurity incidents with a significant impact to the national authorities in their country under the NIS Directive. 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 will be presented as additional information throughout the report.

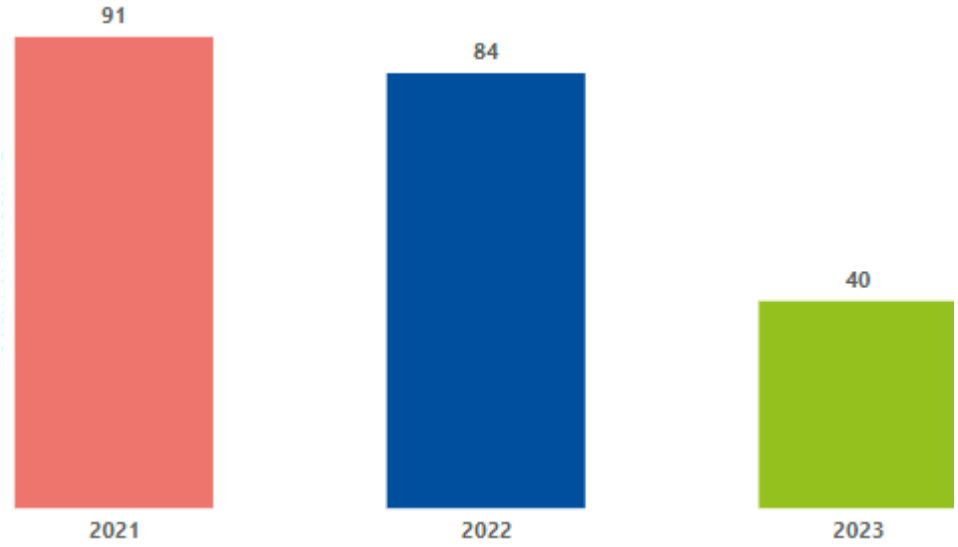
The report is structured as follows.

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

2. THREATS

From January 2021 until March 2023, we analysed a total of 215 publicly reported incidents in the EU and neighbouring countries. These include 208 cyberattacks on the health sector, 5 reports of vulnerabilities being identified but not necessarily exploited and 2 warnings of potential activity affecting the health sector.

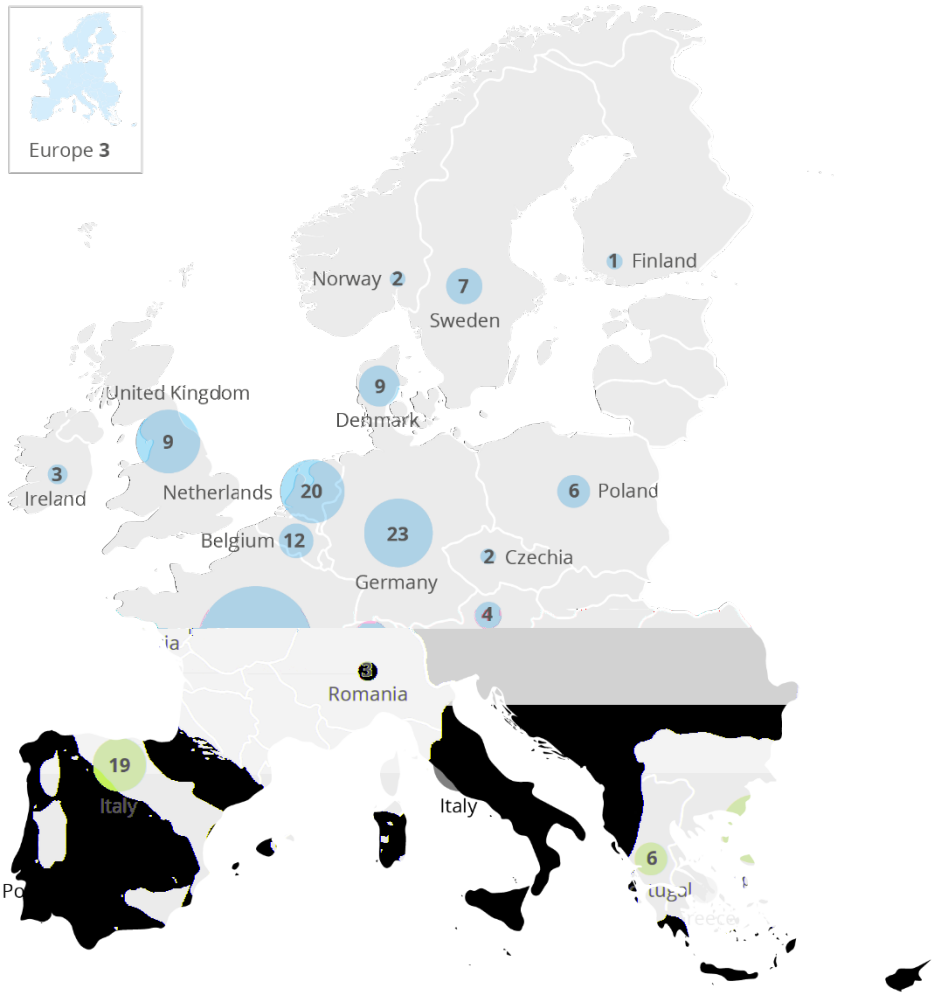
Figure 1: Incidents observed per year (2021, 2022, Q1 2023)



Overall, we observed a stable number of incidents, with a potential increase in 2023 (40 incidents in Q1, as opposed to an average of around 22 incidents per quarter seen during 2021 and 2022). In fact, denial of service (DoS) attacks targeting multiple hospitals in the Netherlands and Spain (January 2023) and in Denmark and Sweden (February 2023) account for a large portion of the activity observed during Q1 2023.

However, the number of incidents observed may be affected by several factors. An increase in the number of reported cyberattacks does not necessarily mean that the number of attacks has actually increased or that the impact of the attacks is increasing. 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 European or national law. Alternatively, the attention of the media or the public could be focused on a particular sector for a particular period of time, resulting in more incidents appearing in OSINT sources. This was particularly the case for the health sector during the Covid-19 pandemic. In this case, a cyberattack may prevent a hospital from treating patients, which may put their well-being and safety in jeopardy. Moreover, as ENISA is increasing its cyber threat intelligence capabilities, we expect more incidents to be captured in the future and thus the aforementioned observational bias to be reduced and to lead to better quality and more informative results.

Figure 2: Map of incidents observed (January 2021 to March 2023)

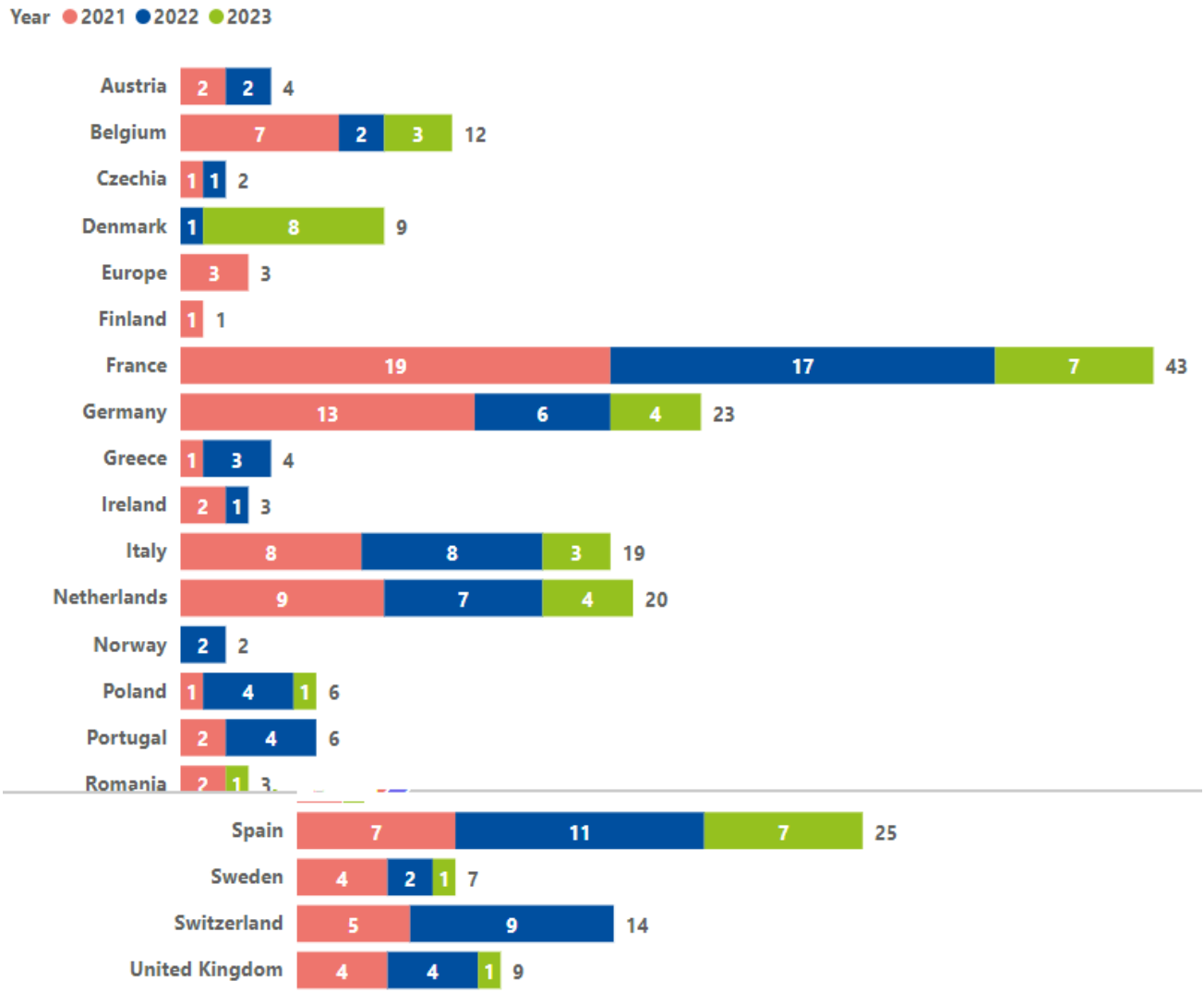


Note: the size of the circle refers to the sum of observed incidents in the country during the reporting period. Incidents labelled as 'Europe' refer to entities that have activity in Europe and not only one country.

Figure 2 shows the total incidents observed that targeted health organisations in Europe during the reporting period.

Figure 3 shows the incidents observed per country and per year. The differences in the number of incidents per country cannot be interpreted as they may be affected by the population size or by differences in reporting capabilities in specific countries or by the data collection process itself. We can observe though that there are cyber incidents which target the European health sector indiscriminately. Moreover, some countries had an increased number of incidents in 2021 and in Q1 of 2023, which are linked to Covid and to pro-Russian hacktivist activity, respectively.

Figure 3: Incidents per country and year (2021, 2022, Q1 2023)



Note: incidents labelled as 'Europe' refer to entities that have activity in Europe but not only in one country.

