Cybersecurity Threat Landscape for the Healthcare Sector 2023

COMPUTER EMERGENCY
RESPONSE TEAM
FOR DUTCH HEALTHCARE

CERT

Colophon

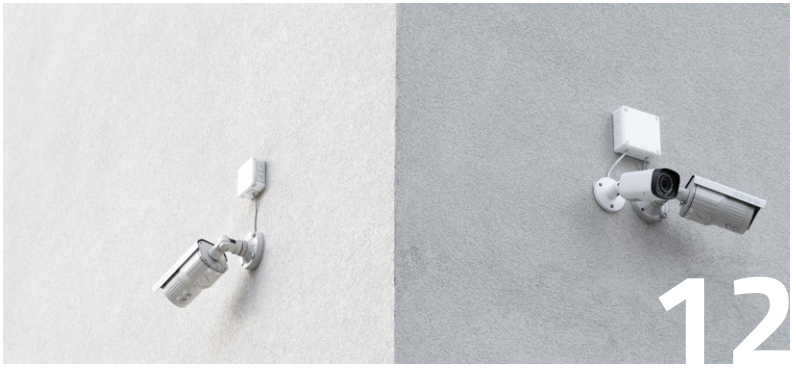
The Z-CERT Foundation is the centre of expertise in the field of cybersecurity in healthcare in the Netherlands. The annual Cybersecurity Threat Landscape for the Healthcare Sector 2023 describes the main threats for the Dutch healthcare sector. We use the information from participants' reports, information from (inter)national partners and knowledge institutes, own findings, interviews with experts, literature research, research from open sources and a survey of Dutch healthcare institutions.

Z-CERT was founded in 2017 on the initiative of the Dutch Association of Hospitals (NVZ), the Dutch Federation of University Medical Centres (NFU) and the Nederlandse GGZ. Z-CERT is a non-profit foundation.

We form a professional network with our affiliated healthcare institutions, the National Cyber Security Center (NCSC), Health-ISAC (Information Sharing and Analysis Center), industry organisations, suppliers and other Computer Emergency Response Teams (CERTs). Together, we tackle cyber challenges, such as ransomware, phishing, data breaches and hacking.

The content of this Cybersecurity Threat for Care 2023 has been compiled with great care. However, an error or incompleteness may occur unexpectedly. Z-CERT and any other parties involved cannot be held liable for this.

Contents



‘Healthcare institutions need to make robust agreements with their suppliers regarding information security’

Foreword

The year 2023 is seen by many as the year of generative AI, exemplified by language models like ChatGPT and AI image generators like Dall-E. These artificially driven chatbots offer many new possibilities for information security professionals but also for malicious actors.

Presently, the impact of AI use by cybercriminals appears insignificant. This is contrasted by the significant impact of ransomware and the extortion of healthcare organisations through leaked data. The ransomware threat in healthcare remains high, alongside fears of extortion through data breaches. Suppliers of healthcare institutions also face heightened risks of becoming victims of incidents involving ransomware and/or extortion with data breaches.

Data published on data breach websites indicates that IT service providers in Europe experience ransomware attacks or data breaches with extortion more often than healthcare providers themselves. However, such incidents at suppliers can significantly impact healthcare institutions as well.

Therefore, healthcare institutions need to make robust agreements with their suppliers regarding information security. The European NIS2 legislation is imposing stricter obligations on suppliers towards healthcare providers.

Keeping sharp

Fortunately, more and more organisations in healthcare (and elsewhere) are adopting multifactor authentication (MFA) for system logins. This is an essential tool in the fight against cyberattacks. Unfortunately, cybercriminals are creative and continually find ways to bypass such MFA barriers. With this annual Threat Landscape for healthcare and our other activities, we at Z-CERT continue to keep the sector sharp by warning about existing and new threats.

One of those relatively new threats comes from the realm of domotics. In the 2022 annual Cybersecurity Threat Landscape for healthcare, we noted that the increased use of domotics in healthcare brings serious security risks. The deployment of healthcare domotics can directly impact care provision because it involves devices such as fall detectors for the elderly, smoke detectors, and cameras. Last year, we also witnessed several incidents involving domotics, such as alarm buttons malfunctioning, requiring staff to conduct additional rounds.

Another concern is the difference in maturity levels among different healthcare institutions. The Health and Youth Care Inspectorate (IGJ) noted in November 2023 that hospitals have made significant progress regarding information security. However, the healthcare sector is much broader than just hospitals. More and more umbrella organisations are joining Z-CERT, such as Vereniging Gehandicaptenzorg Nederland (VGN) and the elderly care organisation ActiZ. We anticipate a growing focus and allocation of budget towards information security in a rising number of Dutch healthcare institutions. Let's hope that this prediction comes true in 2024.

I wish you much reading pleasure and a digitally secure year ahead.

Wim Hafkamp
Director of Z-CERT Foundation

Summary

Ransomware and data breaches pose a serious threat to healthcare. This is mainly due to new phishing techniques used by criminals and attackers becoming faster at exploiting vulnerabilities.

Ransomware

The number of ransomware incidents in healthcare increased significantly worldwide in 2023. Nevertheless, this trend has yet to be observed in the Netherlands and Europe. Due to new phishing techniques used by criminals and attackers becoming faster at exploiting vulnerabilities, Z-CERT expects the threat to the healthcare sector in the Netherlands to rise.

Not only do large organisations fall victim to ransomware attacks, but small organisations with 50-200 employees are also often targeted. For 2024, Z-CERT predicts numerous ransomware attempts and several major incidents.

Z-CERT observes that suppliers are more frequently affected than health-care institutions. Working with suppliers and the transition to cloud-based services can introduce new risks that need to be considered. The growing digital dependency justifies a greater focus on suppliers. In 2023, 9 per cent of respondents reported ransomware incidents involving suppliers.

Data breaches and DDoS attacks

Data breaches can also have a significant impact on healthcare. These breaches can result from hacking attempts, credential phishing attempts, lack of multifactor authentication, malware, misconfigurations, and careless equipment handling.

Furthermore, Z-CERT notes a more significant threat of DDoS attacks by politically motivated hacktivists. In 2023, fifteen Dutch hospitals were affected by DDoS attacks, mainly due to geopolitical issues such as the war in Ukraine. Hacktivists actively target Dutch hosting providers, which has implications for the healthcare sector.

Cyber espionage and CEO fraud

In 2024, the threat of cyber espionage by state actors persists for healthcare institutions involved in pertinent scientific research or holding personally identifiable information of interest to such actors. Over the past year, state actors have succeeded in gaining access to organisations through the supply chain.

A much more common phenomenon is digital financial fraud, such as CEO fraud, fraudulent invoices, and fraudulent online store orders. We expect that criminals will make many attempts to commit financial fraud in 2024.

Developments in AI

Efforts to commit financial fraud can be enhanced through generative AI, primarily known by so-called 'large language models' (such as ChatGPT). The use of AI in carrying out cyberattacks is expected to increase. The deployment of AI may also lead to more difficult-to-detect phishing attacks or the use of advanced fake audio and video in the near future.

As attacks rise on multiple fronts and new techniques emerge, they present unique challenges. It's crucial to uphold robust cyber hygiene practices and bolster measures to stay ahead of threats.

explanation

Threat Radar

The threat radar indicates the timing, impact, and severity of cyber threats in healthcare. The position of the various dots in the inner ring, middle ring, or outer ring indicates when something will pose a threat.

The chart is divided into three sections that indicate the weighting of the threat. In the right section, the most severe threats are listed. The farther to the left the dots are, the lower the threat they pose.

Finally, the colour of the dots indicates a threat's expected impact. The darker the colour, the greater the expected impact.

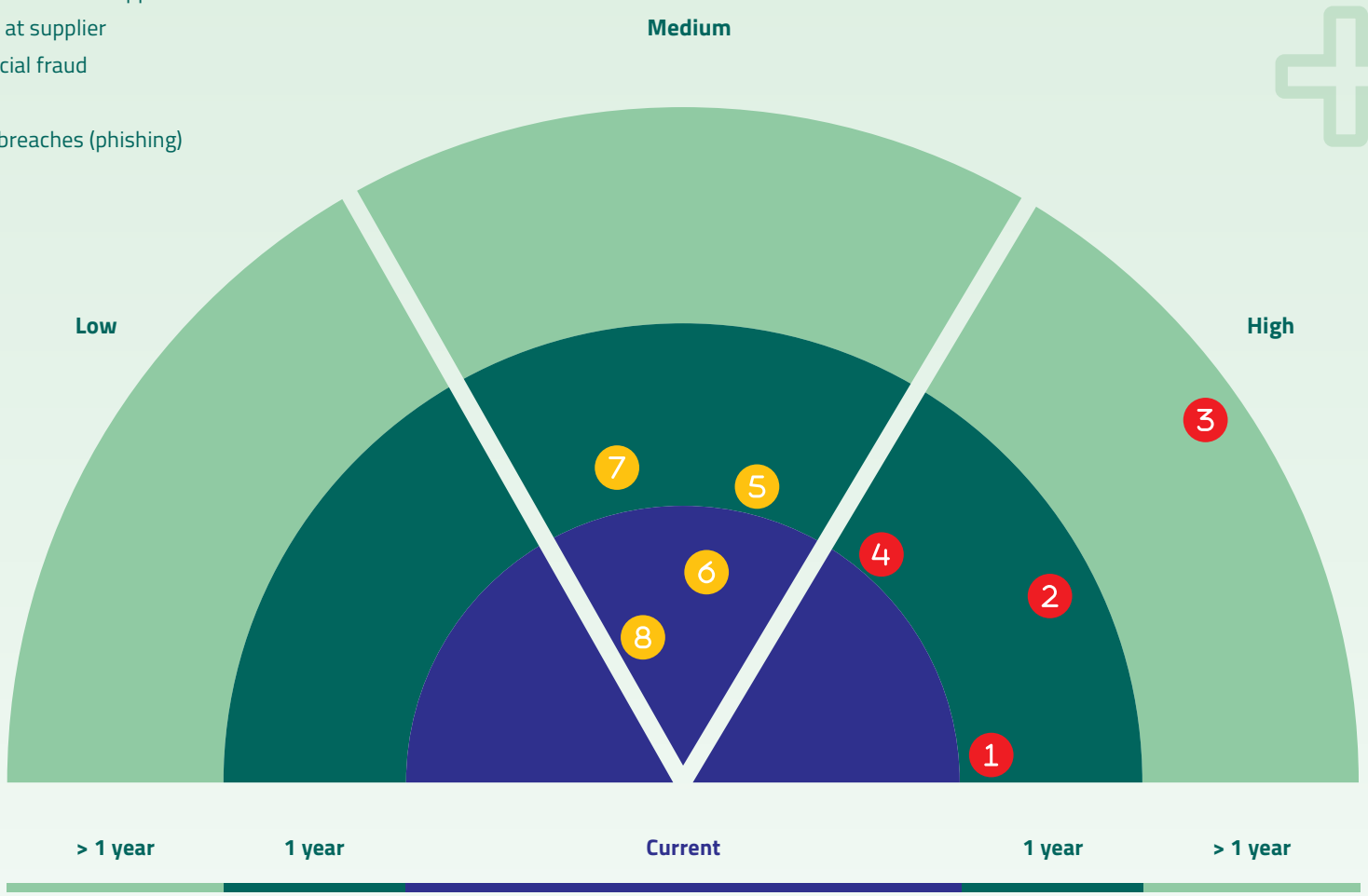
A detailed explanation of the threat radar is provided in Appendix 1 on page 36.

