Cybersecurity Threat Assessment for the Healthcare Sector 2022

COMPUTER EMERGENCY RESPONSE TEAM VOOR DE ZORG

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 Assessment for the Healthcare Sector 2022 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.

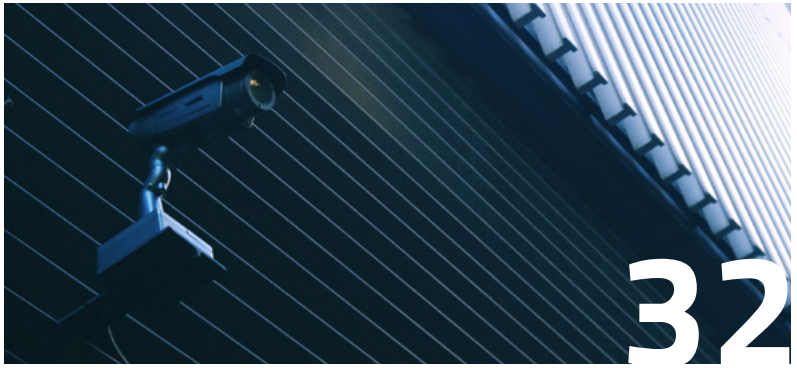
We form a professional network with our affiliated healthcare institutions, the National Cyber Security Center (NCSC), Health-ISAC (Information Sharing and Analysis Center), industry organisations, suppliers and other Computer Emergency Response Teams (CERTs). Together, we tackle cyber challenges, such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

The content of this Cybersecurity Threat for Care 2022 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.

Z-CERT's mission is to strengthen the digital security of the healthcare sector


ZA
CERT
COMPUTER EMERGENCY
RESPONSE TEAM
VOOR DE ZORG

Contents



‘Ransomware still poses the biggest threat to healthcare facilities’

Foreword

The year 2022 was a turbulent year in many aspects. In healthcare, an increasing number of processes are becoming digital, and more systems are operating in the cloud. Due to this growing digitalization, the healthcare sector is more vulnerable to disruptions and data breaches. Of course, there have been other developments that have influenced the threat landscape as well.

In this third edition of the Cybersecurity Threat Assessment for the healthcare, we describe the trends and threats that had the greatest impact on the Dutch healthcare sector in the past year. New this year is the threats we have visualized in a threat radar. This model was developed by TNO and is used, among other things, to depict cyber threats in the financial sector.

Ransomware is still a threat

Based on the feedback from our respondents, news reports, and global experiences, it appears that ransomware continues to be the biggest threat to healthcare institutions. This is also evident from the counter on Z-CERT’s website, which has been running since October 2021. This counter indicates the number of ransomware incidents known to Z-CERT in the healthcare sector in the Netherlands and Europe. Z-CERT has particularly noted a significant increase in healthcare-related ransomware incidents in neighboring countries this year.

This indicates that the volume of ransomware incidents has increased in European healthcare facilities this year. In any case, it confirms that the healthcare sector is vulnerable to ransomware incidents. On the positive side, cybercriminals are often predictable and frequently use familiar techniques. This practice makes them easier to detect. This is good as healthcare facilities can improve detection in particular, according to our threat assessment.

Fewer incidents, more impact

Although Z-CERT did not record more ransomware incidents at Dutch healthcare facilities in 2022 than the previous year, the impact on the total number of healthcare facilities was higher than a year earlier.

Since the spring of 2022, pro-Russian hacktivists have been notable for executing DDoS attacks targeting mainly NATO countries and Ukraine. These attacks targeted various sectors such as banks, aviation, railways, the energy sector, logistics and technology companies and the government. The healthcare sector has also been targeted. In January this year, several hospitals were hit by DDoS attacks. Z-CERT was also targeted in attacks by hacktivist groups.

These and other trends are described in detail in this threat assessment, however, we go beyond noting key trends. To help you with today's knowledge, this report includes many tips and best practices to help you take your healthcare organisation's security to the next level. By sharing knowledge, in particular, we can contribute to a safer digital society.

I wish you a pleasant read and a digitally secure future.

Wim Hafkamp
Director of the Z-CERT foundation

explanation

‘The importance of creating awareness within your organisation and prioritising measures’

Incidents among respondents

For the Threat Assessment, Z-CERT asked participants what type of security incidents they had experienced. The results are shown in the graph to the right. Use it when creating awareness within your organisation and prioritising measures. The incidents will be explained further in the ‘threats’ sections and were used, among other things, to determine the threat level.

Common incidents

Respondents to the Z-CERT questionnaire mentioned a relatively broad spectrum of various incidents they have encountered. The graph refers to incidents that took place in practice. However, for financial fraud, we also asked about the attempts, to highlight the scale of the problem. It turned out that 42 per cent of healthcare facilities recorded 1 or more attempts at financial fraud. These are attempts that occurred through digital media such as e-mail and WhatsApp. In second place among the respondents, credential phishing (22%) appears to be the issue, followed by DDoS attacks at the suppliers (10%), hacking and malware (both 10%) and ransomware at the provider (6%). In last place are cyber-related data breach organisations (5%) and successful financial fraud (3%). Ransomware occurred at 1%, however, the total amount of ransomware incidents in the healthcare sector is higher.

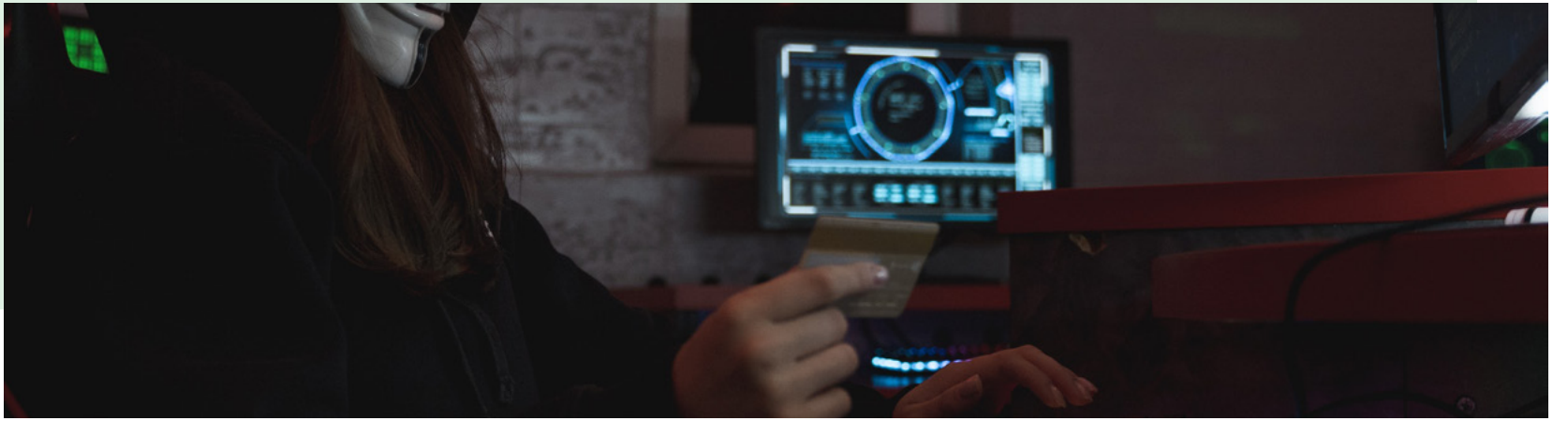
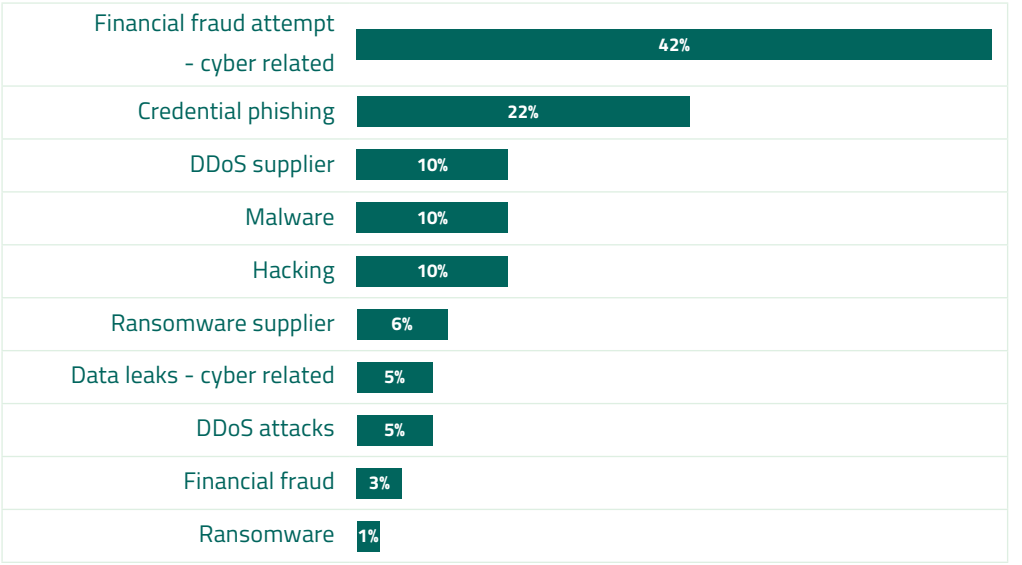


Figure 1

Most common types of security incidents among surveyed Dutch healthcare institutions



Explanation

By 'data breaches- cyber-related' we refer to data breaches that occurred due to malware, credential phishing or hacking. A ransomware incident occurred in 1 per cent of respondents. However, the actual amount of ransomware incidents in the Dutch healthcare sector was higher. This is explained further in the section on ransomware. The financial fraud categories in the graph involve financial fraud committed by using digital media such as mail and WhatsApp.