Figure 4: Targets (number of incidents per entity type)

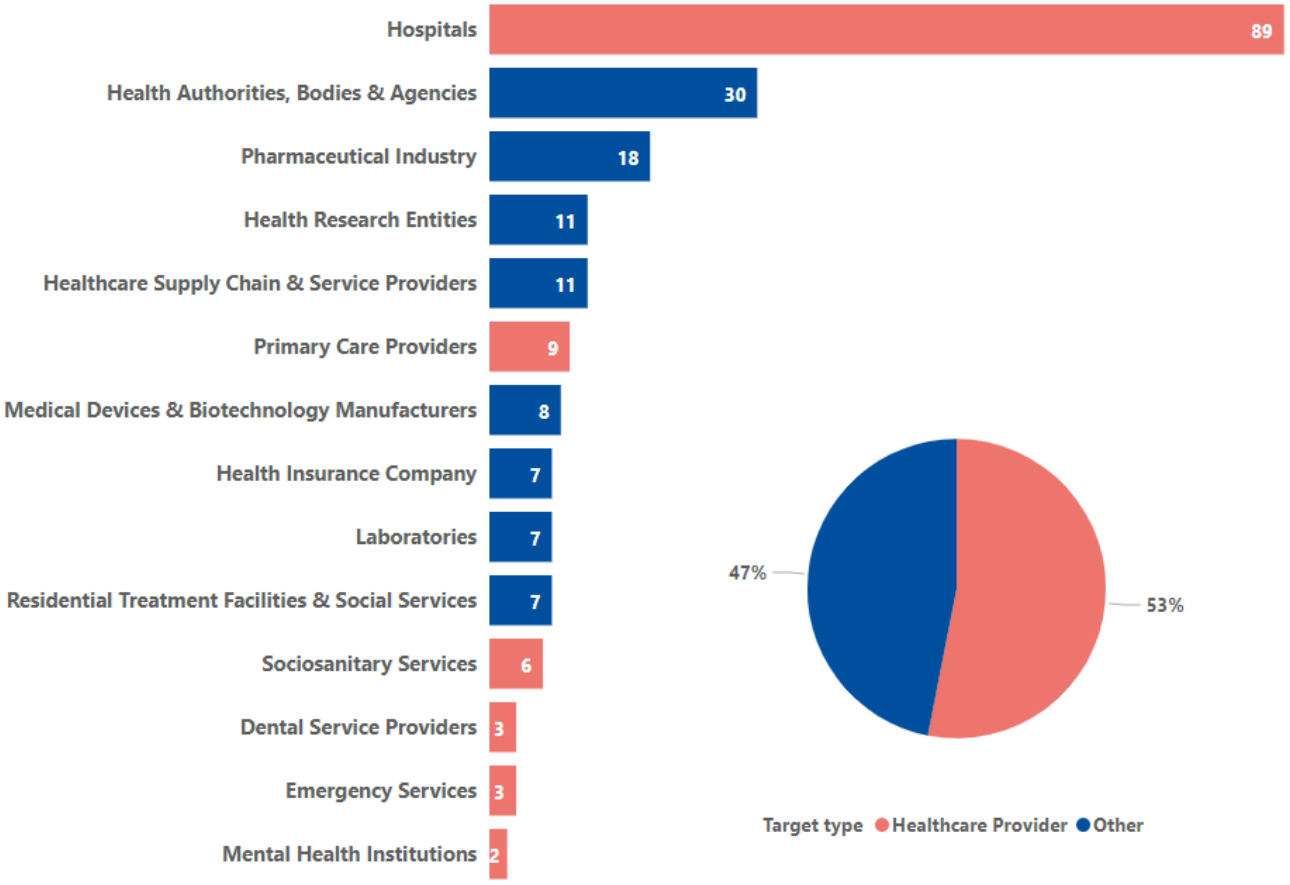
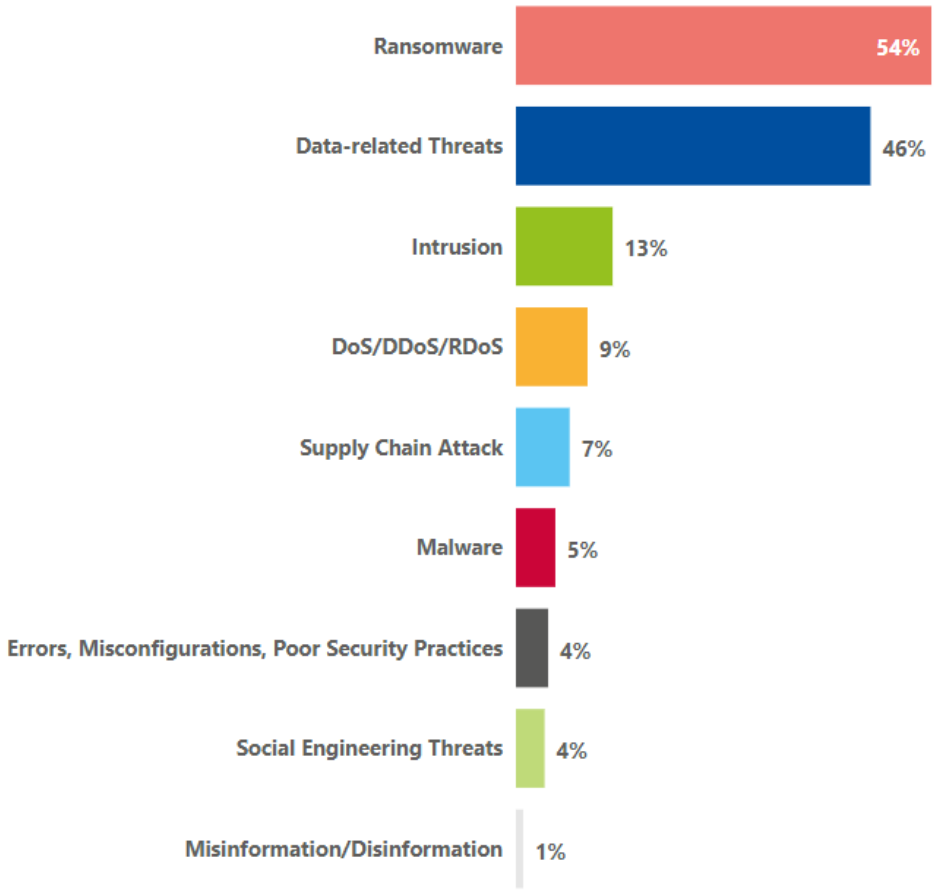


Figure 4 offers a breakdown of the types of health organisations that were targeted during the reporting period. Please note that one incident may affect multiple organisations. Overall, the majority of the incidents affected healthcare providers (53%) and especially European hospitals (42% of the total incidents). They were followed by health authorities, bodies and agencies (14%) and attacks in the pharmaceutical industry (9%).

Throughout the reporting period, we observed the following types of threats (Figure 5) targeting the European health 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 health-themed phishing campaign (*social engineering threats*), followed by a compromise with *ransomware*, which may or may not result in patient data being leaked (*data-related threats*). Likewise, incidents that included an attack on a supplier or provider were categorised both as supply-chain attacks and as the type of attack used for the compromise.

The health sector heavily relies on data that are of a personal and sensitive nature, hence their potential disclosure would have severe ramifications. This is evidently an appealing target for cyber threat actors that would take advantage of the opportunity to monetise their activities based on extortion under the threat of disclosure. This is corroborated by the findings of Figure 5 whereby ransomware and data-related threats rank the highest.

Figure 5: Threats in the health sector (January 2021 to March 2023)



In Figure 6 the differences between the threats observed are depicted on a yearly basis (2021, 2022 and Q1 2023), which allows us to make some early predictions on how the 2023 threat landscape will develop for the health sector.

The health sector has traditionally suffered from data breaches, due to the value of the data that the sector handles and also due to the maturity of the legal framework which allows data breaches to be reported more thoroughly. Throughout 2021 to 2023 data breaches are a key part of the landscape, as they are linked to, and are often the consequence of, other threats. We also need to highlight the rise of DoS (attacks against availability) in Q1 2023, since this trend was identified in the ENISA Threat Landscape 2022 report as one of the top threats with an upward trend. The analysis of incidents in 2023 validates the trend reported in ETL 2022.

Figure 6: Threats to the health sector: 2021 v 2022 v Q1 2023 (in number of incidents)

Note: An incident can be categorised into more than one threat category. Therefore, the total number of incidents per threat in this figure is greater than the sample of the study (215

2.1 RANSOMWARE

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 and confidentiality[14].

Ransomware incidents are presented separately from malware, as they are a significant portion of the identified incidents (116 incidents, 54%), with several high-profile and highly publicised incidents during the reporting period. A confirmed breach or theft of data was confirmed in 43% of these incidents. As for the remainder, we could not establish whether the data was stolen or leaked. Public statements reporting the incidents are rare and, in the few cases that are reported, the statements do not include details on how the attack happened, what ransomware attacked them, what data was possibly taken and whether ransom was demanded.

Moreover, healthcare services (32%) and other services (18%) were also disrupted. In two attacks on hospitals, our assessment is that patient care may have been affected. In the first case, the hospital had to close the emergency department and suspend surgical operations as well as rescheduling and delaying time-critical chemotherapy, while in the second case, operations were cancelled and emergencies were diverted to other hospitals. In two other instances, ransomware infected a service provider, causing service disruption in health organisations (ransomware attack on a supplier).

Trend: Ransomware attacks on the rise in 2022 and early 2023. If we compare 2021 and 2022, we see an increase in ransomware incidents. This trend has been observed in other sectors, as well as in the 2022 ENISA Threat Landscape report[15], and it continues steadily in 2023 (14 incidents in Q1).

2.2 THREATS AGAINST DATA

Sources of data are being targeted with the aim of obtaining unauthorised access and disclosure and 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 or DDoS attacks aim to deny access to data and possibly collect a payment to restore this access. Technically speaking, threats against data can mainly be classified as data breaches and data leaks. A data breach is an intentional attack carried out by a cybercriminal with the goal of gaining unauthorised access and the release of sensitive, confidential or protected data. A 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.

In this reporting period, almost half of the observed incidents (99 incidents, 46%) took the form of a threat against the data of health organisations. Data related threats continue to be one of the main threats in the sector, not only for Europe but also globally[16]. They are closely linked to ransomware and malware. Out of the incidents observed: 52 included a confirmed data loss or leak of patient data or electronic health records; 2 were cases of intellectual property theft; 16 involved other forms of data (e.g. corporate data, financial data, personnel records, credentials, etc.). In the remaining cases, it was unclear or unconfirmed what type of data were lost or leaked.

Trend: European citizens data leaked during Covid-19 pandemic. Patient data of European citizens have been leaked from government Covid-19 systems or from laboratories performing covid-19 tests on multiple occasions and in multiple countries. The data has been leaked either with the collaboration of malicious insiders or, in most cases, accidentally due to poor security practices and misconfigurations. These consist mainly of Covid-19 vaccination or test results and parts of patients' other personal information, such as social security numbers. In some cases, the data of millions of citizens were put on sale. In another case, the leaks made it possible to fake test results and get a covid pass.

[14] ENISA Threat Landscape for Ransomware Attacks, July 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks
[15] ENISA Threat Landscape for Ransomware Attacks, July 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks
ENISA Threat Landscape 2022, November 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
[16] For example, see healthcare data breach statistics in the US since October 2009, https://www.hipaajournal.com/healthcare-data-breach-statistics/

2.3 DENIAL OF SERVICE ATTACKS

Availability is the target of many threats and attacks, among which DDoS stands out. DDoS attacks target system and data availability and, though not a new threat, have a significant role in the cybersecurity threat landscape of the health sector. 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.

Trend: DDoS attacks on the rise in early 2023 due to pro-Russian hacktivism. During the reporting period, geopolitical developments and hacktivist activity increased the number of DDoS attacks against health organisations, reaching 9% of total incidents (20 incidents). The majority, 15 of these incidents, occurred in 2023. In particular, European hospitals and health authorities were targeted by pro-Russian hacktivist groups in early 2023 (Netherlands, Denmark, Sweden, Spain).