'The threat radar indicates the timing, impact, and severity of cyber threats in healthcare'

Threat Radar

Legend

① Ransomware
② Data breaches (hacking)
③ Espionage
④ Ransomware at supplier
⑤ DDoS at supplier
⑥ Financial fraud
⑦ DDoS
⑧ Data breaches (phishing)



explanation

Incidents among respondents

For the threat landscape, Z-CERT inquired with participants about the security incidents they experienced. Nearly a quarter of the participants completed the survey. The results are displayed in a graph alongside this text. This information can aid in increasing awareness within your organisation and determining priority measures. The incidents will be discussed in greater detail in the sections dedicated to 'threats' and have been utilised, along with other factors, to assess threat levels.

Clarification

The percentage indicates how many per cent of the total respondents had 1 or more incidents in this category. Under 'data breaches - cyber-related', we refer to data breaches that occurred due to malware, credential phishing, or hacking. The financial fraud category in the graph pertains to financial fraud committed using digital media such as e-mail and WhatsApp.

'This information can aid in determining priority measures'

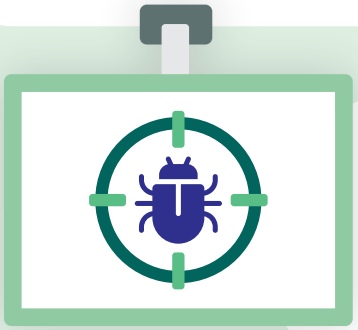
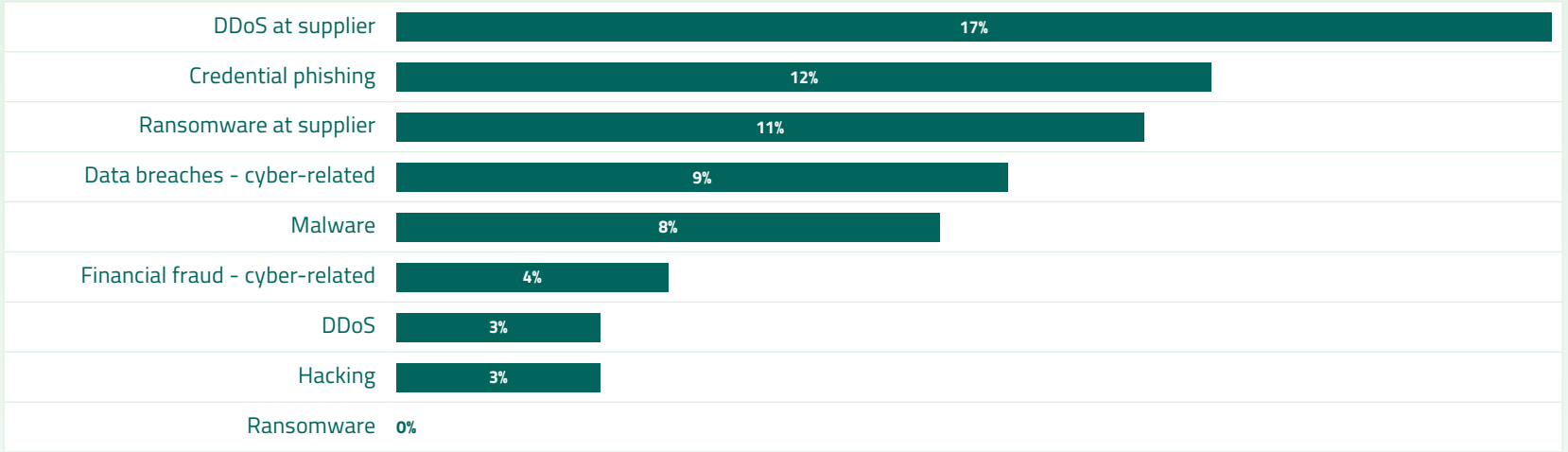


Figure 1

Security incidents that occurred among Z-CERT participants who completed the questionnaire



threat

Ransomware

Threat assessment: high

Z-CERT assesses the threat level for ransomware and/or extortion with data breaches as 'high'. We estimate the threat is slightly higher than last year because the ransomware sector has become more effective and more prominent. Additionally, the healthcare sector is more vulnerable due to actors applying new phishing techniques and exploiting vulnerabilities more quickly.

Prediction for 2024

In 2024, Z-CERT foresees numerous ransomware actors attempting to breach Dutch healthcare institutions. Z-CERT anticipates several ransomware incidents within the Dutch healthcare sector over the next year, each expected to have a significant impact.

Global increase in ransomware incidents in healthcare

In 2023, Z-CERT recorded a worldwide increase of 73 per cent in incidents published on data breach websites compared to 2022. Figure 2 depicts the same growth of incidents among healthcare providers worldwide. Compared to 2022, the total growth was 115 per cent.

This increase is partly due to organisations being much less willing to pay the ransom, resulting in more data being leaked on data breach websites than before [1]. Additionally, developments within the ransomware ecosystem play a role. For example, Microsoft recorded a 12 per cent increase in criminal hackers in ransomware-as-a-service groups and, therefore, expects an increase in incidents in 2024 [2]. Additionally, there was the emergence of new, often prolific groups. Another contributing factor was the established ransomware group Cl0p, which caused numerous incidents by exploiting zero-day[1] vulnerabilities [3]. There are also groups that increasingly resort to extorting organisations solely by leaking data without deploying ransomware. This saves time, enabling them to drive more incidents. This type of hacker is interested in selecting organisations whose data is particularly sensitive, such as healthcare institutions. An example of such a group is Karakurt [4].

The Netherlands and Europe

Measured across all sectors, Z-CERT observed more incidents on data breach websites in Europe and the Netherlands in 2023 than in 2022. Among healthcare providers in Europe, Z-CERT recorded 29 incidents, slightly fewer than last year, impacting 101 locations. Among Dutch healthcare providers, Z-CERT recorded three ransomware incidents in 2023, two fewer than in 2022.

[1] A zero-day vulnerability is a vulnerability for which no patch is currently available.

12

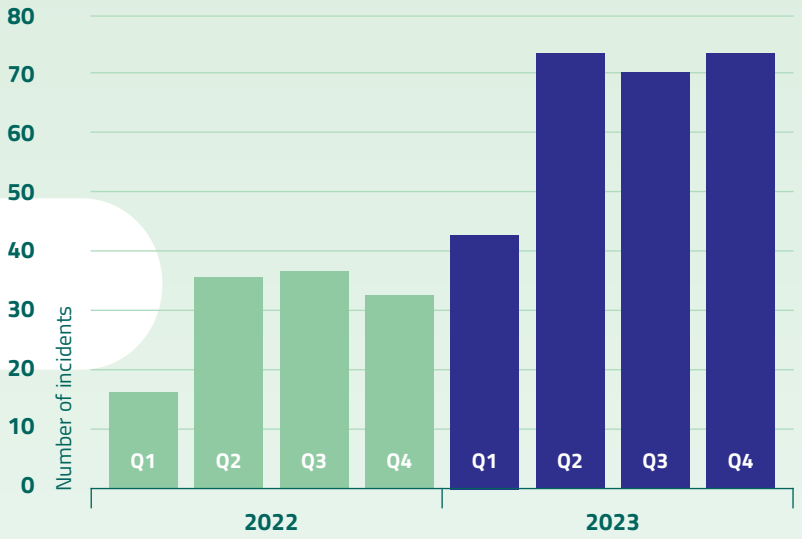


Figure 2

Incidents at healthcare providers worldwide that are published on data breach websites by cybercriminals

The decrease in Europe and the Netherlands is not all good news. As mentioned earlier, Z-CERT recorded a global increase in ransomware incidents. These figures are based on larger datasets than the dataset of incidents in Europe and the Netherlands.

Fact versus fiction: is organisation size relevant?

Within Dutch healthcare organisations, there is sometimes a misconception that ransomware actors primarily target large, wealthy organisations. Figure 3 shows that even organisations with fewer than 200 employees have often been victims of ransomware attacks throughout the past year. Small healthcare organisations, such as GP practices, were also affected.

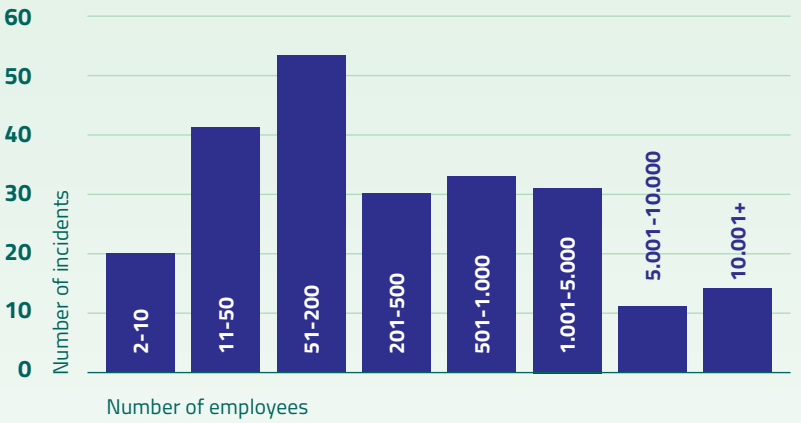


Figure 3

Incidents in 2023 publicly disclosed on data breach websites per healthcare provider size category

Impact

Several examples of the impact of incidents on European healthcare providers were:

- Domotics solutions (e.g., alarm buttons) malfunctioned, requiring staff to make additional rounds.
- Healthcare organisations were resorting to pen and paper for patient registration [5].
- Urgent and/or non-urgent appointments had to be cancelled [6].
- Ambulances had to divert to other hospitals nearby [5].
- Emergency care had to be suspended [7].
- Research increasingly suggests a link between ransomware attacks and an increase in mortality rates within hospital settings [8].
- Of the affected healthcare providers appearing on data breach websites, 45 per cent ultimately had their stolen data leaked.