Explanation of the threat assessment

To compile this threat assessment, Z-CERT used open and closed sources as well as incidents reported to Z-CERT. In addition, a questionnaire was sent to healthcare organisations affiliated with Z-CERT. Z-CERT also held interviews mainly with CISOs of healthcare organisations from different sub-sectors. The questionnaire was completed by participants from all sub-sectors affiliated with Z-CERT.

This threat assessment is generic for healthcare. Therefore, Z-CERT advises each healthcare facility to interpret the threat assessment and translate it to their situation. For example, if a healthcare organisation primarily uses SaaS applications, the threats regarding suppliers probably need to be more severely assessed. If a healthcare facility does scientific research and is engaged in product development in collaboration with medical device suppliers and universities, state threats need to be more severely assessed. However, when you have brought cyber resilience to a high maturity level, many threats to your organisation will not be as severely assessed as in organisations that still require significant steps in this regard.

‘Z-CERT used open and closed sources, reported incidents and a survey among affiliated healthcare organisations’

The threat radar

To help healthcare facilities communicate threats within their organisation effectively, Z-CERT has chosen to display the threats through a visualisation we call the 'threat radar'. The radar is also used in other sectors.

The threat radar was created by incorporating the information entered by our survey participants into a model. The model is based on the FAIR (Factor Analysis of Information Risk) framework (https://www.fairinstitute.org) and linked to a system that calculates a threat score. This threat score is used to visually display the threats within the radar.

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.

current

short term <1 yr

long term >1 yr

The impact coding associated with the threat is:

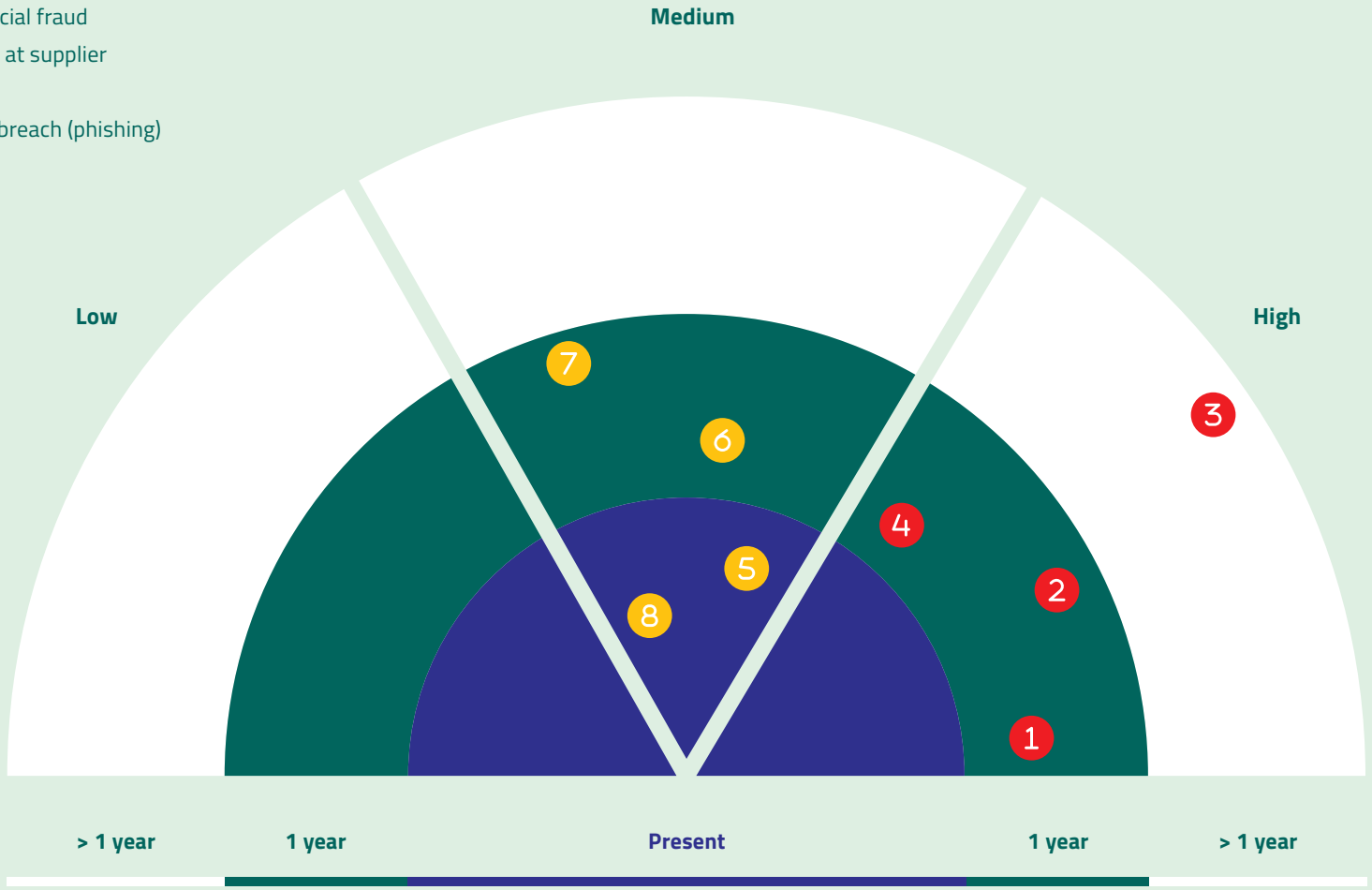
Colour	Impact
	High
	Medium
	Low

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.

Legend

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

Threat Radar



13

> **Shared IT-infrastructure can greatly increase the impact of a single incident**

threat

Ransomware at healthcare facilities

Threat estimate: high

Z-CERT estimates the threat level for disruptions by ransomware as 'high'. In 2023, Z-CERT expects numerous attempts of intrusion by ransomware operators. Z-CERT expects several ransomware incidents in the Dutch healthcare sector within a year.

Incidents

The high threat level is reflected, among other things, in the number of incidents. It is impossible to determine the actual number of incidents in the healthcare sector in Europe as in many countries reporting is not mandatory. However, by monitoring data breach websites on the dark web and incidents that have been in the public eye, Z-CERT recorded 65 per cent more ransomware incidents in European healthcare facilities than in 2021. Globally, Z-CERT recorded 28 per cent more ransomware incidents at healthcare organisations than the year before.

In 2022, Z-CERT recorded five ransomware incidents at Dutch healthcare facilities. That was the same number as in the previous year. However, the difference with 2021 is that the impact on the total number of healthcare facilities that experienced inconvenience in the Netherlands was much higher. This was due to one ransomware incident in which 120 dental practices were temporarily unable to access patient records as their parent company was affected by ransomware [1]. Shared IT infrastructure can significantly increase the impact of a single incident.

Supply Chain effects

An incident at a healthcare facility is rarely limited to the facility itself. For instance, if hospitals are unable to transfer their patients to an elderly care facility, or if an ambulance service breaks down, it affects the chain. When urgent healthcare is unavailable, another healthcare facility will often have to provide it.

Preliminary activities

The malware and phishing incidents from the incident graph at the beginning of this threat assessment paint a picture of preparatory activities, some of which can be attributed to ransomware groups or their partners. It shows that the threat of ransomware is topical for Dutch healthcare facilities.

Operators

Z-CERT notes that in 2022, there were at least 15 active groups, who have both the intention and the means to successfully execute ransomware attacks on European healthcare facilities. Three of the group's operations were so sophisticated that they were able to create dozens (sometimes more than 100) of incidents per month.

15

For the operators monitored by Z-CERT this year, the motive is financial gain. In exceptional cases, it is apparent that if a ransomware victim explains that they are a healthcare organisation, the duped organisation can get the decryption key for free [2].

> **“For the operators monitored by Z-CERT this year, the motive is financial gain”**

Susceptibility to the threat

Research by Z-CERT shows that healthcare is susceptible to ransomware incidents, due to a lack of maturity in terms of prevention and in particular detection.

Recognising that prevention can be improved is important to prevent any unnecessary risk escalation. An example of this is allowing systems to access the internet but lacking the ability to react quickly to patch critical vulnerabilities. This backfired in 2022 when a Dutch healthcare facility failed to patch a mail server in time, allowing an attacker to penetrate and activate ransomware. This healthcare facility has since outsourced to a party who can ensure this via their cloud solution. It requires a certain level-headedness to recognise that an organisation cannot cope with the race against the clock against cybercriminals and that a different path needs to be taken.

Does the type of organisation and organisation size matter?

At the European level, almost all subsectors experienced ransomware incidents (see Annex Figure 1), both large hospitals and small primary care practices. The threat of ransomware is thus topical for every type of healthcare organisation.

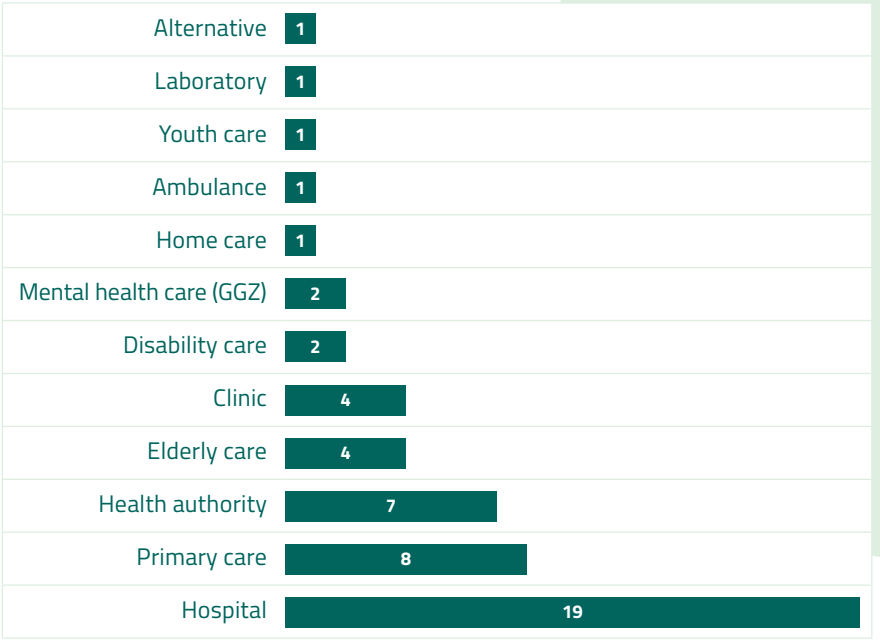


Figure 1

Amount of ransomware incidents in the European healthcare sector in 2022

Regarding organisation size, ransomware groups do not appear to be selective. Smaller organisations are also of interest to cybercriminals. Some ransomware groups prefer to attack ten small organisations rather than one large one. Small organisations often have fewer resources for their security operation and the ransomware operator is less exposed to intelligence services or politics.