Earlier, during 2021, health authorities, bodies and agencies, and pharmacies were affected by denial of service, but these cases were linked to the Covid pandemic. The disruptions were related to services or applications for vaccination and covid testing. They were either targeted by a threat actor or suffered disruptions due to misconfigurations in combination with high demand. Also, during 2022, a national medical prescription system was disrupted as part of a more generalised attack against several governmental services.

Apart from Covid related DDoS and pro-Russian hacktivism, DDoS does not appear to have a significant impact. Impacts associated with DDoS attacks were very limited and often exaggerated by the perpetrators. In the majority of cases, they did not cause disruption of healthcare services. Limited downtime of websites was the most commonly reported impact.

2.4 MALWARE

Malware 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, spyware, adware or other code-based entities that infect a host.

During this reporting period, 5% of incidents targeting the health sector involved malware (11 incidents). Together with ransomware, they make up around 60% of the publicly reported incidents. The main impact of malware infections was the disruption to services unrelated to healthcare, such as internet or e-mail services. In most cases, the malware infected e-mail in order to send phishing e-mails to customers or patients. Malware has been disseminated using COVID-19 themes as part of social engineering campaigns. In an incident involving a pharmaceutical company, production was affected due to malware, causing delays and loss of profits.

2.5 SOCIAL ENGINEERING THREATS

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. In cybersecurity, attackers leveraging social engineering lure users into opening documents, files or emails, visiting websites or granting unauthorised persons access to systems or services. This threat canvas consists mainly of the following vectors: phishing, spear-phishing, whaling, smishing, vishing, business email compromise, fraud, impersonation or counterfeiting. During this reporting period, we only observed a limited number of incidents (~4% of the incidents).

During 2021 and early 2022, four cases of fraud, impersonation and counterfeiting were related to fake covid passes. There was another case where, after the leak of the IT configuration of a hospital by a former employee, there was a subsequent attempt by a third party to generate cryptocurrency ('mining') on the hospital's servers.

In terms of phishing, we only observed a limited number of incidents found in OSINT. These were the consequences of malware infections of mail servers, as well as one case of a trojan being distributed using a covid-19 related theme. We assess that this is an underestimation due to the lack of reliable information being reported on the initial attack vector. The ENISA threat landscape on ransomware attacks found that in 95.3% of the incidents it is not known how

threat actors obtained initial access into the target organisation[17]. This is also the case for this report as well. We observed one incident of a credential stuffing attack in 2023, but we are not sure whether phishing and credential stuffing attacks were used to gain initial access in more incidents. Initial access to healthcare organisations is being sold in the dark web and special access forums. Examples of such cases can be found in a recent report[18]. In fact, phishing amounted to 8% of the significant health-related incidents reported under the NIS directive in 2021 and 26% in 2022[19].

Business email compromise attacks were not available in OSINT reports and we did not have access to law enforcement information where they are usually reported. However, a recent study indicates that, following the transportation and automotive industries, healthcare employees were the most likely to read and reply to malicious emails, falling victim to business email compromise (BEC) attacks[20]. We assess that, despite underreporting, social engineering threats remain a significant concern for the sector, calling for increased awareness raising campaigns such as the ones ENISA undertook in May 2023[21].

2.6 SUPPLY-CHAIN ATTACKS

A supply-chain attack targets the relationship between organisations and their suppliers. For this report, we use the definition as stated in the ENISA Threat Landscape for Supply Chain Attacks[22], in which an attack is considered to have a supply-chain component when it consists of a combination of at least two attacks. For an attack to be classified as a supply-chain attack both the supplier and the customer must be targets.

In this reporting period, we observed both supply-chain attacks, as defined above, and attacks on healthcare supply chain and service providers that caused disruptions or losses to entities in the health sector (7%, 15 incidents). we found incidents where healthcare supply chain and service providers suffered ransomware attacks (2 incidents), malware (1 incident), DDoS (1 incident) or unspecified intrusion (1 incident). The majority of these incidents led to data thefts or leaks either on the supplier or on the customer side or on both (13 out of 15 incidents). We also observed three cases where the cause was either a vulnerability or poor security practices. Vulnerabilities that are deeply embedded in the digital supply chain are often extremely difficult to detect, and thousands of health applications or devices may be impacted simultaneously.

We particularly observed attacks on systems or mobile applications used for vaccination and for Covid-19 testing. In most of the cases, these incidents made it difficult for citizens to book appointments for vaccination or to receive their test results on time. In other cases, the issuing of Covid-19 vaccine passes was suspended for a period of time.

When we consider that 58% of the health organisations that participated in the 2022 ENISA NIS Investment study[23] were already using a digital health platform which runs on a specific healthcare cloud platform, it is our assessment that these types of attacks will remain highly relevant for the sector in the future.

2.7 ERRORS, MISCONFIGURATIONS AND POOR SECURITY PRACTICES

The annual incident reporting under the NIS directive indicates that out of 284 incidents with significant impact which were officially reported during 2021[24], 68% were due to system failures, 16% to human errors and 16% to malicious actions. On the contrary, the incidents collected via OSINT, which are used as the main dataset of this report, comprise of mostly malicious incidents, so they do not reflect non-intentional incidents caused by bugs or errors.

[17] ENISA Threat Landscape for Ransomware Attacks, July 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks
[18] Recorded Future, The business of Fraud: Sales of PII and PHI, by Insinkt Group, February 17, 2021, p. 10. https://go.recordedfuture.com/hubfs/reports/cta-2022-0217.pdf
[19] Data available from https://ciras.enisa.europa.eu/
[20] Abnormal Security Corp, 'Read' Alert: Data Shows 28% of BEC Attacks Opened by Employees, H1 2023 Email Threat Report. https://abnormalsecurity.com/resources/h1-2023-report-employee-open-rates
[21] Cybersecurity Healthcare Week, May 2023, https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/boostyourcybervitals
[22] ENISA Threat Landscape for Supply Chain, December 2021. https://www.enisa.europa.eu/publications/threat-landscape-for-supply-chain-attacks
[23] ENISA NIS Investments 2022, November 2022. https://www.enisa.europa.eu/publications/nis-investments-2022
[24] Data available from https://ciras.enisa.europa.eu/

Trend: Vulnerabilities in healthcare are an emerging threat. In 2021 and 2022, we observed 9 cases (4%) of confirmed and potential data thefts and leaks which were caused either by an unpatched vulnerability or due to bad configuration of systems. These were primarily applications or websites related to covid-19 vaccinations or testing, which left patient data and credentials exposed. They were systems used by the public authorities and laboratories. Similarly, a bug on a hospital website exposed the passwords and email addresses of at least 134,004 users. In 2022 a vulnerability in the system of a healthcare software vendor was exploited by an individual who stole data that contained sensitive personal and medical data of patients of healthcare providers that were using the company's systems (supply chain attack).

In 2022, software bugs were reported under NIS as the cause of 8% of system failures. These, combined with 13% of 'faulty software changes/updates', 8% of 'hardware failures', and 2% of 'faulty hardware changes/updates', amount to around 30% of the officially reported system failures. Similar trends are identified by the 2022 NIS Investment study[25], which also focuses on the EU, but is based on a different data sample. It identifies healthcare as the sector that declared the most security incidents related to vulnerabilities in software or hardware. Eighty percent (80%) of the healthcare organisations interviewed declared that more than 61% of their security incidents were caused by vulnerabilities.

The same study also indicates that 64% of healthcare organisations are already using connected medical devices in their operations. The exploitation of vulnerabilities in e-health devices is considered an emerging threat. These devices contain very sensitive information, and patient safety can depend on their reliability. Data tampering can have severe consequences, such as misdiagnosis or inappropriate treatment.

During the reporting period, some vulnerabilities came to light in this area.

- In February 2023, BD, a global medical technology company, communicated a vulnerability in Alaris™ Infusion Central that could allow an attacker to use a recoverable password after installation and have access to the database[26]. Alaris™ Infusion Central is a standalone software, separate from the pumps, that allows healthcare providers to monitor infusion data sent from BD Alaris™ Plus and BD Alaris™ neXus pumps on a computer.
- In December 2022, a vulnerability in BD BodyGuard infusion pumps was revealed, allowing access through the RS-232 (serial) port interface[27]. If exploited, threat actors with physical access and specialised equipment and knowledge could configure or disable the pump. No electronic protected health information (ePHI), protected health information (PHI) or personally identifiable information (PII) is stored in the pump.
- In November 2022, a vulnerability in KardiaMobile, a smartphone-based personal electrocardiogram (EKG) device, was announced[28]. Successful exploitation of this vulnerability could lead to attackers stealing or faking personal cardiograms or enabling a denial-of-service attack. Attackers would need to be at close range to carry out these attacks.
- In September 2022, Medtronic identified a potential issue with its insulin pump NGP 600. Under specific circumstances, the communication between the components of the pump system could be compromised[29]. The MiniMed™ 600 series pump system consists of components such as the pump, continuous glucose monitoring (CGM) transmitter, blood glucose meter and CareLink™ USB device that communicate wirelessly.
- In July 2022, a zero-day SQL injection authentication bypass vulnerability concerning Sante PACS Server was revealed[30]. This vulnerability allows remote attackers to bypass authentication on affected installations of the Sante PACS Server. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of calls to the login endpoint. When parsing the username element, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to bypass authentication on the system.

[25] ENISA NIS Investments 2022, November 2022. https://www.enisa.europa.eu/publications/nis-investments-2022
[26] https://www.bd.com/en-us/about-bd/cybersecurity/bulletin/alaris-infusion-central-recoverable-password-vulnerability
[27] https://www.cisa.gov/news-events/ics-medical-advisories/icsma-22-335-01
[28] https://www.cisa.gov/news-events/ics-medical-advisories/icsma-22-298-01
[29] https://global.medtronic.com/xg-en/product-security/security-bulletins/minimed-600-series-communication-issue.html
[30] https://www.zerodayinitiative.com/advisories/ZDI-22-955/

- In April 2022, five zero-day vulnerabilities concerning the TUG Home Base Server were found. This server is used to control and communicate with autonomous mobile robots in hospitals[31]. Successful exploitation of these vulnerabilities could cause a denial-of-service condition, allow full control of robot functions, or expose sensitive information.
- In May 2021, two vulnerabilities of critical severity were reported affecting Dräger products and another of medium severity[32]. Successful exploitation could allow a remote attacker to execute arbitrary code or cause a denial-of-service condition.
- In March 2021, six vulnerabilities were reported to GE[33]. Successful exploitation of these vulnerabilities could allow an attacker to escalate unnecessary privileges and use hard-coded credentials to take control of the device.

2.8 MISINFORMATION/DISINFORMATION

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[34]. 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. While these campaigns were related to health in terms of theme, they usually took place on social media or were phishing campaigns via e-mails attempting to steal credentials or infect victims with malware. We observed only a limited number of attacks targeting health organisations directly during the reporting period. For example, there was a low impact attack on a local health authority by 'no-vax' groups in social media.

The relevance of the health sector in disinformation campaigns emerged also from last year's ENISA-EEAS report on foreign information manipulation and interference[35]. Although the report analysed only a limited set of disinformation events, the health sector emerged as the only one to have been critically impacted, besides the media/audio-visual and governmental/administrative sectors. In early January 2021, the European Medicines Agency (EMA) revealed that some of the Pfizer/BioNTech vaccine candidate data, which were stolen in December 2020, was doctored by threat actors before being leaked online with the end goal of undermining the public's trust in COVID-19 vaccines[36].