Trends in techniques and methods

Cybercriminals continue to employ the same methods to gain access as they did a year earlier. In short, a cybercriminal gains entry to an external system through an employee's account, potentially by exploiting weak, easily guessable passwords or purchasing stolen credentials from another cybercriminal. A user launches malware obtained via e-mail or through a link. Alternatively, criminals exploit a vulnerability in an internet-exposed system.

We extensively addressed this issue in previous threat assessments, and the mentioned mitigating measures are still relevant. This year, we want to focus on some specific observations that have stood out and which healthcare institutions can anticipate:

- The rise of phishing attacks that bypass MFA (see data breaches chapter). This enables attackers to access email accounts for spreading malware or stealing data.
- Attackers are becoming faster at exploiting discovered vulnerabilities [9]. A recent study indicates that 1 in 5 vulnerabilities are exploited within 48 hours of a patch release [10]. This year, Z-CERT issued 16 urgent security advisories regarding frequently exploited vulnerabilities. In 2023, the total number of disclosed vulnerabilities subsequently classified as critical increased by just over 3 per cent [11].
- This year saw frequent occurrences of large-scale data theft from online file transfer systems such as MOVEit Transfer, as criminals took advantage of zero-day vulnerabilities. This resulted in dozens of incidents at healthcare institutions and their suppliers worldwide [12].
- We witnessed numerous attacks on VPN solutions. Malevolent actors attempted to guess passwords or use old passwords leaked in data breaches. These attacks often succeed because nearly 50 per cent of VPN accounts lack multifactor authentication [2].
- Malware is being distributed on a large scale (see data breaches chapter).

Key Takeaways from 2023

There is ample information available on preventing and dealing with a ransomware attack; refer to the section titled 'Ransomware response' for more details.

During (attempted) ransomware attacks, European healthcare institutions learned several lessons that we would like to share in this threat landscape:

- **Domotics and the cloud** Ensure there is a backup internet connection for domotics solutions requiring cloud communication, reducing reliance solely on the local network.
- **On-premises domotics** Isolate locally hosted domotics solutions on a separate network segment and avoid reliance on network services in other segments. Ensure that traffic to and from this network segment is configured with 'least-privilege' access and periodically review firewall rules.
- **VPN security** Strengthen password policies and account management for VPN solutions. Refer to, for example, CIS Critical Controls 4 and 5 (version 8). This is in response to the numerous attacks on VPN solutions.
- **Emergency patching** Ensure all internet-connected systems can be patched promptly when necessary. As discussed in the next chapter, it is advisable to make agreements with your supplier regarding this matter. Following patching, verify whether the system had been compromised beforehand.
- **Limited storage of sensitive data** Limit storage of sensitive data on systems connected to the internet and set a retention period after which files are automatically deleted.

This is in response to ransomware actors exploiting several zero-day vulnerabilities in online file transfer environments.

- **Measures against phishing attacks where MFA is circumvented** Refer to the 'data breaches' chapter for mitigations.

Ransomware response

- **CIS Critical Controls** Consider using the CIS Critical Controls framework for selecting and prioritising security measures [13]. Refer to the article 'Praktijkverhaal: CIS Controls framework kan helpen om hackers buiten de deur te houden' for more information, including its relationship with NEN7510 [14].
- **Security baselines** Utilise configuration standards for software and cloud services, such as 'CIS benchmarks' or Microsoft security baselines. This helps prevent overlooking critical configuration options. Z-CERT estimates that substantial improvements can be made with minimal effort and expertise in this regard.
- **NCSC incident response plan for ransomwaree** Refer to the NCSC incident response plan for detailed preparation for ransomware attacks [15].
- **CISA ransomware analyses** Read CISA papers on analyses of ransomware actors and countermeasures. Some relevant papers for the healthcare sector include the paper on the Lockbit actor [16] and Rhysida [17].

threat

Ransomware at suppliers

Threat assessment: high

Z-CERT assesses the threat level for incidents involving ransomware and/or extortion with data breaches at suppliers of healthcare institutions as 'high.' This threat level is based on the reasons discussed earlier in the threat assessment for healthcare providers, as mentioned in the previous chapter.

Furthermore, Z-CERT has observed that IT service providers in Europe are more frequently affected by such incidents than the healthcare providers themselves. This could impact healthcare institutions if they procure services from these suppliers.

Prediction for 2024

In the upcoming year, Z-CERT expects several ransomware incidents to occur at suppliers, impacting Dutch healthcare institutions.

Why the focus on suppliers?

Healthcare is undergoing a digital transformation with a growing reliance on digital service providers. Healthcare institutions are responsible for protecting personal data and for monitoring, assessing, and auditing external suppliers. Therefore, engaging in discussions with suppliers about their resilience to ransomware attacks is essential.

For risk assessments, it is crucial to consider both providers of digital services and suppliers of essential physical products. Incidents involving suppliers can cause problems if deliveries of essential items such as medications or devices are disrupted.

Incident trends

Incidents were also recorded on data breach websites among suppliers of healthcare institutions. Among producers of medical technology, there was a global increase of 63 per cent, while in the pharmaceutical industry, the increase was 75 per cent (see Figure 4). Another sector crucial to the healthcare industry is the IT sector. Incidents in this sector increased globally by 117 per cent.

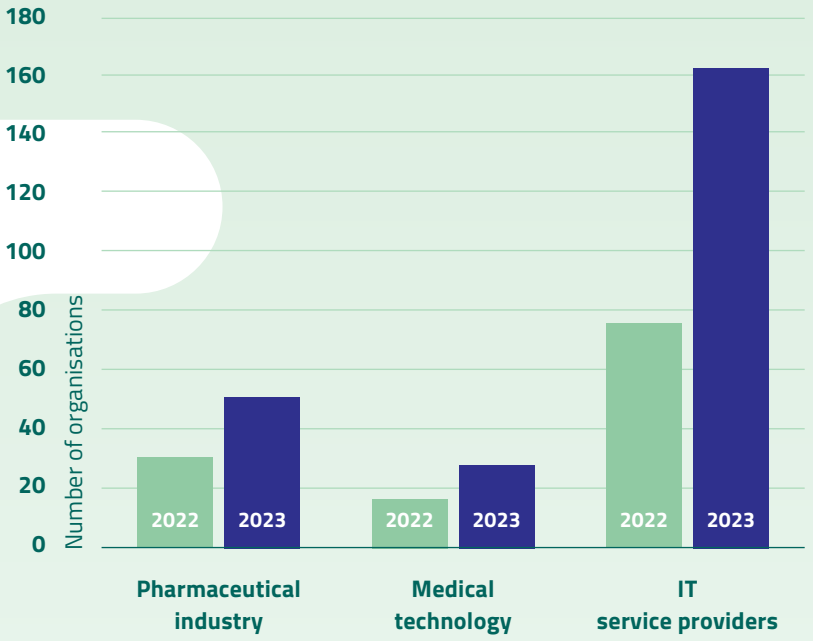


Figure 4

Quantity of incidents in 2022 and 2023

From the questionnaire filled out by Z-CERT participants, it appears that in 2023, 9 per cent of the respondents had a supplier affected by ransomware. In two instances, there were multiple ransomware incidents. Data were leaked in these cases; for example, a healthcare institution could temporarily not use a financial system, causing a partial shutdown of the finance department.

It was also necessary to verify the reliability of the data. In certain instances, proactive measures were taken to close the VPN connection with suppliers of medical systems and building management systems. While the impact may seem small, it takes substantial time to perform the action and verify that there have been no malicious activities.

In 2023, several notable incidents in the Netherlands and Europe exposed the risks of supplier dependency. For instance, there was a ransomware incident involving a supplier of alarm buttons [18]. The communication between the buttons and the control room was no longer operational. Numerous healthcare institutions in the Netherlands depend on these solutions. As a result of the malfunctioning buttons, personnel from an organisation had to implement additional measures to guarantee the safety of a client.

“Several notable incidents in 2023 highlight the risks of dependency on suppliers”

A cyber incident occurred at a supplier in Sweden, causing two ambulance services in the United Kingdom to lose access to their electronic patient records. Although ransomware was not formally named as the cause, ambulance personnel had to rely on pen and paper to transfer a patient to the hospital as a result [19].

Trends in methods and techniques
The risk of incidents due to the absence of MFA on a supplier's account or suboptimal implementation of privileged access management and network segmentation remains relevant. What stood out in 2023 among healthcare institutions in Europe is that there were incidents caused by suppliers being late in updating the on-premise systems of healthcare providers.

This delay presented an opportunity for malicious actors to establish backdoors in systems. Occasionally, these backdoors remained inactive for an initial period. This is because the malicious actor who installed the backdoor may not utilise it personally but instead sell it to others. Subsequently, the individual purchasing the backdoor can use the acquired access for data theft or ransomware distribution. This sales process may take some time.

Response strategy
Refer also to the response strategy in the chapter 'Ransomware at Healthcare Institutions.' The recommendations mentioned are also applicable to suppliers.