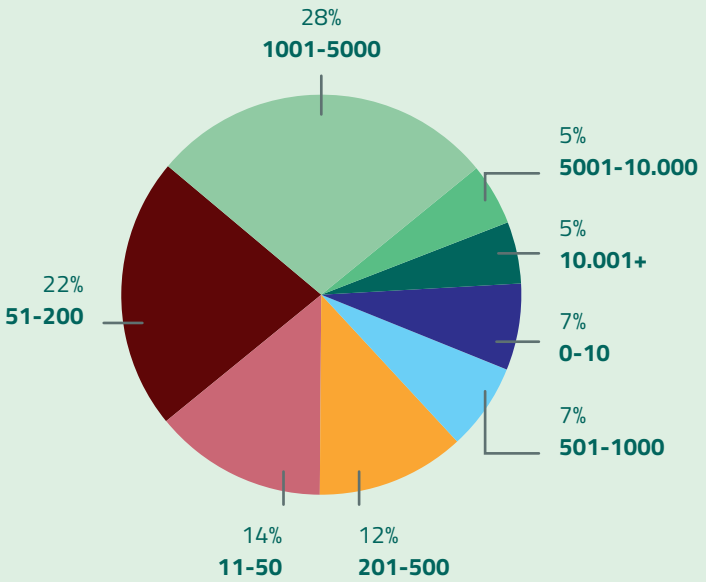


Figure 2

Percentage of ransomware incidents by size of healthcare facility
(number of staff)

Impact

The impact may vary from attack to attack depending on the data the attacker accessed and the recovery capability of the facility. We have compiled some facts for this threat assessment providing more insight into the potential impact.

- In 2021, an (international) study on ransomware at healthcare facilities found that the cost to recover from a ransomware incident was about $1.85 million [3]. Thereby, healthcare was the second most costly sector in terms of recovery.

- The same survey found that 44 per cent of healthcare organisations take a week for a complete recovery. For one-fourth, it takes as long as a month [3].

- Of the 51 observed ransomware attacks in the European healthcare sector, 28 appeared on so-called data breach sites on the dark web, threatening to leak the captured data.

Research on healthcare ransomware incidents worldwide over the first 9 months of 2022 shows that:

- In 50% of the registered cases, patients had to divert to other healthcare facilities.
- In just over half the registered cases, appointments had to be cancelled or rescheduled.
- In 93% of registered cases, IT-systems were unavailable.

Methods

For a threat to be effective, your organisation must be susceptible to the techniques used by the attacker. On that note, there is good news. Although groups have become both more professional and thus more effective, the techniques used by ransomware groups have remained relatively constant in recent years. Meaning that they often exploit the same vulnerabilities and misconfigurations [4].

The most common techniques [5] [6] used to infiltrate an organisation:

- Mail containing malware (links to malware or malicious attachments).
- Access to remote access solutions with stolen or leaked passwords, mainly via RDP but also, for example, the Citrix remote work solution and VPN solutions.
- Misuse of vulnerabilities.

In 2022, vulnerabilities in firewall solutions, Microsoft's mail solution (Microsoft Exchange), online portals and Log4j were the most popular. Z-CERT noticed that ransomware operators also exploited vulnerabilities in firewall products used by small organisations. These were not mentioned in public news media.

Recommendations

It is critical to make the initial entry of a ransomware operator as difficult as possible. In part because practice shows that it is easier for healthcare organisations to stop hackers during this attack phase than when hackers have already penetrated the network.

Also, measures to prevent initial access are often free of charge in acquisition as they involve using pre-existing features in Windows.

To prevent initial access, Z-CERT recommends prioritising the following:

- **Application allowlisting**
  A solution such as AppLocker is used to prevent programmes not approved by the organisation from being started. The method involves defining rules. For example, only applications may be launched that are located in "program files". This allows simple rules to block even advanced malware not yet recognised by the antivirus solution. Good guides are available online to set this up effectively [7].

- **Securing Microsoft Office against exploitation**
  Microsoft Office is extremely popular and hackers, therefore, like to use malicious Office files to penetrate organisations. For this reason, it is important to secure Office as much as possible against such attacks. Accordingly, Z-CERT recommends the following:

  - Phase-out the use of macros. If this is not (yet) possible, regulate the use of macros (see: [8]). Security specialists are often concerned that disabling or managing macros will lead to many complaints. Healthcare organisations have had success by implementing this in stages.
  - Enable "Attack surface reduction rules" related to Office. Practice shows that these frequently succeed in stopping new attacks via Office documents.

    - Use the available configuration options in Office that help against all kinds of misuse (see [9]).

- More often, malware is offered packaged in a **CD image file**. In part, this is done to bypass Microsoft's stricter rules on starting macros. The ability to view the contents of these files can be disabled [10]. However, application allowlisting can also be set to prevent the execution of malware from these CD image files.

- **Use multi-factor authentication** for all services providing access to the network and for accounts with high privileges.

- **Prioritise patching of systems and software that are accessible to the internet.** Make a realistic assessment of whether your IT department can handle the pressure and otherwise opt for a cloud solution, expansion IT department, outsourcing or phasing out.

- **Prioritise patching of commonly used desktop software** such as web browsers, Microsoft Office and PDF readers.

- **If you have outsourced patching, manage your supplier and adjust if risk tolerances are exceeded.** The latter is necessary, as Z-CERT has many examples of vendors who are late with patching. Management can only be implemented effectively if agreements are made with the supplier. Vulnerabilities in a firewall solution classified as critical that can be exploited from the internet, for example, must be patched within the agreed time.

Protecting data

To protect data, it is crucial to have an offline or immutable backup of your important data. Immutable backups are backups that cannot be modified and thus can't be encrypted by a ransomware operator. Not every offsite backup is well protected against ransomware as attackers can often access the offsite backup in a fully compromised environment.

Additional literature

For more literature on ransomware and what can be done against it. Z-CERT refers to our website where we address network attacker detection [11] and the top 10 most useful measures [12]. For more advice on incident response and prevention, Z-CERT refers to the NCSC's white paper *"Ransomware Incident Response Plan"* [13].

threat

Ransomware in the supply chain

Threat estimate: high

Z-CERT estimates the threat level for disruptions by ransomware in the supplier chain of healthcare facilities as 'high'. Suppliers to healthcare facilities are affected more often than healthcare organisations themselves. In the coming year, Z-CERT expects several ransomware incidents in the supply chain that will impact Dutch healthcare facilities.

Other sectors besides healthcare are also affected by ransomware incidents. Research by Z-CERT shows that in Europe, for example, construction, IT service providers and the government probably had more ransomware incidents than healthcare. This was evident in 2022 as incidents in the supply chain frequently impacted healthcare facilities (see table 1). In 2022, fewer incidents were reported to Z-CERT than in 2021. In most cases, the impact was not as severe. On one occasion, an incident led to disruptions of significant processes (see table 1).

Z-CERT recorded 12 incidents in the European pharmaceutical industry and seven at companies that manufacture medical devices or other medical products. This is about the same as the previous year. Ransomware incidents at medical device suppliers or IT service providers can be risky as they may also have access to healthcare facilities' networks and systems. Table 1 shows the impact on Dutch healthcare facilities hit by ransomware via a supplier in 2022.

Table 1

Impact on Dutch healthcare facilities due to ransomware attacks on healthcare facility suppliers in 2022

Product/service affected business	Impact healthcare facility
Apothecary software	Postponed maintenance
Accounts payable/invoicing	Several days of no-invoicing
Websitehosting	Website offline for several hours
Authentication solution	Dataleak
Diagnostics	Deferred maintenance
Property	Dataleak
Primary-care automation	Business not accessible

Specialised products

Some companies supply specialised products, such as dialysis fluid and oxygen. If this supplier cannot deliver these products for an extended period due to a ransomware incident, things can become tense for healthcare facilities. Therefore, supplier management needs to focus on companies providing digital services and those providing products that are not easily replaced by alternatives.

Ransomware incidents at healthcare facilities due to abuse of supplier accounts

Ransomware incidents sometimes occur in organisations because a ransomware operator piggybacks on a supplier's access to its customers' network. Some examples that Z-CERT encountered over the past two years include:

- A supplier has an 'open connection' to a healthcare facility. An attacker can use the VPN connection to reach a healthcare facility's file server and encrypt it using ransomware.
- In a major European manufacturer, the ransomware operator enters the network via a supplier. The supplier has high-level privileges and a lot of room to navigate within the network, allowing the hacker to lock down a large part of the IT infrastructure by activating ransomware.
- A municipality falls victim to a large ransomware incident partly because multi-factor authentication is missing on a compromised supplier account [14].

Recommendations

Suppliers should be 'ransomware-resistant' and follow recommendations as defined by Z-CERT in the chapter ransomware and the resources we refer to.

As for suppliers accessing your network, there are several lessons to be learned from the incidents described above.

- A sound privilege access management solution and process are necessary if you give suppliers access to your network. A solution like this allows a supplier to request access and only get the access required for as long as needed. In addition, activities are logged.

  Evidence from healthcare facilities shows positive results in migrating their suppliers to privilege access management solutions. So, if your organisation does not yet implement this method, there are benefits in doing so.