2.9 INTRUSION

Intrusion refers to incidents where an attack on a system has been confirmed or made public and attackers have gained access to systems but the details of how the breach or intrusion took place are not clear. These types of incidents account for 13% of the total number of incidents, i.e. 27 incidents. They reflect one of the limitations of OSINT in that the information is often too incomplete to allow assessments with confidence.

[31] https://www.cisa.gov/news-events/ics-advisories/icsa-22-102-05
[32] https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-productos-drager-0
[33] https://www.incibe.es/incibe-cert/alerta-temprana/avisos-sci/multiples-vulnerabilidades-varios-productos-ge
[34] 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
[35] https://www.enisa.europa.eu/publications/foreign-information-manipulation-interference-fimi-and-cybersecurity-threat-landscape
[36] https://www.ema.europa.eu/en/news/cyberattack-ema-update-5

3. THREAT ACTORS AND MOTIVATION

As in the ENISA Threat Landscape 2021[37] and ENISA Threat Landscape 2022[38] reports, we considered four main categories of cybersecurity threat actors: cybercriminals, hackers-for-hire, state-sponsored actors and hacktivists.

- **Cybercriminals**' primary motive is financial gain, often stealing data or demanding ransom.
- **Hackers-for-hire** sell their services to people who do not have the skills or capabilities to do so. They will be included as part of the cybercrime ecosystem in this report.
- **State-sponsored** actors target organisations to compromise, steal, change or destroy information. These groups are usually affiliated with a nation state[32].
- **Hacktivists** are politically, socially or ideologically motivated and target victims for publicity or to effect change.
- In addition, for this report, we included the **insider** actor both with malicious intent and with non-malicious intent. We were able to identify a small number of cases where the actor was confirmed by authorities to be a current or former employee (**insider**). Moreover, we had a number of incidents attributed to human errors, misconfigurations and poor security practices, which we characterised as a **non-malicious insider**.

For the cases in which one of these types of actors were not identified, we categorized the incident as **unknown**. During the reporting period, we did not have information on state-sponsored activity and the hacker-for-hire actors targeting the health sector, so they are not included in Figure 7.

For analysis of the incidents, we have considered the following motivations:

- **Espionage**, when the aim of the attack is information gathering (either intellectual property or information of national importance);
- **Financial gain**, when there is a clear monetary gain underlying the attack, such as extortion, selling stolen data, etc;
- **Ideological**, when the attack is linked to hacktivist activity, and there are clear declarations about the aim of the attack by the actor;
- **Other**, when the incident was unintentional;
- **Unknown**, when we can make no clear conclusions on motivation.

The overall statistics are depicted in Figure 8. They indicate that financial gain was the primary motivation of threat actors (83%) during the reporting period regarding the relevant incidents collected. Ideological motivation was the second driver for attacks at 10%, while 6% of the incidents were unintentional. In the limited number of cases (5 incidents) where an insider was attributed as the culprit, patient records and corporate data were stolen or leaked by one or more employees and the motivation in most of these cases was considered to be financial gain. In a significant number of incidents (49 incidents), the motivations could not be determined with certainty by ENISA. 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.

[37] ENISA Threat Landscape 2021 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021
[38] ENISA Threat Landscape 2022 https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

Figure 7: Actor types

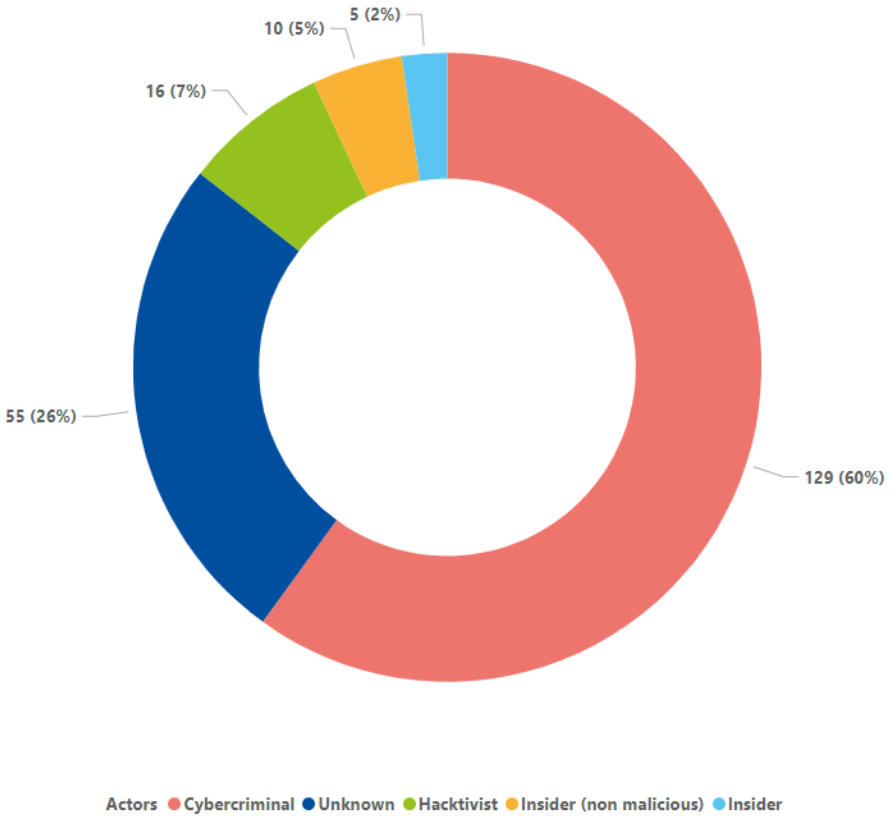


Figure 8: Motivation

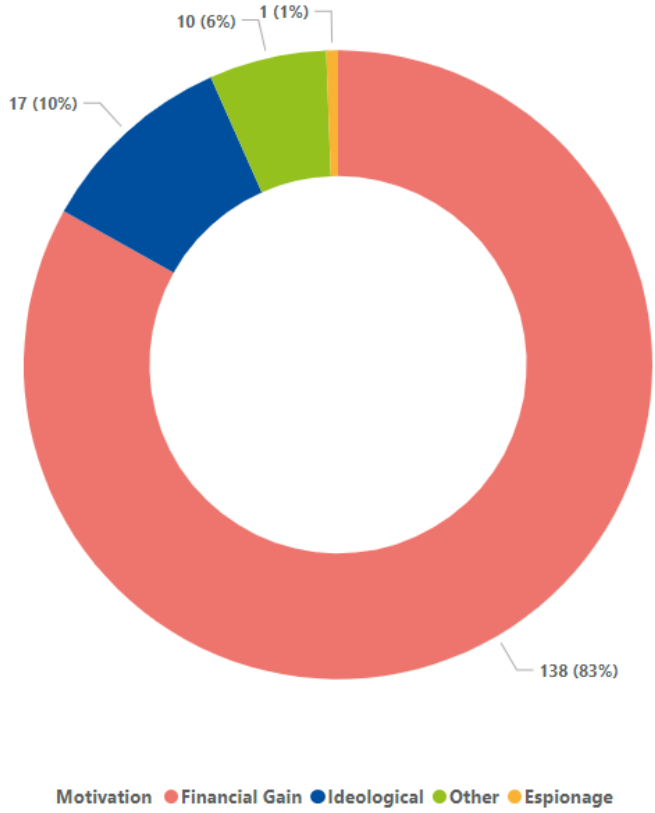
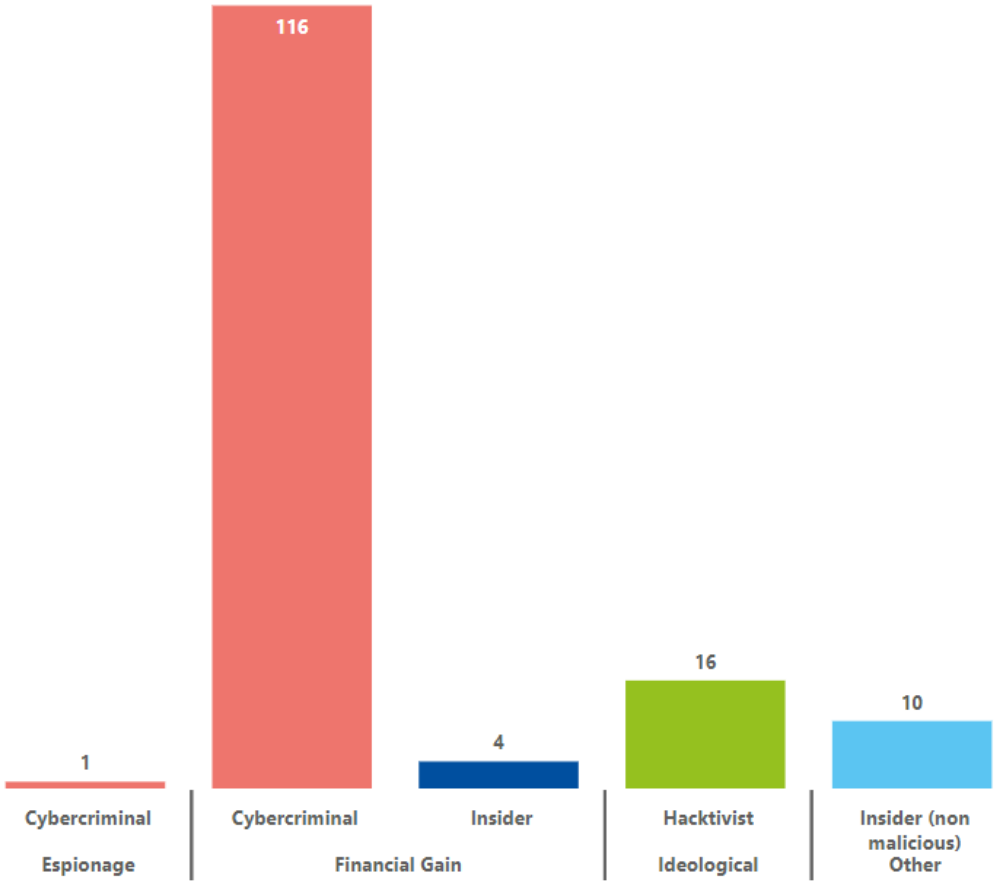


Figure 9: Motivation and actors



When analysing the most prominent actors impacting the European healthcare landscape and their motivation (see Figure 9), two primary categories of actors emerge. The first and predominant group consists of cybercriminals, particularly those involved in ransomware activities, who are primarily motivated by financial gain (53%). The second group comprises hacktivist organisations motivated by ideological reasons, aiming to carry out denial-of-service (DoS) attacks on healthcare organisations and health authorities (7%).

3.1 CYBERCRIMINALS

The primary threat actors that have been observed to target the European health sector, based on the available public information that ENISA has collected, engage in ransomware activities. The tactic of these threat actors is to blackmail their victims by demanding ransom payments. They use leak sites, typically accessed through onion links, to publicise the identities of victims and distribute data dumps. This is done as a means of threatening and pressuring the victims into complying with their demands for ransom. Samples of data are often leaked during their announcements to add credibility to their claims of an attack.

The attributions in this report were based on announcements on these leak sites, as well as the presence of actual data. However, since rebranding is very common among ransomware groups[39], in many cases the same group may appear later with a new name, or another group may use the same type of malware which makes identifying actors challenging. Rebranding may be due to mergers with other groups or a group splitting, to evade law enforcement, or for the group to start anew after a security failure[40]. The names of specific groups that are included in this section are

[39] For a map that tracks the ransomware ecosystem by Orange Cyberdefense World Watch team, see https://github.com/cert-orangecyberdefense/ransomware_map
[40] Cy-Xplorer 2023, When bits turn to blackmail: navigating the ecosystem of cyber extortion and ransomware. https://www.orangecyberdefense.com/global/white-papers/cy-xplorer-2023

mentioned not to focus on these actors specifically but to use known examples to understand the motivation of cybercriminals and of their victimology in the health sector.