During ransomware attacks or attempted ones at suppliers or on systems managed by suppliers in healthcare institutions, healthcare organisations have learned several lessons that we would like to share in this threat analysis:

- **Supplier oversight** Ensure that suppliers are up-to-date with patching your systems, for instance, based on threat intelligence provided by Z-CERT. Hold them accountable for patching agreements outlined in a Service Level Agreement (SLA). Z-CERT observes that this often goes awry.
- **Agreements with suppliers and incident response** Clearly define which supplier is responsible for incident response tasks for systems. This prevents disputes during an incident.
- **Ask a supplier questions** For example, what does your supplier do to mitigate phishing methods where MFA is circumvented? Is your supplier aware that the speed at which vulnerabilities are exploited has increased?
- **Require multifactor authentication** for supplier accounts that provide access to your systems and only grant access to your network through a privileged access management solution.
- **Pen testing and red teaming** Does your supplier regularly conduct penetration tests and red teaming tests? These exercises specifically challenge the 'paper reality.' For these tests, your supplier can use the documents provided by CISA [16] [17] as input. Also, refer to the NEN7510 management control A.15.2.1 for ransomware at suppliers.

threat

Data breaches (non-ransomware)

Threat assessment: medium to high

Z-CERT assesses the threat level for data breaches (non-ransomware) within healthcare as 'medium' to 'high.' This indicates the expectation of incidents involving data breaches in the near term.

There are various ways in which data breaches occur. This section of the threat landscape focuses on data breaches resulting from cyber incidents such as credential phishing, malware, and hacking. Data breaches caused by erroneous e-mails and loss of data storage devices are not included in this threat landscape. Data breaches resulting from extortion were discussed in the previous chapter.

Z-CERT assesses the threat level for data breaches caused by hacking as 'high'. Z-CERT anticipates several data breaches caused by hacking within a year. In these cases, the impact will be higher than, for example, in a phishing incident because more sensitive data are compromised. Z-CERT assesses the threat level for data breaches caused by credential phishing and malware as 'medium'. Additionally, we would like to draw attention to the risk of data leakage due to misconfigurations and improper decommissioning of (medical) equipment.

> **"Z-CERT anticipates several data breaches caused by hacking within a year"**

Incidents

At Z-CERT, several credential phishing attempts and malware phishing emails bypassing spam filters are reported weekly. In the survey among our participants, 12 per cent indicated that passwords were stolen in credential phishing incidents. In these incidents, there was no compromise due to the use of multifactor authentication (MFA). However, this year, five attacks were reported where MFA was bypassed. In one of these cases, it led to the compromise of four mailboxes. Malicious actors often use compromised mailboxes for further malware and phishing attacks.

The compromised mailbox of a medicine supplier has caused a significant impact across multiple healthcare institutions. The phishing email sent from that mailbox ultimately led to the leakage of passwords from over 50 healthcare organisations and several data breaches in organisations that did not have MFA adequately implemented. It is important to realise that malicious actors often use the obtained access to further infiltrate a cloud environment and, in addition to e-mails, steal other data.

Web applications

Data breaches can also arise when scanning web applications for vulnerabilities. This could involve client/patient portals, exchange systems for healthcare providers, and similar platforms. Malicious actors can exploit these vulnerabilities to steal data. Last year, for instance, Z-CERT received a report involving the compromise of email addresses and hashed passwords from a vulnerable online learning platform. Additionally, Z-CERT is aware of cases where ethical hackers demonstrate that sensitive personal data is accessible via the internet.

Data breaches at suppliers

At Z-CERT, eight Dutch cases are known where data from healthcare institutions were leaked through a supplier. In two instances, this occurred via a subcontractor. The impact was, fortunately, often minimal. However, the potential severity of such incidents was starkly highlighted by incidents involving Nebu [20] and MoveIT [21], which received significant media coverage. In recent years, Z-CERT has observed increased dependency within the chain between healthcare organisations and IT suppliers. This brings the risk that a healthcare institution may have its own cybersecurity practices in order while an external party is not adequately equipped to handle today's digital threats.

In summary, the threat of data leakage through a (sub)supplier is real.

Cloud data breaches

The healthcare sector is increasingly transitioning to the cloud, heavily relying on web applications and mobile apps. In 2023, this threat became evident when an ethical hacker accessed sensitive data collected through an app for reporting boundary-crossing behaviour in hospitals. Due to a misconfiguration, they could view sensitive information and intercept the administrator password. A similar situation occurred in Switzerland, where information about patients' mental health could be accessed. This was perceived by one of the affected parties as a severe breach.

Furthermore, in 2023, there was an issue where sensitive data, in the form of configuration files, were inadvertently made public due to an employee's error. Configuration files often contain credentials, including API keys, which provide access to other cloud services without MFA. Malicious actors typically discover these files within two minutes of being made public [22]. Another example is accidentally granting more access than necessary. In 2023, an Indian medical diagnostic laboratory inadvertently made a database containing information on 12 million patients accessible in this way [23].

> **"Malicious actors typically discover configuration files within two minutes of being made public"**

In addition to the discussed misconfigurations, the use of third-party apps within cloud solutions poses a risk to the entire cloud environment. Z-CERT observes this risk, for example, in platforms like Microsoft Appsource and Google Suite Marketplace, where apps often acquire elevated privileges after installation [24].

Cybercriminals can exploit the gained access to a legitimate organisation's Office 365 environment by creating and publishing malicious apps under their name [25]. They then send phishing emails to users, requesting them to grant these malicious apps access to sensitive data, such as client or patient data. Because the app appears to have been published by a legitimate party, the user trusts it and grants access. Once obtained, MFA cannot prevent data leakage.

Data breaches and discarded medical equipment

A device no longer meets an organisation's requirements but is not yet at the end of its life cycle. Or the lease contract of a medical device expires. When the device is sold, donated, or reused, completely removing the stored data can be challenging. On occasion, errors can occur, resulting in data breaches. Z-CERT is aware of one case where data carriers were not adequately cleared. If it concerns a medical device, the consequences can be quite severe.

Of the latter, Z-CERT has no examples from 2023, but the risk is real. Rapid7 researched second-hand infusion pumps in the United States and found that the Wi-Fi login credentials were often still present [26].

Techniques and trends

Firstly, the frequency of business e-mail compromise (BEC) cases continues to persist. Data leakage via APIs also remains relevant. Additionally, Z-CERT observed the following trends in 2023:

- In 2023, Z-CERT observed Attacker in the Middle (AitM) phishing attacks for the first time in healthcare. In this type of phishing, malicious actors bypass the MFA barrier. The MFA request is forwarded to the victim, and if the victim responds, the malicious actor gains access.
  As a result of Microsoft's implemented measures, there is a decreasing trend in the utilisation of Office macros by malicious actors. With the disappearance of this attack vector, malicious actors have alternately utilised various other methods to spread malware and phishing links.
  In doing so, they often leverage major, well-known cloud providers (such as Adobe, Google, Dropbox, and Microsoft) to make phishing links appear legitimate. An article providing further insight into this matter is available on our website [27].
- Another phenomenon observed since last summer was Microsoft Teams phishing. In this type of attack, phishing messages are sent to Microsoft Teams users [28] [29]. In Office365, the 'Safe Links' feature can be activated to protect users from phishing URLs in both e-mail and Teams.

Response strategy

Much information is available on preventing data breaches caused by cyber incidents. We refer as much as possible to existing knowledge products, such as the Critical Controls (version 8) from the Centre for Internet Security (CIS) [30].

1. Utilise phishing-resistant MFA to prevent MFA circumvention. Refer to the factsheet from the NCSC 'Mature Authentication – Use of secure authentication tools' [31].

2. Implement an awareness program for identifying phishing and malware. One-time training is insufficient. Also, focus on QR code phishing and security risks associated with cloud usage. Refer to CIS Critical Control 14 [30].
3. Prevent Teams phishing by managing which domains can contact your users [32].
4. Utilise the 'Identity and Access' functionalities in the cloud and configure them according to security best practices, as defined in CIS Critical Controls 5 and 6. See also: 'Cloud Companion' of CIS Critical Controls [33].
5. Information security requirements should be documented in the agreement you make with a provider or supplier of digital services. Use the risk assessment questionnaire developed by Z-CERT and its participants from the supplier risk management project [34]. Also, this year, the NCSC provided guidance on how to deal with cybersecurity risks in the supply chain [35].
6. In addition to the above, extending the agreements made about data security to subcontractors who process data is advisable. Such agreements can, for example, be documented in a data processing agreement, as may be required by the GDPR. Because data processing often involves collaboration among various parties, it is vital to verify whether sufficient security measures have been implemented throughout the entire chain to minimise the risk of data breaches.
7. Utilise standards for securely configuring applications, network devices, and cloud environments. For instance, the CIS benchmarks [36] are supplier/product-specific and available for all major cloud providers.
8. Take measures to prevent the execution or downloading of malware. Refer to CIS Controls 2, 4, 9, and 10. Consider activating 'Attack surface reduction rules' in Windows environments.
9. To prevent the exploitation of vulnerabilities, pen tests, vulnerability management, and patch management are crucial. Refer to CIS Critical Controls 7 and 18 for this purpose. If you develop your own software, CIS Control 16 is relevant. Including web applications, mobile apps, and API endpoints in pen tests is essential.
10. It is advisable to establish a CVD process so that ethical hackers know how to report their findings. Z-CERT can assist participants in this regard [37].
11. Manage third-party apps in your cloud environments and grant only necessary permissions. Block users from directly granting third-party apps access to your data. This prevents 'consent phishing' from being successful.
12. Never store passwords in configuration files (such as .env or git configuration files), but only in securely designated password vaults. Set rules on your web servers to ensure these files are never internet-accessible.
13. Z-CERT advises removing data and following destruction processes when decommissioning electronic devices. Centralised control and an up-to-date asset database (Configuration Management Database, CMDB) are important for this purpose. Some healthcare organisations outsource destruction to specialised companies, where they review reports and randomly sample the quality. For more information, refer to 'NIST SP 800-88 Guidelines for Media Sanitization' [38].

threat

DDoS

Threat assessment: medium

Z-CERT estimates the threat level for DDoS attacks on healthcare institutions as 'medium.' However, the threat is more significant than last year, as it has become evident in the past year that the Dutch healthcare sector is also actively targeted by politically motivated actors (hacktivists).

Prediction 2024

Z-CERT expects several DDoS incidents this year with low to medium impact on Dutch healthcare institutions. Based on geopolitical developments, this could increase to dozens of incidents.

Incidents

The threat landscape for DDoS attacks shifted this year when healthcare organisations became the target of hacktivists. Fifteen hospitals reported attacks between January 28 and 31, 2023. In February, several DDoS attacks targeted Dutch hospitals, and we witnessed a significant increase across Europe (see Figure 5). Hacktivists were not solely focused on hospitals. Various healthcare-related entities were also mentioned as targets in hacktivist Telegram channels. Microsoft also observed attacks on hospitals (26%), other healthcare-related organisations (16%), and health insurers (16%) at the beginning of 2023 [39].