- An attacker entering through the supplier should not be able to infiltrate the network any further. Z-CERT notes that while network segmentation is often present, it is not always set up in such a way as to stop an attacker.

- Supplier accounts should not be safeguarded from multi-factor authentication.

threat

DDoS

Threat estimate: medium

Z-CERT estimates the threat level for DDoS attacks on healthcare facilities at 'medium' and expects a few low-impact DDoS incidents within a year. However, this could rapidly change due to developments within the conflict between Russia, Ukraine and its allies.

Incidents

Four incidents that appeared to directly target healthcare facilities were reported to Z-CERT in 2022. The DDoS attacks had little impact. Firewalls were overloaded and there was temporarily no access to webmail. No internet traffic was possible at one healthcare facility; at another, the remote accesss solution was temporarily unavailable.

Compared to other sectors, the healthcare sector is relatively unaffected by targeted DDoS attacks [15]. What is the reason? Many DDoS attacks are conducted by cybercriminals with financial gain as their motive. For a company offering services or products over the internet, the financial impact of a DDoS attack may be significant, but for healthcare organisations, the impact is often minor. As a result, they are a less attractive target [16].

Another motive for a DDoS attack could be 'revenge' by a disgruntled client, patient or (former) employee. A youth welfare facility reported to Z-CERT an example of an attack possibly initiated by a disgruntled client. There are hardly any technical hurdles when executing a DDoS attack: anyone can buy a DDoS attack online. An attack is cheap if a website has no mitigating procedures, costing about $50 for a 24-hour attack [17]. These are relatively simple attacks where the website receives a high number of requests. Professional attacks that involve sending very high amounts of data traffic and testing mitigating procedures are more costly. These run into thousands of euros [18]. Due to the high cost, this type of attack is less likely to occur.

Regarding DDoS, the biggest threat to the healthcare sector this year came from pro-Russian hacktivists. In the spring of 2022, they launched DDoS attacks targeting mainly NATO countries and Ukraine. Banks, aviation, railways, the energy sector, logistics and technology companies, and also the government were especially targeted.

Z-CERT noted that healthcare facilities and healthcare-related organisations were also targeted by these hacker groups [19] [20]. A hospital from Eastern Europe confirmed to Z-CERT that a DDoS attack was executed. That attack was repelled. In addition, threats were made to eight UK hospitals in September 2022 [19]

Our analysis is that the target selection seems quite random. Attacks often take place when countries are negatively highlighted in the Russian news. The moment the Netherlands were to receive negative coverage in Russian media, the possibility of DDoS attacks would also target healthcare facilities. In addition, healthcare facilities may experience inconvenience if the IT-service providers they use are attacked.

> **“There is a perception that DDoS attacks are not particularly powerful”**

Techniques

Regarding pro-Russian hacktivist groups, the level of attacks and the methods used can vary, depending on the services or tools used. Generally, the perception is that the attacks are not particularly powerful [21] and can be mitigated with the right resources. On average, attacks on the network layer have a volume between 40-100 Gbps with a duration of one to two days [22]. Application-level attacks have also been observed when websites were targeted [25]. These types of attacks require other mitigating measures [26].

For more technical details on the attacks seen from pro-Russian hacktivist groups, Z-CERT refers to Italy’s national CERT analysis [27] (translation: [24]).

Recommendations

- For recommendations on both organisational and technical levels, Z-CERT would like to denote the following NCSC fact sheets.
  - Factsheet Continuity of online services [28].
  - Factsheet Technical measures for continuity of online services [26].

- For an example of a basic DDoS response plan, Z-CERT would like to refer to the NCSC UK example [29].

threat

DDoS attacks on suppliers

Threat estimate: medium

Z-CERT estimates the threat level for DDoS attacks on suppliers to be 'medium' and expects a few incidents impacting healthcare facilities within a year. However, the threat level may rise quickly due to geopolitical developments within the conflict between Russia and Ukraine.

Incidents and impact

Of the healthcare facilities surveyed, 9 per cent experienced disruption due to DDoS attacks launched against suppliers. This number is almost half that of 2021. In recent years, healthcare facilities have experienced disrupture from DDoS attacks on the following types of suppliers:

1. Authentication providers

Patients or clients cannot log into their designated portals because the pre-requisite authentication does not work. At some healthcare facilities, this prevents patients from accessing the link required for video calls.

2. DNS-providers

Two DNS providers were hit by a DDoS attack in 2022. For a healthcare facility, this means that services can no longer be accessed through their domain name. In practice, this often involves the healthcare organisation's website, patient-client portal or home office.

3. Suppliers hosting web applications in the cloud (SaaS suppliers)

More and more healthcare facilities are buying web applications in the cloud. HR systems, healthcare planning, ERP system and the electronic patient or client file. In two cases in the past two years, an electronic client file was unavailable for several hours due to a DDoS attack on the supplier.

4. Internet service providers (ISPs)

Attacks on these types of suppliers do not only affect a healthcare facility's internet connection. The effects can also be indirect if, for example, an internet service provider of a SaaS supplier is attacked.

24

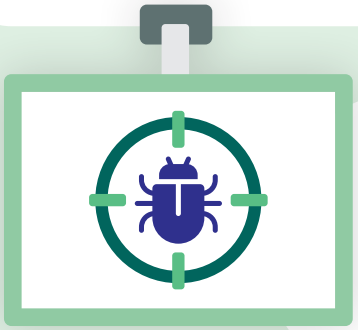


Table 1

Type of suppliers of Dutch healthcare facilities that suffered a DDoS attack in 2022

Organisation type	Impact
IT provider	Temporary inertia of healthcare organisation's systems
Electronic client portal	Several hours of application unavailability
Internet provider	No internet
DNS provider	Websites not accessible, patient portal not accessible
Authentication provider	The hospitals portal not available, video call with patient not possible, not possible to log onto website
SaaS application	Application offline

Trends and techniques

In relation to supplier management, it is good to know which sectors are often targeted by DDoS attacks. International threat reports show that specific sectors are at higher risk of falling victim to network-level DDoS attacks. Healthcare-relevant sectors where this frequently occurs include telecom and IT service providers, web hosting companies and data processing services [30] [31].

Z-CERT does not have a comprehensive overview of the Netherlands on DDoS statistics for each sector it does, however, for ISPs. Where Z-CERT received only four reports of targeted DDoS attacks for healthcare, the National Internet Providers Management Organisation (NBIP) registered 2001 [32]. While these numbers were lower than the previous year, they were higher than in 2020. It demonstrates that specific types of suppliers to healthcare facilities are far more likely to be attacked than the healthcare facility themselves.

DDoS attacks on suppliers

There is no total overview of the number of DDoS attacks worldwide. Most sources report an increase in DDoS attacks in 2022 compared to 2021 [33] [35]. Unlike 2021, 2022 also saw a lot more DDoS incidents caused by pro-Russian and pro-Ukrainian hacktivists. This makes comparison with the previous year more difficult. From an analysis of threat reports from Cloudflare, the number of reports of DDoS attacks in which cybercriminals demand money seems to have remained fairly steady compared to 2021 [34]. The number of reported attacks demanding money from cybercriminals increased every quarter in 2022 [34].

With regard to the trends in techniques, extensive reports are available that you can submit to your supplier [31] [34]. An eye-catching trend in the use of attack techniques seems to be that DDoS attacks are becoming longer and more powerful. NBIP indicates that there is a trend of using multiple attack methods [36].

Z-CERT did not see any targeted DDoS attacks on the Netherlands by pro-Russian hacktivists in 2022. As discussed in the previous chapter, this may soon change given the conflict between Ukraine and Russia. IT service providers have also been attacked in the past [20].

Recommendations

- Assess external vendors' resilience against different types of DDoS attacks. For questions you can ask your supplier see, for example, the NCSC factsheet called "Continuity of online services" [28].
- Lay down agreements about DDoS mitigation in a Service Level Agreement.
- Include DDoS attack scenarios in your business continuity plan.
- Determine which services it is advisable to purchase from multiple suppliers. For example, if your Internet connection is important for critical processes, it may be advisable to have a backup Internet connection.
- You can optimise some services against DDoS attacks. For DNS, for example, see SIDN's article called "Choosing TTL values for DNS records: how does one proceed? " [37].

> **An eye-catching trend in the use of attack techniques seems to be that DDoS attacks are becoming longer and more powerful**

threat

Data leaks due to malware, credential phishing or hacking

Threat estimate: medium to high

Z-CERT estimates the threat level for data breaches in healthcare caused by malware and credential phishing as 'medium' and current. This means that incidents in this category involving a data breach are expected in the short term. Z-CERT estimates the threat level for data breaches in healthcare caused by hacking to be high. Z-CERT expects several data leaks caused by hacking within a year. In these cases, the impact will often be higher than with a phishing incident because more sensitive data is captured.

There are different ways in which data breaches occur. In this threat assessment, Z-CERT zooms in on the data leaks that occurred due to the cyber incidents: credential phishing, malware or hacking.

Incidents

The number of data breaches that were reported to us through the survey that were the result of credential phishing, malware or hacking, remained restricted. Only 5 percent of respondents reported a data breach. This is relatively low. The low percentage can be explained by the fact that many healthcare institutions use multi-factor authentication. This is evidenced by the fact that 22 percent of the surveyed institutions reported an incident where malicious parties managed to steal the password or other information, but where the incident did not always lead to a data breach. Preparatory activities that could lead to data breaches were detected by half of the healthcare institutions surveyed.

In addition, Z-CERT suspects that not every data breach is actually detected. A successful malware infection, for example, is not associated with data breaches by every IT helpdesk, which means that it is not always investigated whether data has been stolen. Stealing the contents of emails is a basic functionality of widely used malware [38]. In addition, knowledge and logging must also be present to be able to determine a data breach.