Figure 10

a decryptor for free[42]. The main types of entities which were impacted by Lockbit 3.0 are hospitals (6 incidents), primary care organisations (4 incidents), and health research entities (2 incidents).

Vice Society is another ransomware gang that has been involved in high-profile attacks. It has been active since 2019. Historically, the group had been deploying variants of existing ransomware strains by leveraging compromised credentials of exploited internet-facing applications[43]. The group, however, started deploying their own locker software recently[44]. The main types of entities impacted by Vice Society were hospitals (6 incidents), medical device and biotechnology manufacturers (2 incidents) out of a total of 9 incidents during the reporting period.

BlackCat, or AlphV ransomware group, has been active since November 2021 but got more traction after REvil was dismantled following arrests in Russia at the beginning of 2022. This event provided an opportunity for BlackCat or AlphV to gain more traction and attention. Like other ransomware groups, they employ an affiliate-based business model, collaborating with other threat partners to carry out their attacks. The main types of entities that were impacted by ALPHV are pharmaceutical companies (3 incidents) out of a total of 5 incidents during the reporting period.

Other ransomware groups that have being active during the reporting period include Conti, Hive, LV, RansomEXX, RansomHouse (3 incidents each) and Wizard Spider and REvil (2 incidents each), followed by single instances of other groups.

Overall, hospitals are the most impacted type of healthcare organisations from ransomware groups (21 incidents). In smaller hospitals, ransom amounts typically vary from tens of thousands of Euros, while in larger hospitals they can escalate to several million Euros. To illustrate, during a 2022 ransomware incident at Hospital Clinic Barcelona, a ransom demand of US$4.5 million was made, although it ultimately went unpaid[45].

During January and February 2022, a survey was carried out amongst 5,600 IT professionals, which included 381 healthcare respondents, in mid-sized organisations with 100-5,000 employees across 31 countries[46]. The survey revealed that healthcare has a high ransom payment rate (61%, versus the global average of 46%), but the average ransom payment was the lowest compared to other sectors (US$197 000 versus the global average of US$812 000). However, the ransom payment is only a fraction of the total cost incurred, with other costs involving remediation and preventative actions, followed by incident handling, reputational costs, etc. In the healthcare sector, the average cost of attack remediation was the second-highest across all sectors (US$1.85 m), most likely attributable to the fact that there was a more significant gap to be filled following a cyber incident given the maturity of the sector. It is important to note that these results are global and not specific to Europe, but they highlight how financially impacted the healthcare sector is when such incidents do occur.

These insights combined indicate a difference between the ransom that was actually paid versus the often-high ransom demanded. The 2022 ENISA Threat Landscape report on ransomware attacks[47] highlights the challenge of accurately reporting on incidents and confirming payments. In 94.2% (or 588) of the cases, confirmation of payment was not possible. These figures highlight the difficulty in drawing significant statistical inferences from the limited data available.

3.2 HACKTIVISTS

During the reporting period, Distributed Denial of Service (DDoS) attacks towards healthcare, became a common method for hacktivists to express their protests or promote a cause. These attacks involve overwhelming targeted systems with a flood of traffic, rendering them inaccessible to legitimate users. Two main actors have also started targeting hospitals in early 2023: Anonymous Sudan and Killnet. Among the sectors they have targeted, European

[42] https://www.bleepingcomputer.com/news/security/ransomware-gang-apologizes-gives-sickkids-hospital-free-decryptor/
[43] https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-249a-0
[44] https://thehackernews.com/2022/12/vice-society-ransomware-attackers-adopt.html
[45] https://www.elnacional.cat/en/news/cyberattack-extortionists-45-million-barcelona-hospital-data_986421_102.html
[46] Sophos, The State of Ransomware in Healthcare 2022. https://news.sophos.com/en-us/2022/06/01/the-state-of-ransomware-in-healthcare-2022/
[47] ENISA Threat Landscape for ransomware attacks, July 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks

hospitals and health authorities in Denmark[48], the Netherlands[49], Spain[50] and Sweden[51] have been subject to their attacks.

Anonymous Sudan is a group that emerged on 18 January 2023, following the creation of a group on Telegram. Their stated objective is to carry out cyberattacks against any country perceived as being against Sudan. Within five days of its formation, the group launched attacks in response to the burning of the Holy Quran in Stockholm, Sweden's capital. These attacks persisted until March 2023. This group mainly employs Distributed Denial of Service (DDoS) attacks as their preferred method to impact or undermine the availability of their targets[52].

Initially, the group was though to act in retaliation for anti-Muslim activity that had taken place in those countries. However, a closer examination of the group suggests that there is a significant likelihood that Anonymous Sudan is actually a sub-group of the threat actor group Killnet, which has publicly expressed alignment with Anonymous Sudan, even though Anonymous Sudan has declined the claim[53] [54] [55].

Having been operational since at least January 2022, KillNet has undergone a transformation from being a DDoS-for-Hire service to a fully-fledged threat group in recent times. The group coordinates its activities through an encrypted chat group hosted on a Telegram channel. Notably, KillNet has gained recognition for its recent assaults on nations that have expressed opposition to the Russian invasion of Ukraine, with a particular focus on NATO countries[56] [57]. KillNet and affiliate hacktivist groups were targeting the US healthcare sector with DDoS attacks[58] [59] in early 2023.

Although these attacks draw attention to the incidents due to their disruptive nature and the claims that the actors make, it is crucial to acknowledge that their actual impact on critical sectors may vary, and this includes the healthcare sector. The significance of hospitals and healthcare organisations in maintaining public well-being cannot be overstated as they depend on uninterrupted operations to deliver life-saving services. The attacks primarily focus on public-facing infrastructure, such as websites or portals, causing, in most cases, inconvenience rather than directly affecting the delivery of healthcare services. However, depending on the network architecture, other services may be impacted. Moreover, the main website often provides a way for patients to gain access to health services and even if the actual healthcare application may not be affected, citizens may still struggle to reach it. Therefore, DDoS has the potential to disrupt business continuity by impeding the access of patients and healthcare personnel to crucial healthcare assets, including electronic health records, software-based medical equipment, and websites that facilitate the coordination of essential tasks.

[48] https://therecord.media/danish-hospitals-hit-by-cyberattack-from-anonymous-sudan
[49] https://nltimes.nl/2023/01/30/pro-russian-hackers-killnet-behind-groningen-hospital-cyberattack
[50] https://www.catalannews.com/society-science/item/pro-russia-hacker-group-killnet-launched-cyberattack-against-four-catalan-hospitals
[51] https://thecyberexpress.com/anonymous-sudan-cyberattacks-swedish-hospitals/
[52] https://threatmon.io/anonymous-sudan-in-depth-analysis-beyond-hacktivist-attacks/
[53] https://files.truesec.com/hubfs/Reports/Anonymous%20Sudan%20-%20Publish%201.2%20-%20a%20Truesec%20Report.pdf
[54] https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/anonymous-sudan-religious-hacktivists-or-russian-front-group/
[55] https://www.trustwave.com/en-us/resources/blogs/spiderlabs-blog/anonymous-sudan-religious-hacktivists-or-russian-front-group/
[56] https://blogs.blackberry.com/en/2023/02/killnet-hits-us-hospitals-with-ddos-attacks
[57] CISA, Russian State-Sponsored and Criminal Cyber Threats to Critical Infrastructure, Cyber Advisory, Alert Code AA22-110A, May 09, 2022. https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-110a
[58] U.S. Department of Health and Human Services, Health Sector Cybersecurity Coordination Center (HC3), HC3: Analyst Note, January 30, 2023. https://www.hhs.gov/sites/default/files/killnet-analyst-note.pdf
[59] https://www.microsoft.com/en-us/security/blog/2023/03/17/killnet-and-affiliate-hacktivist-groups-targeting-healthcare-with-ddos-attacks/

4. IMPACT

In this chapter we analyse the effect of cyber threats to the health sector in the EU during the reporting period. We first analyse which assets were affected by the incidents observed (Figure 11). The main assets of the health sector can be defined under the following broad categories.

Electronic health records and patient data include a patient's medical history and other health data that is sensitive information and crucial for treating a patient adequately, because it can provide clues for diagnosis and treatment, such as the patient's allergies or contraindications in medication.

Health information systems and services include the information systems and services that are key in patient care. They usually include registrations and appointments, tracking patient progress, laboratory services, access to pharmacy services, smart devices for healthcare, automated systems for monitoring the care of the elderly, emergency buttons, etc.

Non-medical IT systems and networks include the remainder of the IT systems that are not used for patient care, for example, the web page of the institution, administrative systems, etc.

Corporate and personnel related data is information that is not related to patient care. This information is confidential but not associated with healthcare.

Intellectual property includes information related to patents, non-functional aspects of a medical device or theories and results associated with scientific research.

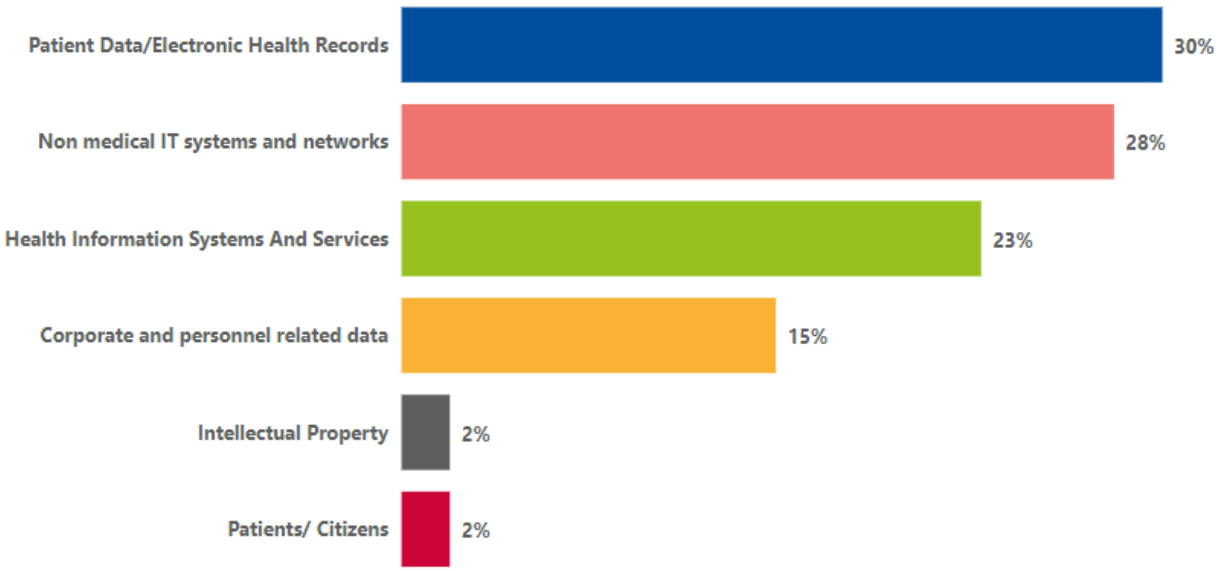
Citizens are the most valuable assets in the health sector because that sector relates to the improvement of the quality of their lives.