Although the focus in the first two months of 2023 was on healthcare, it shifted increasingly to other sectors throughout the year [40].

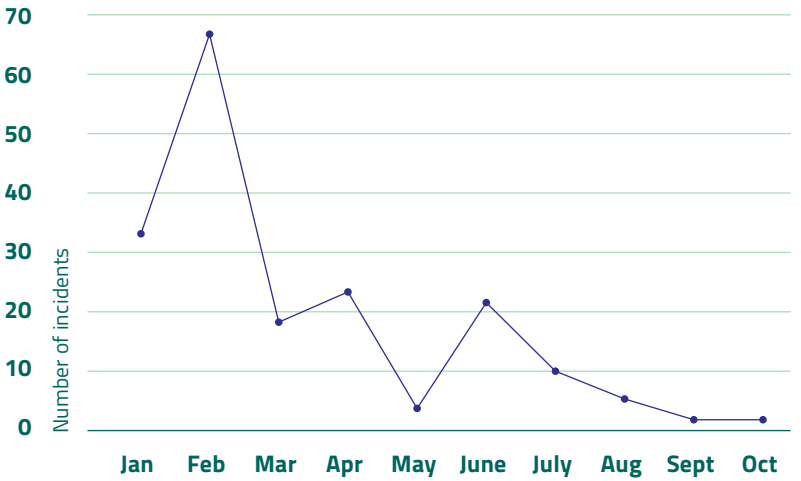


Figure 5

DDoS attacks carried out by hacktivist groups targeting the healthcare sector in Europe

Hacktivism motivations

In DDoS attacks on healthcare providers, Z-CERT has identified various actors with diverse motives. Last year, Z-CERT primarily recorded DDoS attacks from a hacktivist perspective. For example, many of these attacks were motivated by Dutch support for Ukraine. Hacktivist actors often respond to political developments or events featured in the news. Additionally, some groups reacted to issues other than the war in Ukraine. Examples included DDoS attacks in response to the burning of a Quran in Denmark [41] and the role of the United States concerning the conflict in Sudan [42].

The cooperation between pro-Russian groups and groups with other motives is often close. The degree of connectivity between these groups is difficult to determine.

DDoS attacks with motives other than hacktivism

In addition to DDoS attacks with a hacktivist motive, Z-CERT recorded several DDoS attacks where the motive could not be determined. In one case, we suspect that it involved someone dissatisfied with a healthcare organisation's services (and the sometimes sensitive cases they handle).

Impact of DDoS Attacks

Hacktivist attacks typically caused several hours, and in one case three days, of website disruption, resulting in delays or outages. Patients could not access the link to the patient portal during these attacks. At one healthcare institution, the impact was broader because the website was linked to the underlying IT infrastructure, resulting in brief disruption to other digital services, albeit minimal. In these incidents, there is also the need to inform many stakeholders, and the incident can lead to negative publicity.

In one incident, the DDoS attack caused delays in receiving client alarm notifications because the domotics system in the cloud became inaccessible. The impact was mitigated by activating DDoS protection for the cloud solution, which incurred associated costs.

“Hacktivist attacks typically caused several hours, and in one case three days, of website disruption, resulting in delays or outages”

Trends in techniques and methods

DDoS groups employ a variety of techniques. These will be explained in the chapter on DDoS and suppliers.

24

Key Takeaways from 2023

During the attacks, healthcare institutions learned several lessons that we would like to share in this threat report. Below, we will include the general response strategy.

1. **Geo-blocking** During a DDoS attack, blocking network traffic from other countries may be beneficial. Last year, during incidents in the Netherlands, most DDoS attacks originated from China [43]. This does not necessarily mean that the actors behind them are Chinese, but rather that the infrastructure used is located in China. An up-to-date overview of the origins of DDoS attacks can be found on this website [43].
2. **Proactive DDoS protection in the cloud** Identify critical systems and IP addresses in the cloud and actively monitor them for DDoS attacks. Verify whether your cloud provider offers functionality for this purpose and ensure that you can activate DDoS protection for the relevant IP addresses.
3. **Minimise disruptions to other services** Ensure that a DDoS attack on the website does not cause disruptions elsewhere in the network. You can achieve this by hosting the website separately from the rest of the network, for example, with a different web hosting provider.
4. **Limit the impact of an attack**
   - Switch to a simplified, static website during an attack for better performance and reduced downtime.
   - Implement measures such as Content Distribution Networks and web caching.
5. **Develop an incident response plan** When critical systems come under attack (on-premise or in the cloud), it's crucial to be prepared. Refer to [44] for an example incident response plan.

Response strategy

- Factsheet Continuity of online services [45]
- Factsheet Technical measures for continuity of online services [46]

threat

DDoS at suppliers

Threat assessment: medium

Z-CERT assesses the threat level for DDoS attacks on suppliers of healthcare institutions as 'medium.' However, the threat is slightly higher than last year because, in 2023, it was revealed that Dutch hosting providers were also actively targeted by hacktivists. This has an impact on healthcare institutions and their suppliers.

Prediction for 2024

Z-CERT anticipates recording several DDoS incidents affecting the healthcare sector in 2024. Depending on geopolitical developments, this could escalate to dozens. Depending on the type of supplier, the impact may be small. However, if a SaaS provider crucial to the healthcare process is affected, the impact could be more significant.

Frequency supplier incidents

17 per cent of the respondents reported a DDoS attack on a supplier impacting healthcare organisations (see Graph 1). Remarkably, these primarily involved digital service suppliers. In some cases, this was due to hacktivists attacking the hosting provider without explicitly targeting the healthcare institution. This affected a youth care institution, an elderly care institution and a hospital.

In other attacks, the motive behind the attack was not clear. However, it is evident that attacks with a hacktivist motive are on the rise. Research indicates that 66 per cent of the attacks are geopolitically motivated. Only 5 per cent had a different motivation (e.g., financial), and the motive for 28 per cent was unknown. In 2023, the ISP sector experienced around 500 DDoS attacks per quarter.

This illustrates that the threat for these providers is much greater than that for healthcare institutions themselves. Even before the war in Ukraine began, this sector was already dealing with a significant number of DDoS attacks. In 2021, an average of about 700 incidents per quarter were recorded.

Healthcare supplier	Impact on healthcare facility
DNS provider	Website unavailable or delayed through the domain name
SaaS provider	
Website hosting company	Website unavailable or delayed
Cloud supplier	
Network supplier	DDoS attack was mitigated
Patients portal	Unavailable

Figure 6

Suppliers to healthcare institutions affected by a DDoS attack

The impact was usually insignificant. However, with the increasing reliance on SaaS (Software as a Service) in the application landscape, it becomes increasingly important for the healthcare sector to discuss protection against DDoS attacks with suppliers. Illustrative was the attack described in the previous chapter, where the cloud infrastructure of a healthcare institution was targeted. This can also occur with, for example, a supplier offering a domotics service or a supplier of a patient monitoring service in the cloud. They must be able to respond to a DDoS attack, preferably in an automated manner. Realistically, a cloud service is targeted. In early June 2023, Microsoft Azure was hit by a DDoS attack, resulting in disruptions. The group's motive behind this was partly extortion and partly hacktivism [40]. Additionally, a healthcare institution reported experiencing disruptions due to these DDoS attacks. In addition to Microsoft, Google also reports that there have been attacks on Google services and the Google Cloud infrastructure, including the most prominent attack they have ever faced this year [48].

Trends in techniques and methods

There are different types of DDoS attacks, both at the network and application layers. In the Netherlands, in 2023, the attacks primarily targeted SYN floods (70%), Memcached Floods (10%), and Ack floods (6%) at the network layer. The latest information, specifically for the Netherlands, is available online and can serve as input for discussions with suppliers [43].

Although these techniques are widely used, the picture is more nuanced. Organisations monitoring DDoS attacks indicate that the modern DDoS attacker has access to many more attack vectors than ten years ago. A service supplier reported that in the first half of 2023, 53 per cent of attacks used only one attack vector. In 38 per cent of cases, there were two to five attack vectors, and in 9 per cent, there were six to ten attack vectors. Defence against multiple attack vectors is more complex. Even within a specific attack vector, an attacker can sometimes vary their approach [49]. Additionally, sources indicate that attacks involve a larger volume and that the number of attacks has increased, especially in Europe [50].

Another trend this year was a 20 per cent increase in 'DDoS for hire' platforms. On these platforms, a DDoS attack can be purchased for relatively little money (five dollars). This accessibility provides individuals seeking revenge, without much expertise, with a powerful weapon [40].

Key Takeaways from 2023

During the attacks, healthcare institutions learned several lessons that we would like to share in this threat report. For the general response strategy, we refer to the previous chapter (DDoS).

1. **Assess Suppliers** Evaluate suppliers for their resilience against DDoS attacks (see NEN 7510 control measure A.15.2.1).
2. **Opt for a new supplier** Choose suppliers with effective DDoS mitigation, such as those affiliated with a scrubbing service. However, verify whether the IP addresses you acquire are included in the mitigation. Z-CERT has noted that this is not always the case.
3. **Ensure advance communication with suppliers** This helps avoid discussions about costs while dealing with a DDoS attack. Before any incidents, discuss the DDoS measures implemented with suppliers and make clear agreements to avoid conflicts over costs.

threat

Cyber espionage by state actors

Threat assessment: high or low (depending on the type of organisation)

Z-CERT assesses the threat level for cyber espionage by state actors differently for various organisations. Z-CERT assesses this threat as 'high' for healthcare organisations conducting significant scientific research relevant to state actors or holding pertinent personal data. The high threat is attributed to attackers possessing high sophistication, patience, and financial resources to accomplish their missions.

Additionally, healthcare institutions may be targeted if they possess information about individuals that can be used for purposes such as recruitment and/or influence. We assess the threat as 'low' for healthcare institutions that do not have such relevant information or data.

Prediction for 2024

Z-CERT expects cyber espionage to remain relevant throughout 2024.

Incidents

State actors are known to gain access to organisations through the supply chain. This was also the case this year. The legitimate desktop application of the VoIP software solution 3CX was found to contain malware. The malicious update was actively distributed to customers. Several participants of Z-CERT and dozens of primary care practices, such as general practitioner offices and physiotherapy practices, were found to be using the software. The actor behind this attack was a subgroup of Lazarus, a group associated with North Korea. The motive of this group is most likely financial gain, as they primarily targeted companies involved in cryptocurrency [51]. The healthcare institutions were likely collateral damage. Z-CERT has not received any reports of concrete abuse.