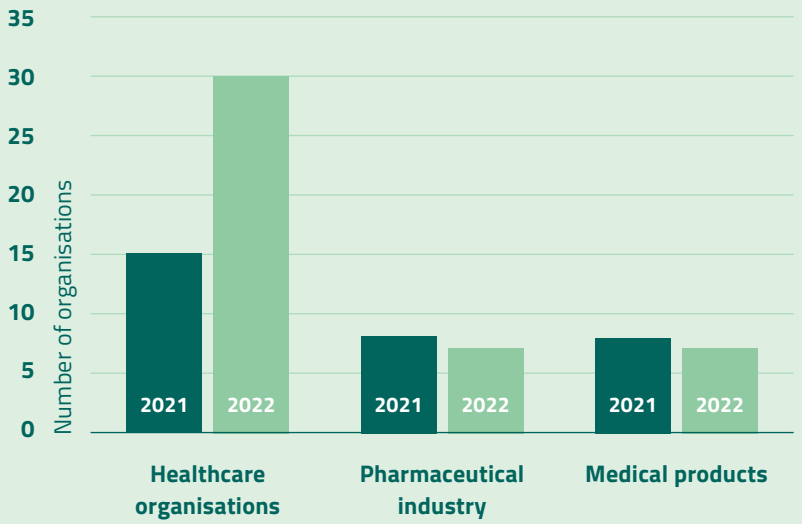
Extortion by threatening to leak data

A major concern for security professionals is the groups of cybercriminals who steal data to blackmail organisations. They threaten to leak sensitive data if the victim does not pay. This often goes hand in hand with ransomware, but not always. There are also some active groups that omit ransomware altogether and only threaten to leak data.

28

Figure 5

Number of European organizations that were published in 2022 on data breach websites



As Figure 5 shows, the number of incidents at European healthcare institutions seemed to be increasing, but remained fairly steady for the pharmaceutical industry and manufacturers of medical products. Data from Dutch healthcare institutions has also been leaked in these types of incidents.

Data breaches at suppliers and partners

A source of data breaches that do not occur at the healthcare institution itself are hacked mailboxes of partners, suppliers or fellow healthcare institutions. If a mailbox of such a relation is hacked, the mail is often stolen. The content of this email is then used by the cybercriminal to send phishing mail. Because the phishing mail contains trusted content, the recipient is more inclined to click on the malicious links or to launch the attached malware.

Monthly campaigns were reported to Z-CERT in which malicious emails were sent to sometimes dozens of healthcare institutions. Organisations that still do not require multi-factor authentication for their mail access increase the risk of security incidents in healthcare. According to Z-CERT, such organisations should be made aware of this.

> **“Organisations that do not yet require multi-factor authentication for access to their webmail should be made aware of this”**

This type of data breach is often not aimed at extorting organisations. They are caused by cybercriminals gaining access to systems or usernames and passwords and then selling that data on the dark web.

Script kiddies

In addition to cybercriminals, there are also hackers in the 'script kiddies' category. These are often young people who find it exciting to hack. Things got out of hand in 2022 when a 19-year-old boy exploited a vulnerability in a system of a digital healthcare platform [39] and, according to news media, gained access to the sensitive data of twenty healthcare institutions [40].

Scriptkiddies sounds like a 'derogatory' term, and can therefore be seen as a smaller risk by some, however the level can vary greatly from one individual to another. Often they do not operate as an organised business like ransomware operators, but are hobbyists instead. They usually do not oversee the consequences of their actions for their victims. And they do not always realise that they are committing criminal offences.

Techniques and trends

International research shows that data breaches in healthcare are increasingly occurring due to attacks on web applications [15]. These are usually basal attacks. For example, the attacker uses stolen passwords or exploits known vulnerabilities or misconfigurations. Because healthcare organisations increasingly purchase their web applications in the cloud, this is a point of attention for healthcare.

How do these actors steal passwords? Of course, there are the default methods, like trying passwords that have been leaked from website data breaches (e.g. the data breach at Dropbox and LinkedIn). However, not everyone knows that many of these stolen passwords have been stolen using malware. Research in 2022 showed that 675,000 passwords were stolen from Dutch computers within seven months by using malware [41].

The combination of poor security against malware and the lack of multi-factor authentication for web applications is a serious risk. In addition, malware can also piggyback on existing web browser sessions by stealing certain cookies. In some cases, this can even lead to a cybercriminal temporarily gaining access to a web application, even if multi-factor authentication is enabled [42]. A recent example of this is the hack on a software development platform, where the hacker gained access to the platform in this way despite the fact that multi-factor authentication was enabled [43].

> **"The combination of poor protection against malware and the lack of multi-factor authentication for web applications is a serious risk"**

Multi-factor authentication

Multi-factor authentication works extremely well against most attacks that require a login with a username and password. However, examples appeared in the press this year in which hackers succeeded in circumventing traditional multi-factor authentication methods [44] [45]. Z-CERT has not yet identified such attacks in the Dutch healthcare sector. It is good to keep an eye on developments in this area.

APIs

What is increasingly being reported to Z-CERT are vulnerabilities and misconfigurations in APIs (application programming interface). Software such as web applications and mobile apps communicate with each other through these APIs. If not configured properly, this can lead to data leaks. In December 2022, an ethical hacker was able to access more than 15,000 usernames and other GP data using a poorly configured API [46]. Incidents were also reported at Z-CERT where access to patient data could also be obtained.

Recommendations

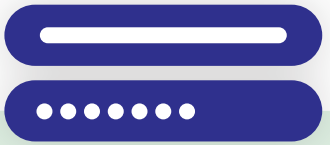
- As far as suppliers of web applications (SaaS suppliers) are concerned, Z-CERT recommends careful selection of software suppliers of web applications and, in particular, selecting suppliers that have a thorough Security Development Lifecycle (SDL). As part of this lifecycle, pentests are performed and a supplier uses guidelines for the safe development of software. For example, the guideline drawn up by the National Cyber Security Center (NCSC) [47].
  A well-known model for an SDL that you can use is the one developed by Microsoft [48].

- When assessing the security of, for example, mobile and web applications, pay attention to the APIs that the applications use. It often happens that these API endpoints are insufficiently secured. Another point of attention here is how the software handles passwords and other credentials. Z-CERT notes that some software vendors store the credentials for accessing these APIs in configuration files or in source code. In a number of cases, the credentials were therefore accessible from the internet. Credentials should be stored in a specially designed secure area (often referred to as "vault").

- Check whether your authentication provider offers functionality that prevents hackers from circumventing the multi-factor authentication method used. Microsoft has e.g. options available that make so-called "MFA fatigue attacks" more difficult [49]. In addition, Microsoft (and many other providers) offers so-called "phishing resistant" MFA, a method that can withstand advanced phishing attacks where the attacker also tries to evade MFA [50].

  In the factsheet "Mature authenticating" of the NCSC, different multi-factor authentication methods are compared and the advantages and disadvantages are discussed [51]. Maturity levels are also defined.

- For recommendations that protect against malware, Z-CERT refers you to the recommendations in the ransomware chapter.



threat

Cyber espionage by state actors

Threat estimate: high

Z-CERT estimates the threat level for cyber espionage by state actors differently for different types of organisations. Z-CERT estimates this threat as 'high' for healthcare organisations where extensive scientific research is carried out that is relevant to state actors. The high threat is caused by the attackers having a high level, a lot of patience and a lot of money to complete their missions. In addition, the defensive capabilities of healthcare organisations are not sufficient to keep these types of attackers out.

For organisations that do not conduct scientific research and do not have clients or patients of interest to state actors, the threat is still a potential threat. A potential threat can quickly develop into a concrete threat. The moment your organisation - for whatever reason - becomes interesting for a state actor.

Incidents

Z-CERT reported one incident in 2021 in which the digital traces point to a Chinese state actor. Further investigation did not seem to indicate a targeted attack. Although Z-CERT has not observed any digital espionage activities, recent examples are known from other countries [52]. This means that such attacks are also conceivable for our country. In addition, state actors are very good at covering tracks and "staying under the radar", so there is a chance that healthcare institutions and Z-CERT will not detect everything.

Are you a target?

There are a number of goals that state actors want to achieve:

- **Gathering knowledge and technology.**
  This can give them an economic advantage [53]. In addition, China, for example, wants to become less dependent on the West in terms of knowledge and skills. They have the ambition to become world leaders in certain fields such as biotechnology and neuroscience. Organisations conducting extensive (applied) research are therefore interesting [54]. Recent observed espionage campaigns by Chinese state actors have focused on infectious disease research, genomics and medical technology [52]. In the past there was also a lot of interest in research into chronic diseases such as cancer [55].

- **Collection of personal data in bulk [53] [55].**
  A large dataset can be useful, for example, if a country wants to conduct research into a specific target that appears in the data set. A recent example of such activity is the hack on the Red Cross in which sensitive personal information of 515,000 people was captured [56]. Data from 4600 Dutch people also leaked here. It is not possible to say with 100 procent certainty that this hack was carried out by a state actor, but it certainly looks like it.

  The AIVD indicates that it has not seen this type of information gathering in the Netherlands before, and cites medical institutions as an example of an attractive target [53].

- **Gathering information about (former) citizens who have emigrated to another country.** They like to keep a finger on the pulse and even undertake influence and interference activities [57]. Refugees and dissidents from the country can also be of interest. A healthcare institution with information about important targets could be interesting.

- **Proactively create access to organisations where scientific research is conducted.** They can use this access at a subsequent stage if it suits the attackers [54].

Methods and techniques

- A well-known method used by state actors is to exploit vulnerabilities for which there is not yet a patch (zero-day vulnerability). For example, this year a vulnerability in Log4j was used to gain access to organisations [49].

- Compromising suppliers is a common method of gaining quick access to multiple organisations. The best-known example is the hack on Solarwinds, which probably gave Russian state actors access to various Dutch healthcare institutions, including hospitals and mental healthcare institutions. However, it seems that these healthcare facilities were not a direct target, but rather a by-catch.

- If you travel to a risk area, it is known that data from data carriers is stolen by state actors. Knowledge Transfer Desk has drawn up guidelines that help prevent these kinds of scenarios [57].