Patient Data including Electronic Health records were the most targeted assets in 63 identified cases (30%). Patient data are considered a commodity, as they can be used to steal a person's identity and conduct fraud[60] or for extortion and blackmail. Patient records not only include personal data (e.g. full names, social security numbers, identification information, email addresses, credit card information), but also information related to health, such as demographic information, medical histories, test or laboratory results, mental health conditions, etc. These data can then be sold on the dark web and other special access forums. A sample of such records being sold can be found in a recent study, with prices varying depending on how complete the stolen medical record is[61].

Non-medical IT systems and networks were affected in 55 incidents (26%), health information systems in 48 (23%) and corporate and personnel related data in 31 incidents (15%). Note that in several cases, more than one single asset was impaired by an incident.

[60] https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/medicare-fraud-risks/
[61] Recorded Future, The business of Fraud: Sales of PII and PHI, by Insinkt Group, February 17, 2021, p. 10. https://go.recordedfuture.com/hubfs/reports/cta-2022-0217.pdf

Figure 11: Impact (affected assets)



We analysed the impact from the perspective of the consequences. It is worth mentioning that detailed and reliable information about the impact of incidents is not readily available in OSINT reports. In the case of hospitals and healthcare institutions that have intensive healthcare operational activities, disruptions are often highly visible. In these cases, impacts can be deduced from the description of the incident, however public information does not necessarily reflect the reality. Further, the publication of leaked data by cybercriminals is unfortunately easily available and so it can be verified that it was effectively leaked. The impacts of incidents on other entities with fewer operationally visible activities are less available, and that data can have an even lower level of confidence.

The classification of the main impacts has been made according to the following broad categories.

Breach or theft of data. A data breach or the theft of data results in unauthorised access or exposure of confidential information. The information can be corporate data including invoices, lists of providers, etc. or health data such as healthcare personal data records. The breach can be intentional, such as an intrusion into a database, or accidental, such as an employee emailing confidential files to the wrong recipient.

Disruption of services not related to healthcare. The disruption of services not related to healthcare can include informative web pages, Internet access (when there is no need of this service for healthcare), billing systems or any other impact that does not affect healthcare.

Disruption of healthcare services. The disruption of healthcare services includes situations when operations must be cancelled, the admission of patients is slower and less efficient, the forced rerouting of patients to other hospitals or the use of pen and pencil to treat patients because the IT systems are not working properly.

Reputational harm. The reputational image of an organisation can be damaged when the credibility of the entity is impaired. An example can be an intrusion in the email server of the organisation and the sending of emails with an impersonation of the entity.

Patient safety. Patient safety can be put at risk in some cyber threats such as the illegitimate manipulation of medical devices or when IT services needed in an emergency situation are unavailable.

Legal and Regulatory. Legal and regulatory impacts include, for example, the liability associated with the lack of adequate cybersecurity measures in the case of a data breach.

Financial losses. Although many cyber threats can have a financial impact, financial losses in this case include only threats that caused a direct reduction of revenues or a monetary loss.

Figure 12: Impact (consequences)

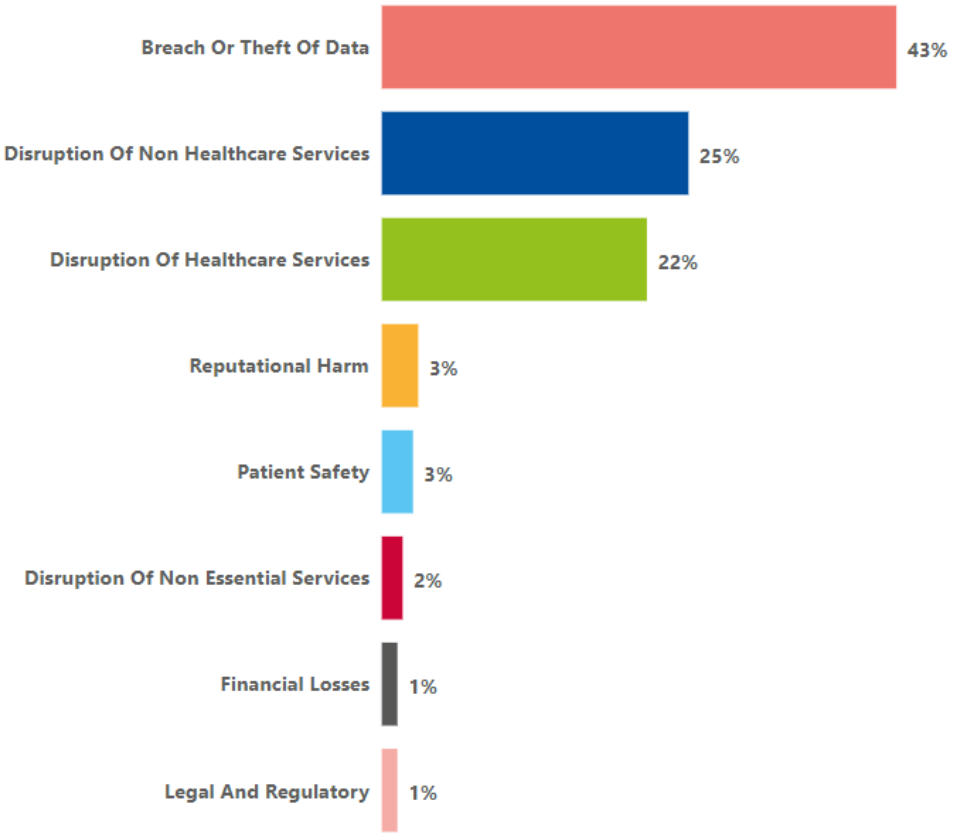


Figure 12 shows the types of consequences. Please note that one incident may be provoking multiple consequences, but information is not readily available especially for specific types of consequences. Breach or theft of data is the most common impact (43%, 99 incidents), followed by disruption of services not related to healthcare (25%, 59 incidents) and the disruption of healthcare services (22%, 51 incidents). It is more challenging to collect and assess information related to other impacts, as organisations are reluctant to make consequences known, especially those related to reputational harm or patient safety.

We cannot precisely assess the level of reputational impact. Examples of reputational harm were a medical software firm in Germany in 2021 that urged customers to reset their passwords after a ransomware attack, and the sending of phishing e-mails by the employees of the Bavarian Hospital Association (BKG) in December 2021 after the company's e-mail server was infected with malware[62].

Legal and regulatory impacts have been assessed mainly through available information regarding sanctions imposed by data protection authorities. Such consequences can occur after the incident with a delay, e.g. sanctions being imposed by the health or data protection authorities several months after the incident. This is mainly due to the time needed for investigation and for the legal processes to conclude. The Swedish Authority for Privacy Protection (IMY) issued in June 2021[63] an administrative sanction of 12 million SEK (€1 193 813) on Medhelp (Swedish Medical Consultation Service) because it came to light in 2019 that a vast number of recorded calls became available without password protection or other security protection.

[62] https://www.heise.de/news/Hackerangriff-auf-Krankenhausgesellschaft-in-Bayern-6281905.html
[63] https://edpb.europa.eu/news/national-news/2021/swedish-dpa-investigation-1177-incident-finalized_en

Financial losses are commonly the most noticeable consequence of the majority of cybersecurity incidents. The ENISA NIS Investment 2022 study indicates that the median cost of a major security incident in the health sector is 300 000 Euro.[64] However, it is rare that organisations publicly comment on the financial impact of security incidents. Sigfried, a Swiss pharma company, admitted that a pleasing financial result was achieved despite the negative impact of a cyberattack in May 2021, which affected almost all sites on the Siegfried network and led to a loss of production capacities and sales volumes[65].

A representative incident with multiple impacts could be the data breach that a Finnish psychotherapy centre suffered affecting thousands of patients. In this case, the reputational harm was high due to the repercussions of the incident affecting very sensitive information and to the fact that many patients suffered extortion[66]. They received emails with a demand in bitcoin of around €200 to prevent the contents of their discussions with therapists being made public. The Data Protection Ombudsman issued a reprimand for violating the GDPR and imposed an administrative financial sanction of €608 000 on the psychotherapy centre[67] which was declared bankrupt in February 2021. In February 2023, the police arrested a 25-year-old Finnish man as suspect for the break-in, dissemination of sensitive information and extortion[68]. In April 2023, the District Court of Helsinki sentenced the former CEO of the centre to three months in prison for a data protection crime.

When it comes to analysing the more common impacts identified (breach or theft of data, disruption of services not related to healthcare and disruption of healthcare services), we had a look at the kinds of entities that suffered these impacts and the assets that were targeted. This analysis is depicted in specific chapters in this section of this report.

4.1 BREACH OR THEFT OF DATA

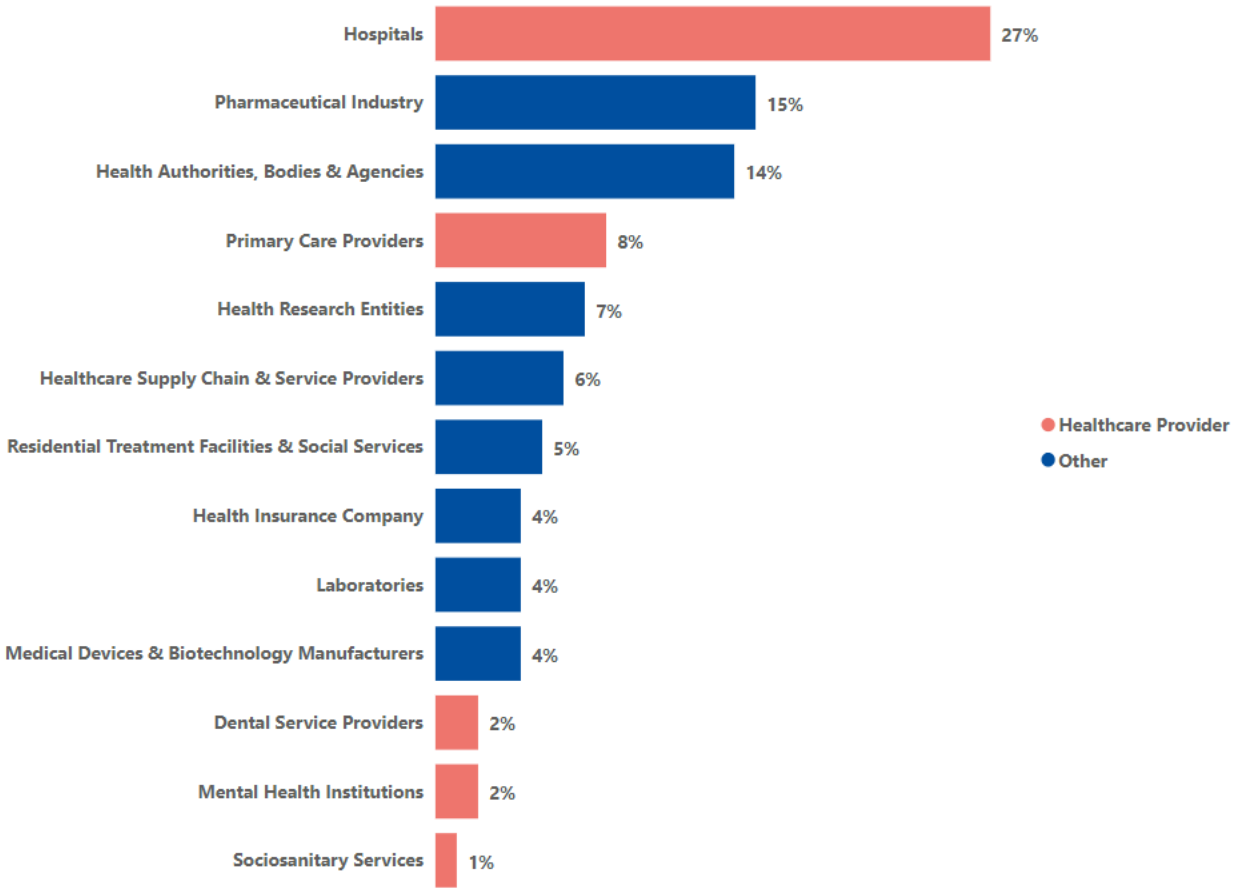
Data breaches affected healthcare entities in 40% of the cases and in particular hospitals in 27% and primary care in 8% of the incidents. They are closely followed by pharmaceutical entities at 15%, health authorities and agencies at 14%, and health research entities at 7% (see Figure 13).