The Netherlands ranks eighth on the list of European countries most targeted by digital attacks from state actors [9]. However, it does not seem likely that the healthcare sector is currently the primary target of state espionage campaigns. For example, Z-CERT has not received any reports of incidents involving espionage activities. Additionally, the healthcare sector is not listed in Microsoft's annual threat report as one of the top 10 actors affected by cyber espionage [2]. However, we know from international sources that healthcare is indeed a target, as occasional incidents are reported [52]. Furthermore, the AIVD notes that various digital attack campaigns frequently target knowledge institutions and scientists, primarily to acquire high-value technological knowledge [53].
Additionally, some governments have an interest in obtaining large quantities of personal data, which can be used for various purposes. These data are stored in large quantities by healthcare institutions.

Z-CERT considers it conceivable that there are targeted professional attacks on institutions on a limited scale to gather information about individuals important to them.

Impact

The consequences of stolen knowledge can range from unfair competition to unwanted use, such as for military purposes. Additionally, there is a risk that information about individuals could be used for recruitment or influence purposes [53]. For example, psychological and physical health data could be used to exert pressure on individuals.

Trends and developments

- A trend observed in 2023 and 2022, unrelated to espionage, pertains to ransomware. There are several instances of actors associated with North Korea targeting American healthcare institutions with ransomware [54]. We haven't witnessed these attacks in Europe yet. It's not ruled out that these actors, possibly working for known ransomware groups, are conducting attacks. Given their focus on financial gain and intent to target healthcare institutions, such attacks are also conceivable in Europe.
- State actors extensively employed 'Living off the land' techniques this year. With these techniques, the attacker primarily aims to utilise the system's own functionalities to achieve their goals [9] [55]. This indicates that the attackers seek to remain as covert as possible.

Response strategy

- **Cyber hygiene** Strategies from the chapter on ransomware and data breaches also apply to the threat of espionage by state actors in terms of cyber hygiene measures. A framework like 'CIS Critical Controls' is particularly practical in this regard.
- **Risk analysis and risk management** View your organisation from an attacker's perspective and identify technologies and crown jewels in terms of knowledge and research that may interest state actors. The AIVD, for example, has guidelines to assist you with this (In Dutch: 'handleiding kwetsbaarheidsonderzoek spionage') [56]. The Contact Point for Knowledge Security also has a document, 'National Knowledge Security Guidelines', that further elaborates on this [57].
- **Detection and mitigation of 'Living off the Land' techniques** More technical in nature are the recommendations from CISA regarding Chinese state actors attempting to evade detection [55].
- **Quickscan** At the government level, the 'Quickscan/risicomitigatie nationale veiligheid bij inkoop en aanbesteden' is utilised [58]. Based on the quickscan, it is determined whether a risk analysis is necessary.

threat

Digital financial fraud

Threat assessment: medium

In this threat landscape, we define digital financial fraud as fraud utilising digital media such as email and WhatsApp. Z-CERT assesses the threat level of this as 'medium'. Participants frequently report attempted financial fraud to Z-CERT. Therefore, this threat is classified as 'current' on the threat radar.

Most participants assess the impact of financial fraud as 'limited'. In rare instances, incidents involve over a hundred thousand euros. This occurred in 2023 with two municipalities [59] [60].

Prediction for 2024

Z-CERT expects numerous attempts at financial fraud in 2024 and anticipates several actual incidents.

Incidents

In 2023, there were numerous attempts at financial fraud involving digital means. These attempts often consisted of sending fraudulent e-mails, but WhatsApp, SMS, and telephone calls were also used as attack vectors.
In the questionnaire distributed for the threat landscape, 33 per cent of the respondents indicated that they collectively observed 415 attempts at digital financial fraud. Over 4 per cent of the respondents reported that the attempt was successful.
The incidents can be divided into a few types.

CxO Fraud

A specific form of financial fraud that emerged again this year is CEO fraud. This is a type of fraud in which an executive is impersonated, and the attacker attempts to convince an organisation employee to transfer money. Of the surveyed participants, 40 per cent detected attempts of CEO fraud (the total quantity could be higher); 2 per cent reported successful CEO fraud attempts.

Note that where 'CEO' is mentioned, it can also refer to CFO, CIO, CISO, and similar roles. Hence, we have titled this section 'CxO fraud'.

Fraudulent invoices

Fraudulent invoices or ghost invoices are still prevalent. Some of these are automatically intercepted, but the emails also land in employees' mailboxes.

Changing bank accounts

What applies to fraudulent invoices also applies to attempts to change bank account numbers of employees or suppliers. In the Z-CERT survey, both fake invoices and changing bank account numbers were queried in a single question. Of the surveyed participants, 21 per cent detected fraudulent invoices or an attempt to change a bank account number; 3 per cent reported a successful attempt.

Impact and actors

Financial fraud targets financial impact: Malicious actors attempt to transfer money or obtain (digital) gift cards. The actors can be individuals who repeatedly employ the same technique.
In gift card fraud or fraudulent invoices, the impact is usually limited to a few hundred euros. In other cases, if medical or IT equipment is purchased illegitimately in the organisation's name, the damage can amount to tens of thousands of euros. In a rare instance, a malicious actor succeeded in changing an account, enabling them to confiscate a one-time sum.

Other actors delve deeper into their targets and are thus able to orchestrate more targeted attacks. These actors are proficient in Dutch and excel in social engineering to achieve their objectives. They can learn from information published on LinkedIn, email signature templates mandated by the organisation, and other sources. As an indication of potential damage, the aforementioned incidents in municipalities resulted in losses of €176,040 [59] and €236,000 [59], respectively.

Methods and techniques

The manifestations of financial fraud are similar to previous years and have already been mentioned earlier in this chapter. Z-CERT also recorded several new techniques that are important to be aware of, such as:

- Orders were placed at online stores by impersonating a healthcare institution. For this purpose, a 'lookalike' domain of the healthcare institution was registered. The goods are delivered to the malicious actor, and the bill is sent to the healthcare provider.
- A malicious actor gathered job advertisements from multiple websites (such as those pertaining to healthcare or IT specialists) and issued invoices for services allegedly rendered to the organisations hosting the job postings on their platforms. The visibility of your authentic job listings on the respective platform might lead you to settle the invoice. With the current scarcity in the labour market, such fraudulent attempts may increase.
- An attacker established a deceptive website offering visitors the option to book appointments with medical specialists for a fee. However, the 'phantom appointment' arranged by the visitor is never registered by the institution, resulting in significant frustration. Moreover, it could potentially have adverse medical consequences for the visitor as the diagnosis or treatment may be delayed.

Key Takeaways from 2023

During the attacks, healthcare institutions learned several lessons that we would like to share in this threat report. Alongside this list, we will provide the general response strategy.

- Foster a culture where incidents are easily reported and share examples of such reports so that colleagues can learn from them.
- Implement policies within your email solution to block impersonation attempts of supervisors (spoofing), ensuring that e-mails pretending to originate from them are automatically blocked.
- Processes should apply to your executives and board as well. If high-ranking officials adhere to regular processes, CEO fraud is much less likely. In such cases, the fake messages are more easily noticeable.

> **“ If high-ranking officials adhere to regular processes, CEO fraud is much less likely ”**

Digital financial fraud response strategy

- Implement e-mail standards (SPF, DKIM, and DMARC).
- Monitor for ‘lookalike’ domain names that may be exploited for criminal purposes.
- Security awareness training on this subject is crucial because technical measures are ineffective against this type of fraud.
- Adjust internal authorisation procedures and processes to prevent fraud.
- Establish a procedure for employees to report attempted financial fraud. Employees should feel empowered to report issues without fear of reprisal if they make a judgment error.
- Financial fraud is a crucial aspect of supplier management. It’s not always the healthcare institutions that fall victim. Suppliers are also tempted to ship items to an address where criminals can easily intercept the package. Therefore, establish clear agreements with suppliers regarding modifying e-mail addresses, account numbers, and delivery locations. Additionally, only invoices submitted through the agreed-upon procedures should be processed.

- Additionally, Z-CERT has created a factsheet with recommendations and a checklist [61]. This includes measures related to email security, employee training, and process controls, among others.

32

theme

The use of generative AI in cyber attacks

Current state of affairs and future developments

Generative AI, mainly known through so-called 'large language models' (such as ChatGPT), has brought revolutionary changes. Generative AI will fundamentally change our way of working, learning, and creating. It can generate text, images, audio, and video based on user commands. However, what implications does this have for cybercrime, and how can organisations prepare themselves?

Current state of affairs

The use of generative AI in cyber attacks is still limited [62]. Z-CERT has yet to receive any reported incidents. However, it is only sometimes possible to determine this because AI-generated phishing emails, for example, are not always distinguishable from genuine ones. Z-CERT considers it very likely that generative AI is being used for targeted attacks, such as digital financial fraud and spear-phishing [63].

Developments in the threat landscape

The use of AI in cybercrime will increase, initially gradually, but possibly with a sudden acceleration, for example, due to open-source initiatives becoming more mature and more usable for cybercriminals [63]. There are already some initiatives in the field of AI focused on cybercrime that may also become increasingly mature [64].

How will the threat landscape change?

- **Enhanced phishing attacks** Cybercriminals who previously targeted healthcare institutions with generic, low-quality emails can now send targeted emails in competent Dutch.
- **Advanced fraud with audio and video** Fraud will also increasingly occur through fake audio and video, commonly known as deepfakes, which are almost indistinguishable from reality.
- **More efficient cyberattacks through AI** Cybercriminals become more effective with the aid of AI. It can be utilised to develop malware and exploits and automate complex attacks like ransomware. However, technical expertise from the attacker remains necessary.
- **Increase in successful attacks, but also increased defensive measures** It is expected that AI will lead to a rise in successful cyberattacks. However, the likelihood and impact of these attacks may be mitigated as AI is also increasingly utilised in defensive technologies. That said, introducing new technologies may create gaps that temporarily advantage attackers.

Types of AI-driven cyberattacks in the healthcare sector

The following attacks are expected to become increasingly relevant in the near future:

- **Fraudulent e-mails**
  AI can be utilised to generate convincing, targeted emails. This is achieved by training language models on specific information about the target, such as LinkedIn profiles or previously intercepted emails. E-mail interception is common in healthcare. These generated emails can be used to solicit sensitive information, credential phishing, and digital financial fraud.