Recommendations

- Do you want to determine whether you are vulnerable to digital espionage? The AIVD has created a document called “espionage vulnerabilities investigation manual” that can help you with this [58]. This is not just about technical matters, but also about identifying what kind of information may be of interest to a state actor.

- Digital espionage is not limited to a hacker trying to penetrate an organisation’s IT infrastructure from the outside. It is known that states also purposefully send students, researchers and employees to foreign institutions with the assignment to undertake espionage activities [57]. For questions in the field of international cooperation and security, please contact the knowledge security desk. The product called “National Knowledge Security Guide for Safe International Collaboration” [57] was also published this year by this desk, which helps you to weigh up the opportunities and the associated risks against each other.

threat

Financial Fraud

Threat assessment: medium

Z-CERT estimates the threat level for financial fraud by using digital media such as mail and WhatsApp at 'medium'. Z-CERT expects digital fraud attempts in the short term and a number of successful fraud attempts this year. Most participants estimate the damage they experience as a result of financial fraud using digital means as 'limited'. Z-CERT emphasizes that the amounts involved can sometimes be high. In the previous edition of the threat assessment, we mentioned an example of an attempted fraud in which people tried to steal 150,000 euros.

Incidents

In 2022, there were many financial fraud attempts involving the use of digital resources. In many cases, these attempts consisted of sending fraudulent emails, but WhatsApp and SMS were used as well.

CEO Fraud

This is a form of fraud in which a manager is imitated and in which the attacker tries to persuade an employee of the organisation to transfer an amount. Of the surveyed participants, 40 percent have detected attempted CEO fraud (so the total amount could be higher). Attempted CEO fraud succeeded with 2 percent of surveyed participants.

Malicious invoices or changing bank accounts

Of the surveyed participants, 28 percent detected fraudulent invoices or a fraudulent attempt to have an account number changed. 2 Percent of the surveyed participants reported a successful attempt.

Methods and techniques

The people behind these fraud attempts often use the same techniques. Employees are asked to transfer money for gift cards. Attacks can be more sophisticated. Then, for example, a fake domain name is created resembling the domain name of the healthcare institutions. Items can then be ordered for thousands of euros.

Often, the attacker appears to pull people's names from LinkedIn. For example: look up a director of a healthcare institution and an HR employee on LinkedIn. Create an email address and send an email, supposedly on behalf of the director, to the real email address of the HR employee with the request to adjust the bank account before the next salary payment. Such attacks do not always use social media as a source. This year there was only one case where an employee's new job was not yet known on social media. Also, CISOs were imitated for the first time. This is beyond the standard 'gift card fraud' because specific knowledge is used.

A common problem is that legitimate email addresses are often used. For example, a Gmail or a Hotmail address. A spam filter generally doesn't pick out these legitimate-looking emails because they don't contain any malware or malicious links. Therefore, the email will most likely reach a healthcare employee.

Recommendations

- Implement email standards (SPF, DKIM and DMARC). If these are missing, it becomes very easy for an attacker because they can then email with the real email address of a CEO. In 2021, this happened at one organisation because an error was made when implementing these standards and a cybercriminal could pose as a colleague. For more information: [59].

- Monitor for 'look-a-like' domain names that may be misused for criminal purposes. Many security providers already do this and there are free tools available that offer this feature. See for example: [60].

- Register financial fraud attempts and include them in the security reports. 4 percent of those surveyed did not record attempted fraud. Statistics in this area help with security awareness training and demonstrate the importance of taking preventive measures against this threat.

- Security awareness training on this subject is important because technical measures are not very effective with this type of fraud. The financial department, but also other departments with payment powers, are important in this respect. However, every employee should be taught this because especially in the case of gift card fraud, an employee is tempted to advance money from their personal assets.

- Internal authorisation procedures and processes must be set up in such a way to prevent fraud. For example, one healthcare institution reported that maleficent attempts to change bills were unsuccessful because employees have to do this themselves in a dedicated portal. The fact that a financial or HR employee cannot and is not allowed to do this ensures that this type of fraud does not occur in this organisation.

- Create a procedure for employees to report attempted financial fraud. In addition, there must also be a culture that if there is any doubt as to whether a report is legitimate or not, someone within the organisation or a manager can be contacted. Employees must experience room to report matters, without feeling that they will be punished if they make an error of judgment.

- Financial fraud is an important issue in supplier management. It is not always the healthcare institutions that 'fool for it'. The suppliers are also tempted to send items to an address where the package can easily be intercepted by the criminal. Therefore, make good agreements with the supplier for changing email addresses, account numbers and delivery locations. In addition, only invoices that are submitted through the agreed procedures may be processed.

theme

Developments with opportunities for hackers and healthcare providers

Developments are taking place in society, but certainly also in healthcare, such as the increase in working from home or a shortage of staff. In this chapter, we take a closer look at a number of trends and examine which threats are linked to these developments. The aim of this is that healthcare providers are aware of the opportunities that a development can offer attackers. Healthcare providers can also incorporate these insights into their risk analyses and supplier management. Some developments may also offer opportunities for healthcare institutions to increase resilience.

Development/Threat	Ransomware	Ransomware suppliers	DDoS	DDoS suppliers	Data leaks	Financial fraud	Espionage
Transition to the cloud		x	x	x	x		x
Professionalization of cybercrime	x	x		x	x		
Russia-Ukraine conflict			x	x			x
Staff shortage	x				x	x	x
Lack of security awareness	x				x	x	x
IT and security staff shortage	x		x		x	x	x

Table 1

Overview of the developments and threats involved

Trend: transition to the cloud

Healthcare is digitising and is increasingly dependent on the cloud. This growing dependency was particularly noticeable in the following categories:

1. Remote consultations

Many healthcare institutions are focusing on remote consultations using cloud solutions. For example, the Dutch Association of Hospitals (NVZ) reported that in the first quarter of 2022, almost 28 percent of all outpatient care was handled digitally [61]. Many healthcare institutions have set themselves the goal of carrying out more consultations by means of video calls [62]. In addition to video calling, people can also often ask questions in a portal, app or secure email [63].

> **“Many healthcare institutions are focusing on remote consultations using cloud solutions”**

2. Remote patient monitoring

Many hospitals are fully committed to remote patient monitoring [62]. It is expected that the global market, worth USD 1.2 billion in 2021, will be worth USD 4.1 billion in 2028 [64]. Because patients are monitored remotely, the solution often depends on the cloud. The patient can perform measurements himself using a medical device and send them together with a questionnaire in an app. Certain matters can also be monitored by means of sensors and measurement results can be automatically forwarded to practitioners [65].

3. Care domotics

The care domotics market is growing [66]. The ‘middleware’ part of smart automation solutions is increasingly being purchased in the cloud. In the middleware part, data is stored and alarms are routed [66]. Many care domotics solutions play a daily role in the care for often tens of thousands of clients [66].

Domotica, for example, is widely used in elderly care, care for the disabled, and mental health care for the safety or convenience of the patient or client. It is a technology that fulfills a task in and around the home. The applications are endless. For example, it is possible to monitor whether medicines have been taken, an alarm has sounded if someone falls and the location of a person with dementia is monitored. Smoke detectors and cameras are also examples of domotics.

4. Migration to cloud services

Most healthcare organisations are increasingly switching to cloud services for the applications they use. These are often business support applications, but also electronic client files. Especially in youth care, GGD, care for the disabled and care for the elderly, there is often a ‘cloud unless’ policy, which focuses mainly on Software as a Service (SaaS services). Hospitals are often more conservative, but more and more cloud services are also being purchased there. In addition, a lot of infrastructure is being moved to the cloud. Sometimes the healthcare institution even feels compelled to go to the cloud because the application in question can only be purchased in the cloud. Healthcare institutions are also experiencing great ‘pressure’ from major suppliers to go to the cloud.

developments with opportunities for hackers and healthcare providers

Opportunities for attackers:

- The market for digital products and services in the cloud is growing. This means that there are opportunities and new companies are being set up to provide specialised services for, for example, telemonitoring or domotics. In addition, there are software suppliers who feel compelled by the market to offer their application in the cloud. Without having experience in managing and securing a cloud service.

  In practice, maturity in terms of information security and cyber security is not always sufficient for these types of companies, which increases the risk of cyber incidents.

- Concentrating data from healthcare providers with the same suppliers means that one incident can have an impact on multiple healthcare institutions and sometimes thousands of clients. This makes these suppliers an attractive target for cybercriminals. For such a supplier, a high level of cybersecurity maturity is essential. In May 2022, the United States, the United Kingdom, Canada, Australia and New Zealand warned that threat actors are paying increased attention to managed service providers who, for example, manage cloud solutions [67].

- Healthcare institutions are highly dependent on their internet connection due to the purchase of cloud applications. If the internet connection does not work e.g. due to a DDoS attack on the external firewall, the healthcare institution may not have access to the applications in the cloud.

- Software hosted in the cloud presents new risks such as vulnerabilities and misconfigurations that can often be exploited from the internet in this new situation. Poorly secured APIs are a particular concern.

- A software solution that runs in the cloud often depends on several suppliers. For example, a video call solution sometimes requires a login to a portal. An identity provider is used for logging in. In addition, a DNS provider is required to surf to the URL and there is a supplier who provides hosting and connectivity. Last year, Z-CERT saw incidents at all these points in the chain, as a result of which a digital service from a healthcare provider could not be used or was reduced.

Opportunities for healthcare institutions:

- Where fast patching is sometimes a challenge for a healthcare institution, this is often safe with cloud solutions by large cloud suppliers.

- Some cloud solutions offer extensive information security and cybersecurity functionality.

- Mature cloud services can reach a high level of maturity in terms of the security of their own infrastructure, beyond what a healthcare institution could deliver on its own.