Data breaches were related to data-related threats in 52% of cases, to ransomware threats in 35%, to user errors, misconfigurations and poor security measures in 5%, to intrusions in 5% and to supply chain attacks in 1% of cases.

Data breaches associated with ransomware attacks have been shown to be a common practice. The number of cases where the information was published by cybercriminals is high and the amount of data allegedly stolen spans from some gigabytes (GBs) to terabytes (TBs). For example, in the case of the Scottish Association for Mental Health in March 2022 the amount of data mentioned was 12,5GB[69], in the case of the Consorci Sanitari Integral in October 2022 it was 54GB[70], in the case of the Elsan Clinic in France in January 2023 it was 821GB[71], and in the case the E.015 TwID 66 g6

Netherlands. Because of outdated systems and insufficient access control, almost all GGD employees had access to sensitive information, which was allegedly illegally traded on the internet[75].

Figure 13: Breach or theft of data (affected entities)



During the reporting period, other incidents that caused a breach or theft of data were as follows.

- In November 2021, servers of the International Committee of the Red Cross (ICRC) hosting personal data belonging to more than 515,000 people worldwide were hacked[76]. The hackers were able to enter the network and access the systems by exploiting an unpatched critical vulnerability in an authentication module (CVE-2021-40539).
- In February 2021, a massive data breach involving the company Dedalus Biologie[77] and affecting nearly half a million people was revealed in the press. The name, first name, social security number, name of the prescribing doctor, date of the examination and, worst of all, the medical information (HIV, cancers, genetic diseases, pregnancies, drug therapy of patients or genetic data) of these people were released on the Internet. The lack of satisfactory security measures caused the leak of the medical and administrative data of almost 500 000 people. The French LSA considered that the company failed to comply with Articles 28, 29, and 32 of the GDPR and decided to impose an administrative fine of 1.5 million euros.
- In April 2022, an IT systems intrusion in the hospital Vitry-le-François et Saint-Dizier caused a data breach of essentially administrative data[78].

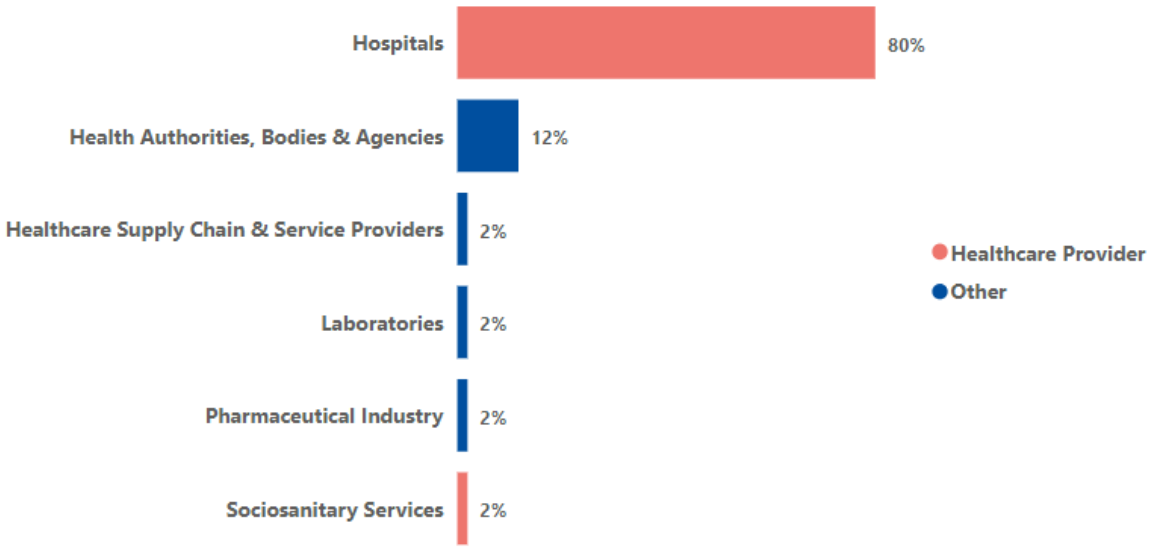
[75] https://www.computerweekly.com/news/252495983/Data-of-thousands-of-Dutch-citizens-leaked-from-government-Covid-19-systems
[76] https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know
[77] https://edpb.europa.eu/news/national-news/2022/health-data-breach-dedalus-biologie-fined-15-million-euros_en
[78] https://ght-coeurgrandest.fr/actualites/informations-cyberattaque/

- In January 2022, the Hospital Centro de Andalucía suffered a ransomware attack that included a data leak of internal documents and some patient-related files[79].

4.2 DISRUPTION OF HEALTHCARE SERVICES

We observed disruption of healthcare services when healthcare entities (82%, primarily hospitals) were attacked but also when health authorities or central government systems for healthcare were attacked (12%) (Figure 14). Healthcare services were also disrupted in cases where laboratories or pharmacies suffered an attack.

Figure 14: Disruption of healthcare services



The disruption of healthcare services was related to ransomware threats in 65% of cases, to data related threats in 20%, to intrusions in 6% and to DoS attacks in 5%.

A documented example of the impact on healthcare operational activities is the attack in February 2021 on the Dax Hospital Center (France) where the entire computer system had to stop[80]. Radiotherapy specialists analysed how they faced this threat and how important is human and technological cooperation with IT specialists to reduce this risk as much as possible but also in the event of an attack to be able to reconstruct the system as quickly as possible. Other less documented cases highlight how, due to the continuity plans of hospitals and healthcare institutions, impacts are often reduced significantly.

During the reporting period, other relevant incidents that disrupted healthcare services include the following.

- In May 2021, the HSE Health Service Executive (HSE), an organisation that provides all of Ireland's public health services through hospitals and communities across the country (with approximately 4,000 locations, 54 acute hospitals and over 70,000 devices), was subjected to a serious cyberattack through the criminal infiltration of their IT systems (PCs, servers, etc.) using Conti ransomware[81]. On 18 March 2021, the source of the cyberattack originated when a malicious software (malware) infected a HSE workstation (the Patient Zero Workstation). The malware infection happened when the user of the Patient Zero Workstation clicked and opened a malicious Microsoft Excel file that was attached to a phishing email sent to the user on 16 March 2021. The Incident had a far greater and more protracted impact on the HSE than initially expected, with recovery efforts continuing for over four months. The release of the decryption key by the attackers on

[79] https://amavecasalud.es/nota-de-prensa-ciberincidente/
[80] https://pubmed.ncbi.nlm.nih.gov/36028420/
[81] https://www.hse.ie/eng/services/publications/conti-cyber-attack-on-the-hse-full-report.pdf

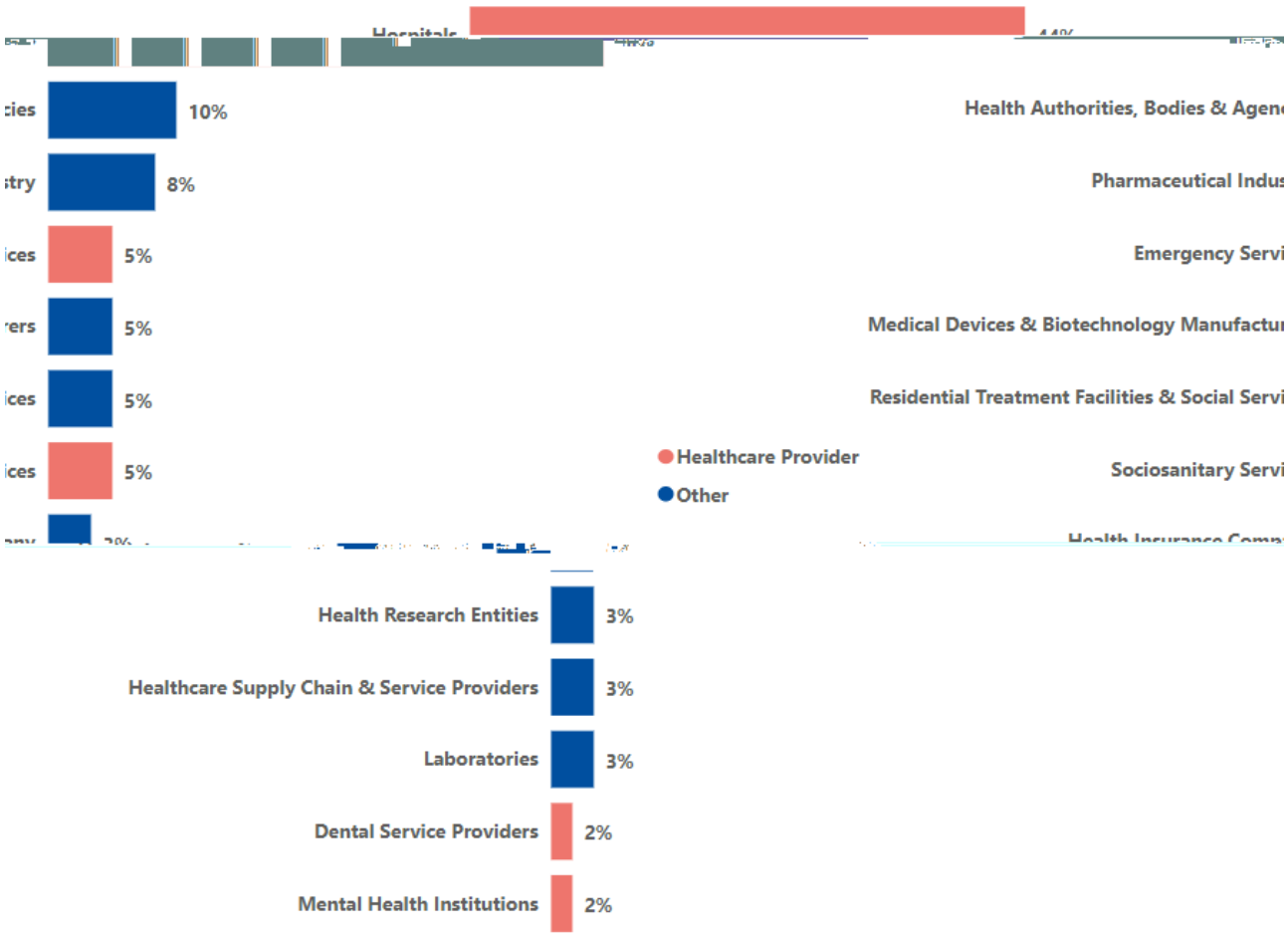
20 May 2021 allowed an accelerated recovery process and it is unclear how much data would have been unrecoverable if a decryption key had not been made available.

- In March 2023, a hospital clinic in Barcelona suffered a cyberattack that forced it to cancel 150 interventions and between 2000 and 3000 external consultations[82].