- **Deepfake audio and video**
  Deepfake audio or video involves the replication of voices or images of individuals, often using material available online. This can be utilised for various types of fraud. While there are no known examples of this occurring in healthcare institutions, there was an incident in the news this year where criminals attempted to help request fraud by impersonating the voice of a family member [65].

Key Takeaways from 2023

The attacker of the future is more focused on their target, is more effective, and has fraudulent means that are almost indistinguishable from reality.
How should we respond to this?
Essentially, all the recommendations described earlier in the chapters on ransomware, financial fraud, and data breaches become more critical. However, we want to highlight some priorities that will help you be prepared for this new reality.

- **Identity and access management**
  Technologies that verify and control someone's identity are becoming increasingly important:
  - E-mail security standards SPF/DKIM/DMARC and BIMI.
  - Check your e-mail solution for functionality to prevent identity impersonation [66] and activate it.
  - Enable phishing-resistant MFA.
  - Add additional conditions for accessing data, such as access only from an organisation-managed system.

> **"The attacker of the future is more focused on their target, is more effective, and has fraudulent means that are almost indistinguishable from reality"**

- **Financial fraud**
  It is becoming increasingly important to structure financial processes in such a way that a misled employee cannot bypass them. Our knowledge product on financial fraud (https://z-cert.nl/factsheet-financiele-fraude) outlines various measures that address this issue. For instance, a good example is that only employees themselves should be able to change their own bank accounts.

- **Block malware**
  Preventive measures against malware are becoming more important. What we are seeing now is that e-mails are stolen by malware and reused for fraud. With AI, an attacker can train their models using this stolen material to generate emails in the victim's style.

- **Security awareness**
  Security awareness training becomes even more crucial than it already is. Training individuals to distinguish between real and fake by verifying the source is essential. People need to be trained to recognise professional cyberattacks involving AI, such as cases where a voice is simulated.

AI Applications in healthcare

While this chapter primarily focuses on using AI in cyberattacks, AI is also increasingly utilised in the healthcare sector for various applications, from diagnostics to voice-controlled reporting. This integration of AI brings risks in terms of cybersecurity and privacy. For more information on this topic, we recommend the following sources:

- Cybersecurity and privacy in AI - Medical imaging diagnosis [67] by ENISA.
- AI systems: develop them securely [68] by the AIVD.
- Guidelines for secure AI system development [69] by mainly national CERTs.

‘The threat radar indicates the timing, impact, and severity of cyber threats in healthcare’

Explanation of the threat radar

The threat radar is based on the FAIR (Factor Analysis of Information Risk) framework (www.fairinstitute.org) **and linked to a system that calculates a threat score. The methodology was developed in the Shared Research Programme (SRP) Cyber Security coordinated by TNO. Participants included ING, ABN AMRO, Rabobank, Volksbank and Achmea.**

The radar is divided into a 3x3 matrix and shows the time and impact of cyber threats in healthcare. The impact of a threat can be low/medium/high. The timeline is divided into the current situation, the situation that can be expected in the short term (within 1 year) or threats that may impact the future (more than 1 year from now).

The positioning of the various dots (with impact low/medium/high) in the radar graph is related to the threat assessment relative to time. If a particular threat is currently perceivable, the threat with its associated number will be positioned in the radar section of current threats. If a particular type of threat can be expected in the short term, within now and one year, then the threat in question will be positioned in the second ring.

Finally, Z-CERT also looks ahead by positioning threats expected beyond one year in the outer ring.

The placement of the dots also indicates the severity of the threat. The most severe threats are in the right-hand pie chart. The more dots to the left, the lower the threat they represent.

The impact coding associated with the threat is:

Colour	Impact
	High
	Medium
	Low

The assessment of the impact and the position of the threat is based on a calculation model from TNO. The estimated time is based on expert knowledge.

current

short term <1 yr

long term >1 yr

Bibliography

[1] **Coveware**, Januari 2024. [Online]. Available: https://www.coveware.com/blog/2024/1/25/new-ransomware-reporting-requirements-kick-in-as-victims-increasingly-avoid-paying.

[2] **Microsoft**, *"Microsoft Digital Defense Report 2023,"* 2023. [Online]. Available: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

[3] **CISA**, *"#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability,"* 7 Juni 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a. [Accessed 2023].

[4] **CISA**, *"Karakurt Data Extortion Group,"* 12 December 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-152a.

[5] **Le Soir**, *"Retour à la normale au CHU Saint-Pierre cible d'une cyberattaque,"* 11 Maart 2023. [Online]. Available: https://www.lesoir.be/500384/article/2023-03-11/retour-la-normale-au-chu-saint-pierre-cible-dune-cyberattaque.

[6] **Bleeping Computer**, *"Hospital Clínic de Barcelona severely impacted by ransomware attack,"* 7 Maart 2023. [Online]. Available: https://www.bleepingcomputer.com/news/security/hospital-cl-nic-de-barcelona-severely-impacted-by-ransomware-attack/.

[7] **KHO**, *"IT-Systemausfall nach Cyberattacke,"* 24 December 2023. [Online]. Available: https://www.kho.de/kho/index.php.

[8] **C. C. McGlave**, H. Neprash and S. Nikpay, *"Hacked to Pieces? The Effects of Ransomware Attacks on Hospitals and Patients,"* 4 Oktober 2023.

[Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4579292.

[9] **Microsoft**, *"Microsoft Digital Defense Report 2023,"* 2023. [Online]. Available: https://www.microsoft.com/en-us/security/security-insider/microsoft-digital-defense-report-2023.

[10] **ASD**, *"ASD Cyber Threat Report 2022-2023,"* 14 November 2023. [Online]. Available: https://www.cyber.gov.au/about-us/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023.

[11] **CVEdetails.com**, *"CVSS Scores Between 2022-01-01 and 2023-12-31,"* 2023. [Online]. Available: https://www.cvedetails.com/cvss-score-charts.php?fromform=1&vendor_id=&product_id=&startdate=2022-01-01&enddate=2023-12-31&groupbyyear=1.

[12] **CISA**, *"#StopRansomware: CL0P Ransomware Gang Exploits CVE-2023-34362 MOVEit Vulnerability,"* 7 Juni 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-158a.

[13] **CIS**, *"CIS Critical Security Controls,"* [Online]. Available: https://www.cisecurity.org/controls.

[14] **SURF**, *"Praktijkverhaal: CIS Controls framework kan helpen om hackers buiten de deur te houden,"* [Online]. Available: https://www.surf.nl/praktijkverhaal-cis-controls-framework-kan-helpen-om-hackers-buiten-de-deur-te-houden.

[15] **NCSC**, *"Incidentresponsplan Ransomware,"* 3 juni 2022. [Online]. Available: https://www.ncsc.nl/documenten/publicaties/2022/juni/3/incidentresponsplan-ransomware.

[16] **CISA**, *"Understanding Ransomware Threat Actors: LockBit,"* 14 Juni 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-165a.

[17] **CISA**, *"#StopRansomware: Rhysida Ransomware,"* 15 November 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-319a.

[18] *"Q & A Cyberaanval (update 16 november 2023),"* Tunstall, 16 November 2023. [Online]. Available: https://www.tunstall.nl/q-a-cyberaanval-update-16-november-2023/.

[19] **Ortivus**, *"Ortivus' electronic patient record system are down for some United Kingdom based customers due to a cyber-attack,"* Juli 2023. [Online]. Available: https://www.ortivus.com/mfn_news/ortivus-electronic-patient-record-system-are-down-for-some-united-kingdom-based-customers-due-to-a-cyber-attack/.

[20] **NOS**, *"Nos.nl,"* 6 4 2023. [Online]. Available: https://nos.nl/artikel/2470392-softwarebedrijf-moet-marktonderzoeker-meer-over-datalek-vertellen. [Accessed 3 12 2023].

[21] *"Techtarget - Health IT Security,"* 17 10 2023. [Online]. Available: https://healthitsecurity.com/news/rcm-company-reports-data-breach-tied-to-moveit-software-1.9m-impacted. [Accessed 3 12 2023].

[22] *"2023 Honeypotting in the Cloud Report,"* 2023. [Online]. Available: https://orca.security/lp/2023-honeypotting-cloud-report/.

[23] **J. Fowler**, *"Millions of Highly Sensitive Patient Records Exposed in Medical Diagnostic Company Data Breach,"* 25 Oktober 2023. [Online]. Available: https://www.websiteplanet.com/news/redcliffe-breach-report/.

[24] **Adaptive Shield**, *"Kickstarting a Robust Security Program,"* 2023.

[25] **Proofpoint**, *"OiVaVoii – An Active Malicious Hybrid Cloud Campaign,"* 27 Januari 2022. [Online]. Available: https://www.proofpoint.com/us/blog/cloud-security/oivavoii-active-malicious-hybrid-cloud-threats-campaign.

[26] **Rapid7**, *"New Report: Medical Health Care Organizations Highly Vulnerable Due to Improper De-acquisition Processes,"* 2023. [Online]. Available: https://www.rapid7.com/info/medical-devices-report/.

[27] **Z-CERT**, Februari 2024. [Online]. Available: https://z-cert.nl/nieuwe-phishingtechnieken.

[28] **J. Nordenlund**, *"DarkGate Loader Malware Delivered via Microsoft Teams,"* 9 Juni 2023. [Online]. Available: https://www.truesec.com/hub/blog/darkgate-loader-delivered-via-teams.

[29] **Y. Tas**, *"Microsoft Teams Chat: the rising phishing threat and how to stop it,"* 2023. [Online]. Available: https://www.eye.security/blog/microsoft-teams-chat-the-rising-phishing-threat-and-how-to-stop-it#.

[30] **Center for Internet Security**, *"CIS Critical Security Controls (vesie 8),"* [Online]. Available: https://www.cisecurity.org/controls.

[31] **NCSC**, *"Factsheet 'Volwassen authenticeren – gebruik veilige middelen voor authenticatie,"* 25 April 2022. [Online]. Available: https://www.ncsc.nl/documenten/factsheets/2022/april/24/factsheet-volwassen-authentiseren-gebruik-veilige-middelen-voor-authenticatie.