Professionalised cybercrime

Cybercrime groups are well organised and work together to increase effectiveness. This means that these cybercrime groups can deal with dozens and sometimes more than a hundred ransomware incidents per month. Because cryptocurrencies can be collected anonymously, this ecosystem of cybercrime will continue to exist. In addition, an organised "ransomware as a service" group lowers the threshold for getting started as a new cybercriminal. The large amounts that are earned also have a drawing effect on new recruits.

Cybercriminals create user-friendly tools to automatically exploit vulnerabilities, often reselling this access. Automation means that a healthcare institution that does not patch on time is often automatically compromised. This also applies to the distribution of malware and misuse of stolen passwords. Where multi-factor authentication and protection against malware is not optimal, a healthcare organisation runs the risk that a hacker gains access to its systems. The obtained access can be misused for various purposes.

Lack of security awareness among employees

Many participants report that awareness is a concern. Many employees work in healthcare who are naturally inclined to help. The statement 'I like people not computers' is one that many healthcare workers recognise. An underlying problem for a lack of security awareness is that some employees have limited digital skills. Working on digital skills and security awareness often go hand in hand.

In addition, there is sometimes a high turnover among healthcare personnel or temporary workers are employed. Due to the workload, in combination with the temporary nature of the employment, there is no time or capacity to offer these employees adequate security awareness training. A lack of security awareness generates opportunities for cybercriminals in the field of financial fraud, data breaches and ransomware.

Geopolitical developments

The conflict between Russia and Ukraine has had no impact on healthcare in the Netherlands in the past year. However, several healthcare institutions in Europe suffered from DDoS attacks that were undertaken by pro-Russian hacktivists. We will discuss this further in the DDoS chapter.

Suppose the conflict escalates and the Netherlands becomes directly involved in the conflict, Z-CERT mainly expects a current threat to healthcare from pro-Russian hacktivists. Z-CERT does not expect that Dutch healthcare will immediately become a target for state actors. In the case of attacks initiated by state actors, there will be a risk of collateral damage that can arise, for example, if internet service providers or energy suppliers are attacked. This mainly concerns DDoS attacks, attacks with ransomware and wiper software. Malware that is distributed by state actors affiliated with Russia and unintentionally ends up at healthcare organisations could also cause incidents. Examples from the past are the attacks with the NotPetya malware that probably accidentally hit hospitals in the US [52] and the Solarwinds hack that had an unintended impact on several Dutch healthcare institutions.

The supply chain turned out to be vulnerable in 2022 because several pro-Ukrainian hacktivists introduced malicious code in widely used open-source software components [68]. In one case, this unintentionally led to data loss at an aid organisation that hosted its servers in Belarus. Managing this 'third party components' is a topic for supplier management with software vendors.
Outside the conflict between Russia and Ukraine, there were also examples of open-source components being modified with malware [69] [70] or fake versions of existing components being distributed.

Working from home
Since corona, working from home has become very normal. Working from home has changed a few things.

- Some employees have received authorisations that they did not have before corona, but now need them because of working from home. The authorizations were not withdrawn after corona because the way of working seems to have changed permanently. In the event of a security incident, an attacker may have more access to sensitive data than before.
- More people are using remote access solutions than before corona. This increases the chance that an attacker can obtain credentials for remote access. In the event of a DDoS attack, there will also be an impact on more users than before.
- In the workplace, contact frequencies are greater and things are shared more quickly. When people work from home, it is less obvious to have a colleague take a look at a suspicious email or share information about phishing campaigns. This increases the chance that a phishing attack or attempted CEO fraud will succeed.

IT staff shortage and security
Healthcare institutions report that it is difficult to find IT and security staff due to shortages in the labour market. Nor are they always able to offer competitive wages. This means that healthcare institutions do not always have enough qualified security personnel. This can lead, among other things, to security reports not being dealt with in time, patching not being carried out on time and growth in maturity stagnating. Some healthcare facilities have noticed the same problem with suppliers and are concerned about it.

The attack possibilities that staff shortages trigger can vary per institution. However, because it often has an impact on multiple aspects of an organisation's resilience, the risk of various types of incidents will be increased.

“ Because staff shortages often have an impact on multiple aspects of an organisation’s resilience, the risk of various types of incidents will be increased ”

theme

Evaluating the Log4j crisis

Log4Shell, the vulnerability in the Apache Log4j logging tool, hardly needs any introduction. This vulnerability caused quite a stir in late 2021 and in 2022. The vulnerability exploited functionality in Log4j that attempted to enrich logging data. This allowed an attacker to 'instruct' the Log4j module to retrieve and execute malicious commands. To avoid reinventing the wheel, many software developers use Log4j to handle the logging part. As a result, Log4j was present in many applications and the attack surface was large.

Impact

Because of the large attack surface, the chance of abuse was higher and the risk therefore greater. Large-scale misuse was therefore taken into account. In practice, however, this turned out not to be too bad. Although there have been incidents reported by healthcare institutions using Log4Shell as an attack vector, this has remained with a few. There was one incident that had significant impact and in another serious incident the impact was limited because they were caught in time.

Many cybersecurity parties were very concerned about the possible impact of the vulnerability in Log4j. The amount of applications that use Log4j is large, and the vulnerability allowed an attacker to join 'Remote Code Execution'. This allows an attacker to give commands to a computer as if he were sitting in front of it. On top of that came the uncertainty about which applications used which versions of Log4j. This combination of factors created the conditions for a 'perfect storm'.

Why has there been no large-scale misuse?

Misuse has remained limited because many healthcare institutions have responded adequately by quickly taking preventive measures and patching. Many healthcare institutions set up a crisis organisation to monitor the situation. In addition, exploiting the vulnerability was made more difficult because the vulnerability was contained in a logging module. Depending on the configuration of systems, logging is not always handled on the system where the application is running. Because the actually vulnerable, underlying systems were often not accessible to the internet, the vulnerability could not be abused. In other cases, attackers received signals that an attack or reconnaissance was successful, but this did not come until many hours later, from unexpected places. In many cases, this meant that attackers were hindered.

However, a number of solutions turned out to be designed in such a way that they were very suitable for abuse if they were made accessible to the internet.

Over time, users of these products have seen more widespread abuse by both ransomware and state actors worldwide. This led to security incidents in both foreign healthcare institutions and in the two aforementioned incidents in the Netherlands.

Lessons learned

Although Log4j is used in many applications, this was not often very clear. Applications are usually built with the reuse of components, but insight into which components are all used is by no means always a habit. Therefore, there are supply chain risks. Fortunately, we are working hard on solutions in this regard. One of the best candidates for this is the so-called Software Bill of Materials (further, SBoM). This standard prescribes a list of components used in a structured, agreed format. The use of this standard can be very useful in the context of vulnerability management.

Z-CERT therefore also calls on developers of software and hardware to use the SBoM, and motivates healthcare institutions to request use in their relationship with suppliers. to make the SBoM.

Evaluation

In the absence of a high adoption rate of the SBoM, the effort of the NCSC and its partners was a welcome addition during the Log4j crisis. A publicly available Github page kept track of which suppliers did (not) use Log4j. However, this was easier with regular software and hardware than with suppliers of medical software and hardware. It is therefore desirable to further strengthen ties with these parties in order to support healthcare institutions more specifically.

In addition to the reports from suppliers themselves, various parties scanned for vulnerable systems. Thanks to an ever-increasing degree of information sharing among cybersecurity parties in the Netherlands, which Z-CERT values as very positive, healthcare institutions could be informed more quickly about vulnerable systems. In order to be able to contribute even more actively to this, Z-CERT is working on the implementation of scan tooling.

> **“Thanks to an ever-increasing degree of information sharing, healthcare institutions could be informed more quickly about vulnerable systems”**

Summary

The greatest threat to the healthcare sector lies in disruptions caused by ransomware infections at a healthcare institution itself or at an IT supplier of the healthcare organisation. Suppliers of healthcare institutions are affected more often than healthcare organisations themselves. In the coming year, Z-CERT expects a number of ransomware incidents in the supply chain that will have an impact on Dutch healthcare institutions.

Z-CERT registered 65 percent more ransomware incidents at European healthcare institutions last year than a year earlier. In the Netherlands, Z-CERT has seen at least five ransomware incidents at healthcare organisations. That is the same number as in 2021. One difference is that the impact on the total number of healthcare institutions experiencing nuisance in the Netherlands was much greater in 2022.

There is also a high risk of data leaks in healthcare as a result of hacking. Data leaks that occur due to attacks on web applications are particularly common. For example, the attacker uses stolen passwords or exploits known vulnerabilities or misconfigurations. Because healthcare organisations increasingly purchase their web applications in the cloud, this is a point of attention for healthcare. Most attacks that require login with a username and password can be effectively stopped by using multi-factor authentication.

Data in healthcare is often sensitive. Security professionals are therefore concerned about the groups of cybercriminals who steal data to extort organisations. They threaten to leak sensitive data if the victim does not pay. This often involves ransomware attacks, but it can also involve extortion in which cyber criminals threaten to shut down an organisation with a DDoS attack.

However, the risk of systems or services in healthcare failing due to DDoS attacks does not seem that great. Z-CERT received only three reports of targeted DDoS attacks on healthcare. However, there is a risk that healthcare institutions will suffer from DDoS attacks that have been carried out on suppliers, such as cloud providers or hosting and internet service providers. It is striking that the conflict between Russia and Ukraine has hardly had any impact on healthcare in the Netherlands in the past year.

Another threat is cyber espionage by state actors. This is especially a risk for healthcare organisations where a lot of scientific research is conducted that is also relevant for state actors. Examples include large amounts of personal data or specific knowledge and technology.

Finally, financial fraud poses a real threat to healthcare. The best-known form of this is CEO fraud. While many of these fraud attempts are blocked in time, 2 percent of healthcare institutions surveyed by Z-CERT report that a CEO fraud attempt was successful. The amounts that organisations lose as a result can quickly add up to 150,000 euros. Because technical measures are not always sufficient to stop such attacks, attention to security awareness training is of great importance.