4.3 DISRUPTION OF SERVICES NOT RELATED TO HEALTHCARE

We observed disruption of services not related to healthcare primarily in healthcare entities (around 58% of the cases), health authorities and agencies (10%) and pharmaceutical entities (8%).

Figure 15: Disruption of services not related to healthcare (entities affected)



These types of disruption of services were related to ransomware threats (35%), to intrusions (22%), to DoS attacks (16%), to data related threats (14%) and to malware (10%).

During the reporting period, some relevant incidents that caused the disruption of services not related to healthcare include the following.

- In January 2022, the Health service of the Balearic Islands suffered a cyberattack that forced users with access to the system to change their passwords and restrict Internet browsing[83].
- DDoS attacks analysed during in the report had little impact, mainly affecting public information web pages and irrelevant webservices were not accessible during a short period of time. These include DDoS attacks on eight Danish hospitals in February 2023 and DDoS attacks on four Spanish hospitals in January 2023.

[82] https://govern.cat/salapremsa/notes-premsa/488382/ciberatac-al-clinic-afecta-seva-activitat-assistencial-habitual
[83] https://www.incibe.es/incibe-cert/publicaciones/bitacora-de-seguridad/sanidad-las-islas-baleares-sufre-ciberataque

- In May 2021 the Swiss pharmaceutical company Siegfried suffered an attack with malware that had an impact to its IT network[84].
- In September 2021 Olympus was subjected to an attempted malware attack affecting parts of its sales and manufacturing networks in the EMEA (Europe, Middle East and Africa). As a result data transfers were suspended in these areas[85].

4.4 PATIENT SAFETY

The selling of vaccines on the dark web in 2021 during the covid pandemic or the possibility of faking covid passports as happened in several countries during 2021 have been assessed as having potential impacts on patient safety. Incidents like the ones covered earlier as data breaches may also be considered. Being subject to extortion or having sensitive medical information leaked can cause harm to patients, especially considering that they may already be in a vulnerable mental state due to a medical condition.

Healthcare organisations are reluctant to publicly admit impacts on patient safety. However, some studies show that delays in treatment, operations cancelled or diversion to other facilities can have an impact. The study by the Ponemon Institute published in January 2023 on the impact of ransomware on patient safety shows that ransomware attacks result in a significant increase in complications from medical procedures. More than half of respondents in organisations that experienced a ransomware attack, 53 percent, say it resulted in a disruption to patient care, the most adverse event being the increase in patients transferred or diverted to another facility[86]. The study from Proofpoint and the Ponemon Institute of 2021, found that mortality rates increased at a quarter of facilities following a ransomware attack[87]. In another recent study[88], none of the ransomware attacks studied was directly linked to a case of patient harm, but staff who were interviewed deemed it a high-risk situation. Ransomware attacks were found to have a significant impact on emergency department workflow, acute patient care and the personal wellbeing of healthcare providers.

The number of deaths investigated by authorities in order to determine whether they were directly associated to a cyberattack is very limited worldwide. Historically, there have been only a few cases where the authorities have investigated cyberattacks that may have contributed to the death of a patient but, in most of these cases, the causal relationship was not established. While we did not see any incidents of this kind during the reporting period, the concern of patients and medical professionals remains as to whether the effects of cyberattacks jeopardise the proper and timely treatment of patients. Assessing this remains a puzzle, as we cannot measure accurately the impact of delayed treatment and care to a patient's health, and we rely on related estimated projections. Moreover, healthcare organisations may be reluctant to admit that healthcare was jeopardised as this would entail liabilities and sanctions.

[84] https://www.siegfried.ch/siegfried+affected+by+attack+on+its+it+systems/news-en/11760

5. CONCLUSIONS

In this report, we have performed a deep dive into the threat landscape of the health sector. While the annual ENISA threat landscapes reports include a few sectorial aspects, the documents do not analyse the context for each sector. In this report, we have tried to shed more light on the types of incidents, the actors and their motivations, the affected assets, the victims and the potential impacts on the European health sector. This can provide more valuable information for risk management to cybersecurity professionals in the sector.

Challenges for the healthcare sector. Looking ahead to the challenges the sector is facing, a main area of concern is vulnerabilities in medical devices and their potential effect on patient safety and privacy. The ENISA Foresight Cybersecurity Threats for 2030[89] includes, at the top of future threats, targeted attacks on individuals enhanced by data collected by smart devices, including health data from wearables and medical equipment.

Vulnerabilities may also be present and affect patient safety in all types of medical devices used for elderly care, home care, mental health care and disabled care, such as emergency buttons, *r*emote monitoring technologies (RMTs), i.e. smartphone applications, wearables and home-based sensors. If such devices are exploited or blocked, the safety of patients and, in some cases, the safety of healthcare professionals may be at stake. Moreover, the use of unsupported medical devices, in terms of patches, is a significant challenge for healthcare professionals who may have no options to replacing the device.

Another issue that we have witnessed during the Covid pandemic was the need to rapidly develop and deploy applications for vaccination and testing which in many cases were vulnerable and left patient data exposed. The rapid evolution of healthcare systems and medical devices, which are becoming increasingly connected to the internet, must be accompanied by putting cybersecurity measures in place. This is an area where the sector and its supply chain are lacking, as vulnerabilities have been recognised as the primary cause for incidents by health organisations.

As ransomware groups are advancing their tactics, patients whose sensitive health data have been stolen may face extortion after a data breach (triple extortion[90]). We have seen such cases in the EU[91] and in the US already[92]. The experience of extortion or having sensitive medical information leaked can cause harm to patients.

Healthcare organisations are reluctant to publicly admit impacts on patient safety. However, some studies show that delays in treatment, operations cancelled or diversion to other facilities can have an impact both on patients and also on healthcare professionals.

Key recommendations for health professionals. According to a recent study by ENISA, only 27% of organisations surveyed in the health sector have a dedicated ransomware defence programme and 40% of the organisations (OES) surveyed have no security awareness programme for non-IT staff[93]. In a recent survey by the NIS cooperation group, 95% of the health organisations surveyed face challenges when performing risk assessments, while 46% have never performed a risk analysis[94].

Health organisations should follow cyber hygiene practices such as the following.

- Offline encrypted backups of mission critical data with confidential information (data at rest) can mitigate the risks of data leaks.

[89] ENISA Foresight Cybersecurity Threats for 2030, March 2023. https://www.enisa.europa.eu/publications/enisa-foresight-cybersecurity-threats-for-2030
[90] After a ransomware operator extorts the affected organisation (double extortion – to decrypt the data and to return stolen data), the ransomware operator may also contact customers, and request ransom so as not to disclose their information.
[91] https://www.politico.eu/article/cybercriminal-extorts-finnish-therapy-patients-in-shocking-attack-ransomware-blackmail-vastaamo/
[92] https://www.scmagazine.com/analysis/ransomware/ransomware-groups-take-extortion-tactics-to-new-heights-in-attacks-against-hospitals-schools
[93] ENISA NIS Investments 2022. https://www.enisa.europa.eu/publications/nis-investments-2022
[94] Threat and risk management in the health sector, NIS Cooperation Group publication, July 2023. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group

- Awareness raising and training programmes for healthcare professionals can play a role in mitigating social engineering attacks[95] and improving security practices among users.
- Regular vulnerability scanning to identify and address vulnerabilities, especially those on internet-facing devices, should be undertaken to limit the attack surface.
- Regular patches and updates on software and operating systems to the latest available versions should be carried out.
- Good practices for authentication methods for remote access should be followed.
- Create, maintain, and exercise basic cyber incident response plans to ensure that patient care is not affected. These may include contingency plans in each department or service, improved communication channels, but also care for the healthcare professionals and their mental and physical well-being[96].
- The commitment of senior management is key, especially now that the NIS2 directive introduces liabilities for top management.

Additional resources for mitigation controls for each threat type can be found at the ENISA Threat Landscape 2022[97] report. They are based on international standards. Moreover, a recent report from the NIS cooperation group includes business continuity and mitigation recommendations for health organisations[98].

Challenges in data collection and underreporting. The information presented in this report is based on publicly disclosed incidents. It is crucial to recognise this aspect when considering the conclusions made in this report. Public disclosure of incidents can occur deliberately, such as when the victim makes a public announcement or when (healthcare) customers are directly affected by the impact of incidents. They can also be made public unintentionally, e.g. through internal communication leaks or if the victim's details (organisation name, website) are being listed on leak sites associated with threats; or even worse, when healthcare data is stolen and made available online. There are multiple reasons why incidents would not be disclosed.

In Europe, healthcare organisations must comply with various regulations and standards, such as Good Clinical Practice (GCP)[99], Medical device regulations (MDR)[100], and the General Data Protection Regulation (GDPR). Failing to comply with relevant standards can result in severe consequences, such as legal actions, penalties and license revocation. Data protection authorities (DPAs) can investigate and impose fines for non-compliance with GDPR. Since it came into effect and up to May 2023, DPAs have imposed 163 GDPR fines for a total of 16 million euros in the healthcare industry.[101] These numbers show that the industry is under heavy pressure to comply.

This industry handles very sensitive and personal information. Therefore, compliance with these regulations is crucial to protect patient privacy, maintain trust and ensure the safety and well-being of patients. Reporting incidents and their potential impact can raise concerns about failures in compliance thus potentially disclosing non-compliance. This can inhibit organisations from being transparent about incidents.

Communicating information about incidents can have a significant impact on the reputational damage of a brand. In the case of public entities that rely on government funding and taxpayer support, incidents have a rather public impact. While there may be financial implications, these are often less direct compared to private entities. On the other hand, for the private sector, incidents can have a direct impact on customer trust and brand reputation. This can have a cascading effect on investor confidence and financial performance. Private entities will weigh the financial impact after disclosure versus the risk of fines for non-compliance with reporting obligations and could choose to minimise the impact or disclosure to mitigate costs. While not desirable and potentially opening even more legal risks in the future, it is a reality we need to consider when undertaking incident analysis.

Another contributing factor to the underreporting of incidents could be the lack of detection in general. In small organisations, the level of security and privacy awareness often falls below the desired threshold. Insufficient

[95] https://www.enisa.europa.eu/topics/cybersecurity-education/awareness-campaigns/boostyourcybervitals
[96] HSE NQPSD (2022) A mixed methods analysis of the effectiveness of the patient safety risk mitigation strategies following a Healthcare ICT failure. Dublin: National Quality and Patient Safety Directorate (NQPSD) of the Chief Clinical Officers Office, Health Service Executive.
[97] ENISA Threat Landscape 2022, Annex D, November 2022. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022
[98] Threat and risk management in the health sector, NIS Cooperation Group publication, July 2023. https://digital-strategy.ec.europa.eu/en/policies/nis-cooperation-group
[99] https://www.ema.europa.eu/en/human-regulatory/research-development/compliance/good-clinical-practice
[100] https://www.ema.europa.eu/en/human-regulatory/overview/medical-devices
[101] https://www.enforcementtracker.com/?insights

knowledge within the organisation hampers the understanding of risks related to cyber incidents and the importance and requirement of reporting incidents. It may even be that the organisation lacks the necessary technical capabilities to effectively detect any ongoing incidents. Threat actors leverage sophisticated compromise techniques, making the incidents difficult to detect and allowing long periods of undetected malicious access even before data exfiltration occurs. In fact, very small organisations may not even have a rudimentary IT security organisation in place to face these threats.

ENISA
European Union Agency for Cybe

Athens Office
Agamemnonos 14, Chalandri 15

enisa.europa.eu