[32] **Microsoft**, *"IT Admins - Manage external meetings and chat with people and organizations using Microsoft identities,"* 1 Juni 2023. [Online]. Available: https://learn.microsoft.com/en-us/microsoftteams/trusted-organizations-external-meetings-chat?tabs=organization-settings.

[33] **CIS**, *"CIS Controls Cloud Companion Guide (versie 8),"* 2022. [Online]. Available: https://learn.cisecurity.org/cis-controls-v8-cloud-companion-guide.

[34] **Z.-C. e. m. v. e. a. d. v. Z-CERT**, *"CSAP (Z-CERT's besloten platform voor het delen van informatie),"* 07 December 2023. [Online]. Available: https://z-cert.cyware.com/dashboard/doc-library/9e6e4eb6-e224-41b2-86f1-d7299f8850a9/.

[35] **NCSC**, *"https://www.ncsc.nl/documenten/publicaties/2023/augustus/15/risicos-in-de-toeleveringsketen,"* 2023.

[36] **C. f. I. Security**, *"CIS Benchmarks List,"* [Online]. Available: https://www.cisecurity.org/cis-benchmarks.

[37] **Z-CERT**, *"Coordinated Vulnerability Disclosure,"* [Online]. Available: https://z-cert.nl/cvd-meldingen/.

[38] **NIST**, *"Guidelines for Media Sanitization,"* 2014. [Online]. Available: https://csrc.nist.gov/pubs/sp/800/88/r1/final.

[39] **Microsoft**, *"KillNet and affiliate hacktivist groups targeting healthcare with DDoS attacks,"* 17 Maart 2023. [Online]. Available: https://www.microsoft.com/en-us/security/blog/2023/03/17/killnet-and-affiliate-hacktivist-groups-targeting-healthcare-with-ddos-attacks/.

[40] **ENISA**, *"ENISA THREAT LANDSCAPE FOR DoS ATTACKS,"* 10 December 2023. [Online]. Available: https://www.enisa.europa.eu/publications/

enisa-threat-landscape-for-dos-attacks/@@download/fullReport.

[41] *"SC Media,"* 26 Februari 2023. [Online]. Available: https://www.scmagazine.com/news/danish-hospitals-latest-target-of-ddos-attacks-on-nato-backed-countries.

[42] **Radware**, *"Anonymous Sudan,"* 2023. [Online]. Available: https://www.radware.com/cyberpedia/ddos-attacks/anonymous-sudan/.

[43] **Cloudflare**, *"Security & Attacks in,"* 1 Januari 2023. [Online]. Available: https://radar.cloudflare.com/security-and-attacks/nl?dateRange=52w.

[44] **The Scottish Government**, [Online]. Available: Google: *"scottish government ddos incident response"*.

[45] **NCSC**, *"Factsheet Continuïteit van online diensten,"* 2 Maart 2023. [Online]. Available: https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-continuiteit-van-onlinediensten.

[46] **NCSC**, *"Factsheet Technische maatregelen voor continuïteit voor online diensten,"* 2 Maart 2023. [Online]. Available: https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-technische-maatregelen-voor-continuiteit-van-online-diensten.

[47] **NBIP**, *"Cijfers DDoS-aanvallen in het vierde kwartaal 2021,"* 2021. [Online]. Available: https://www.nbip.nl/wp-content/uploads/2022/01/NBIP-Infographic-DDoS-data-Q4-2022-01.png.

[48] **Google**, *"Google mitigated the largest DDoS attack to date, peaking above 398 million rps,"* 10 Oktober 2023. [Online]. Available: https://cloud.google.com/blog/products/identity-security/google-cloud-mitigated-largest-ddos-attack-peaking-above-398-million-rps.

[49] **Akamai**, *"The Relentless Evolution of DDoS Attacks,"* 23 Juni 2022. [Online]. Available: https://www.akamai.com/blog/security/relentless-evolution-of-ddos-attacks.

[50] **Netscout**, *"NETSCOUT DDoS THREAT INTELLIGENCE REPORT / FINDINGS FROM 1ST HALF 2023,"* 2023. [Online]. Available: https://www.netscout.com/threatreport/emea/.

[51] **Kaspersky**, *"3CX attack targeted cryptocurrency companies with Gopuram malware,"* 3 April 2023. [Online]. Available: https://usa.kaspersky.com/about/press-releases/2023_3cx-attack-targeted-cryptocurrency-companies-with-gopuram-malware.

[52] **American Hospital Association**, *"HC3 TLP Clear Threat Profile: China-Based Threat Actors - August 16, 2023,"* 16 Agustus 2023. [Online]. Available: https://www.aha.org/cybersecurity-government-intelligence-reports/2023-08-16-hc3-tlp-clear-threat-profile-china-based-threat-actors-august-16-2023.

[53] **AIVD**, *"Dreigingsbeeld Statelijke Actoren (DBSA 2),"* 28 November 2022. [Online]. Available: https://www.aivd.nl/documenten/publicaties/2022/11/28/dreigingsbeeld-statelijke-actoren-dbsa-2.

[54] *"#StopRansomware: Ransomware Attacks on Critical Infrastructure Fund DPRK Malicious Cyber Activities,"* 9 Februari 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-040a.

[55] **CISA**, *"People's Republic of China State-Sponsored Cyber Actor Living off the Land to Evade Detection,"* 24 Mei 2023. [Online]. Available: https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-144a.

[56] **AIVD**, *"Handleiding Kwetsbaarheidsonderzoek spionage,"* 2 Februari 2011. [Online]. Available: https://www.aivd.nl/documenten/publicaties/2011/02/17/handleiding-kwetsbaarheidsonderzoek-spionage.

[57] **Loket Kennisveiligheid**, *"Nationale leidraad kennisveiligheid - Veilig internationaal samenwerken,"* 14 Januari 2022. [Online]. Available: https://www.rijksoverheid.nl/documenten/rapporten/2022/01/14/nationale-leidraad-kennisveiligheid.

[58] **Rijksoverheid**, *"Quickscan/risicomitigatie nationale veiligheid bij inkoop en aanbesteden,"* 2019. [Online]. Available: https://www.pianoo.nl/nl/regelgeving/crisis-en-inkoop/nationale-veiligheid/quickscanrisicomitigatie-nationale-veiligheid-bij.

[59] **Gemeente Krimpen aan den IJssel**, *"Gemeente Krimpen aan den IJssel,"* 14 Maart 2023. [Online]. Available: https://krimpenaandenijssel.nl/gemeente-krimpen-aan-den-ijssel-doelwit-van-externe-fraude/.

[60] **Gemeente Alkmaar**, "*De gemeente Alkmaar getroffen door internetfraude,"* 14 September 2023. [Online]. Available: https://www.alkmaar.nl/actueel/de-gemeente-alkmaar-getroffen-door-internetfraude/.

[61] **Z-CERT**, *"Factsheet digitale financiële fraude,"* 2024. [Online]. Available: https://z-cert.nl/factsheet-financiele-fraude.

[62] **Mandiant**, *"Threat Actors are Interested in Generative AI, but Use Remains Limited,"* 19 Oktober 2023. [Online]. Available: https://www.mandiant.com/resources/blog/threat-actors-generative-ai-limited.

[63] **NCSC**, *"AI: Cruciaal moment in de geschiedenis of een hype?,"* 6 Juni 2023. [Online]. Available: https://www.ncsc.nl/actueel/weblog/weblog/2023/ai-cruciaal-moment-in-de-geschiedenis-of-een-hype. [Accessed 2023].

[64] **D. Kelley**, *"WormGPT – The Generative AI Tool Cybercriminals Are Using to Launch Business Email Compromise Attacks,"* 13 Juli 2023. [Online]. Available: https://slashnext.com/blog/wormgpt-the-generative-ai-tool-cybercriminals-are-using-to-launch-business-email-compromise-attacks/.

[65] **RTL Nieuws**, *"Marion werd opgelicht met stem van zoon: 'Hij liep net op tijd de woonkamer binnen',"* 23 Mei 2023. [Online]. Available: https://www.rtlnieuws.nl/nieuws/nederland/artikel/5385957/oplichting-stem-klonen-familie-kunstmatige-intelligentie.

[66] **Microsoft**, *"Anti-spoofing protection in EOP,"* [Online]. Available: https://learn.microsoft.com/en-us/microsoft-365/security/office-365-security/anti-phishing-protection-spoofing-about?view=o365-worldwide. [Accessed 2023].

[67] **Enisa**, *"Cybersecurity and privacy in AI - Medical imaging diagnosis,"* 7 Juni 2023. [Online]. Available: https://www.enisa.europa.eu/publications/cybersecurity-and-privacy-in-ai-medical-imaging-diagnosis.

[68] **AIVD**, *"AI-systemen: ontwikkel ze veilig,"* 15 Februari 2023. [Online]. Available: https://www.aivd.nl/documenten/publicaties/2023/02/15/ai-systemen-ontwikkel-ze-veilig.

[69] **NCSC UK**, *"Guidelines for secure AI system development,"* 27 November 2023. [Online]. Available: https://www.ncsc.gov.uk/collection/guidelines-secure-ai-system-development.

Acknowledgements

We extend our gratitude to everyone who contributed to the production of this Cybersecurity Threat Landscape for healthcare, including several reviewers from healthcare institutions, CISOs from various healthcare organisations, and suppliers.

In particular, we would like to thank:

National Cyber Security Centre (NCSC)
Ewald Beekman (Amsterdam UMC)
Lion van Galen (CuraMare Spijkenisse, cooperating in Stichting Samenwerkende Rijnmond Ziekenhuizen)
Renco van Leeuwen (WVO Zorg)
Dick van Mourik (Stichting Beweging 3.0)
Adrie Rolloos (Parnassia Groep)
Mitchell Sudmeijer (GGD-ZW)
Jos Toet (Franciscus Gasthuis & Vlietland, cooperating in Stichting Samenwerkende Rijnmond Ziekenhuizen)
Leon Urbanus (ASVZ)
Erick van Veghel (Catharina Ziekenhuis)
Dennis Verschuuren (Maasstad Ziekenhuis, cooperating in Stichting Samenwerkende Rijnmond Ziekenhuizen)

Lastly, we would like to thank **Artiënne Buissant des Amorie** of Artgen for the layout of the threat report.

Stichting Z-CERT
Stationsplein 121
3818 LE Amersfoort
033 737 06 09

info@z-cert.nl
www.z-cert.nl