The increasing digitisation of healthcare and the movement of applications to the cloud offers new opportunities for healthcare institutions and patients and clients. This is a good development as long as healthcare providers are aware of the security risks and take sufficient mitigating measures.

Bibliography

[1] **Colloseum Dental**, *"Informatiepagina cyberincident augustus 2022,"* [Online]. Available: https://www.colosseumdental.nl/mededeling-cyberincident.

[2] **Secutec**, *"Hackers show remorse after attack on Flemish facility for people with disabilities,"* 1 Maart 2022. [Online]. Available: https://secutec.eu/hackers-show-remorse-after-attack-on-flemish-facility-for-people-with-disabilities/.

[3] **Sophos**, *"The State of Ransomware in Healthcare 2022,"* Sophos, 31 Mei 2022. [Online]. Available: https://news.sophos.com/en-us/2022/06/01/the-state-of-ransomware-in-healthcare-2022/.

[4] **Microsoft**, *"Cyber Signals: 3 strategies for protection against ransomware,"* 30 Augustus 2022. [Online]. Available: https://www.microsoft.com/security/blog/2022/08/30/cyber-signals-3-strategies-for-protection-against-ransomware/.

[5] **Coveware**, 26 Oktober 2022. [Online]. Available: https://www.coveware.com/blog/2022/10/26/q3-2022-quarterly-report.

[6] **Kaspersky**, *"Common TTPs of modern ransomware groups,"* 23 Juni 2022. [Online]. Available: https://go.kaspersky.com/rs/802-IJN-240/images/Common-TTPs-of-the-modern-ransomware_low-res.pdf.

[7] **Sami Laiho**, *"AppLocker whitelisting vs. blacklisting,"* 10 Juni 2020. [Online]. Available: https://4sysops.com/archives/applocker-whitelisting-vs-blacklisting/.

[8] **ACSC**, *"Microsoft Office Macro Security,"* Oktober 2021. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/publications/microsoft-office-macro-security.

[9] **ACSC**, *"Hardening Microsoft 365, Office 2021, Office 2019 and Office 2016,"* Januari 2022. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/publications/hardening-microsoft-365-office-2021-office-2019-and-office-2016.

[10] **Redcanary**, *"Why so, ISO? Mark-of-the-Web, explained,"* 3 November 2022. [Online]. Available: https://redcanary.com/blog/iso-files/.

[11] **Jan Hanstede**, *"Detectie van ransomware,"* 2020. [Online]. Available: https://www.z-cert.nl/kennisbank/ransomware-logging/.

[12] **Z-CERT**, *"Tien gouden tips tegen ransomware,"* 12 Oktober 2021. [Online]. Available: https://www.z-cert.nl/wp-content/uploads/2021/02/Z-CERT_FactsheetRansomware_2560x1920px_04-1.pdf.

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

[14] **Hunt & Hackett BV**, *"Red Mudnester: Rapportage,"* 4 Juli 2022. [Online]. Available: https://openpub.buren.nl/wp-content/uploads/2022/07/20220701_Red-Mudnester_Report_v3.0_Publiek.pdf.

[15] **Verizon**, *"2022 Data Breach,"* 2022. [Online]. Available: https://www.verizon.com/business/resources/reports/dbir/.

[16] **NBIP**, *"DDoS-aanvallen steeds vaker onderdeel van bredere aanval,"* Juli 12 2022. [Online]. Available: https://www.nbip.nl/nieuws/ddos-aanvallen-q2-2022/.

[17] **Privacy Affairs**, *"Dark Web Price Index 2022,"* 19 September 2022. [Online]. Available: https://www.privacyaffairs.com/dark-web-price-index-2022/.

[18] **Netscout**, "*findings from 2nd half 2021 - netscout threat intelligence report,*" 2021. [Online]. Available: https://www.netscout.com/sites/default/files/2022-03/ThreatReport_2H2021_WEB.pdf.

[19] **Z-CERT**, Telegram kanaal van de pro-Russische hacktivisme groep Phoenix, 2022.

[20] **Z-CERT**, Telegram kanaal van de Pro-Russische hacktivisme groep *"Killnet"*, 2022.

[21] **FBI**, *"Hacktivists Use of DDoS Activity Causes Minor Impacts,"* 4 November 2022. [Online].

[22] **SingCERT**, *"Dangers and implications of Hacktivism during the Russia-Ukraine Conflict,"* 7 April 2022. [Online]. Available: https://www.csa.gov.sg/singcert/Publications/dangers-and-implications-of-hacktivism-during-the-russia-ukraine-conflict.

[23] **B. Toulas**, *"Russian hacktivists launch DDoS attacks on Romanian govt sites,"* 29 April 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/russian-hacktivists-launch-ddos-attacks-on-romanian-govt-sites/.

[24] **Digital shadows**, *"Killnet: The Hactivist Group That Started A Global Cyber War,"* 8 juni 2022. [Online]. Available: https://www.digitalshadows.com/blog-and-research/killnet-the-hactivist-group-that-started-a-global-cyber-war/.

[25] **Sysdig**, *"2022 Sysdig Cloud Native Threat Report,"* 2022. [Online]. Available: https://sysdig.com/wp-content/uploads/2022-cloud-native-threat-report.pdf.

[26] **NCSC**, *"Factsheet Technische maatregelen voor continuïteit voor online diensten,"* 14 Maart 2016. [Online]. Available: https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-technische-maatregelen-voor-continuiteit-van-online-diensten.

[27] **CSIRT-ITA**, *"Attacco DDoS ai danni del sito istituzionale dello CSIRT Italia.,"* 31 Mei 2022. [Online]. Available: https://www.csirt.gov.it/contenuti/attacco-ddos-ai-danni-del-sito-istituzionale-dello-csirt-italia-del-30-maggio-2022-analisi-preliminare-bl01-220531-csirt-ita.

[28] **NCSC**, *"Factsheet Continuïteit van online diensten,"* 14 Maart 2016. [Online]. Available: https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-continuiteit-van-onlinediensten.

[29] **NCSC UK**, *"A minimal Denial of Service (DoS) response plan,"* 20 Januari 2019. [Online]. Available: https://www.ncsc.gov.uk/collection/denial-service-dos-guidance-collection/a-minimal-denial-of-service-response-plan.

[30] **O. Yoachimik**, Cloudflare, 12 Oktober 2022. [Online]. Available: https://blog.cloudflare.com/cloudflare-ddos-threat-report-2022-q3/.

[31] **Netscout**, *"DDoS THREAT INTELLIGENCE REPORT (1st half 2022),"* 2022. [Online]. Available: https://www.netscout.com/threatreport/.

[32] **NBIP**, [Online]. Available: https://www.nbip.nl/nieuws/. [Accessed https://www.nbip.nl/nieuws/ Januari 2023].

[33] **Imperva** , *"81% Increase in Large-Volume DDoS Attacks,"* 27 September 2022. [Online]. Available: https://www.imperva.com/blog/81-increase-in-large-volume-ddos-attacks/.

[34] **Cloudlare**, *"Cloudflare DDoS threat report for 2022 Q4,"* 10 Januari 2022. [Online]. Available: https://blog.cloudflare.com/ddos-threat-report-2022-q4/.

[35] **Cloudflare**, *"Cloudflare threat rapports of Q1, Q2, Q3 and Q4 2022,"* 2022.

[36] **NBIP**, *"Cijfers DDoS-aanvallen in het vierde kwartaal 2022,"* 18 Januari 2022. [Online]. Available: https://www.nbip.nl/wp-content/uploads/2023/01/NBIP%20-%20Infographic%20-%20DDoS%20data%20-%20Q4%202022%20%5BNL%5D.pdf.

[37] **G. Moura**, *"TTL-waarden voor DNS-records kiezen: hoe doe je dat?,"* SIDN, 17 September 2019. [Online]. Available: https://www.sidnlabs.nl/nieuws-en-blogs/ttl-waarden-voor-dns-records-kiezen-hoe-doe-je-dat.

[38] **Kaspersky**, *"QakBot technical analysis,"* 2 September 2021. [Online]. Available: https://securelist.com/qakbot-technical-analysis/103931/.

[39] **Nedap**, *"Beveiligingsincident Carenzorgt.nl,"* 2022 Oktober 2022. [Online]. Available: https://nedap.com/wp-content/uploads/2022/10/Persbericht-Beveiligingsincident-Carenzorgt.nl_.pdf.

[40] **Security.nl**, *"Zorginstellingen melden datalek na inbraak bij digitaal zorgplatform Carenzorgt,"* 2 November 2022. [Online]. Available: https://www.security.nl/posting/773253/Zorginstellingen+melden+datalek+na+inbraak+bij+digitaal+zorgplatform+Carenzorgt.

[41] **Security.nl**, *""Criminelen stelen 675.000 wachtwoorden van Nederlandse computers","* 23 November 2022. [Online]. Available: https://www.security.nl/posting/775361/%22Criminelen+stelen+675_000+wachtwoorden+van+Nederlandse+computers%22.

[42] **Sophos**, *"Cookie stealing: the new perimeter bypass,"* 28 Augustus 2022. [Online]. Available: https://news.sophos.com/en-us/2022/08/18/cookie-stealing-the-new-perimeter-bypass/.

[43] **Security.nl**, *"Inbraak CircleCI via gestolen '2FA-backed' SSO-sessie van laptop engineer,"* 16 Januari 2023. [Online]. Available: https://www.security.nl/posting/781495/Inbraak+CircleCI+via+gestolen+%272FA-backed%27+SSO-sessie+van+laptop+engineer.

[44] **Bleepingcomputer**, *"MFA Fatigue: Hackers' new favorite tactic in high-profile breaches,"* 20 September 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/mfa-fatigue-hackers-new-favorite-tactic-in-high-profile-breaches/.

[45] **Bleepingcomputer**, *"Microsoft accounts targeted with new MFA-bypassing phishing kit,"* 3 Augustus 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/microsoft-accounts-targeted-with-new-mfa-bypassing-phishing-kit/.

[46] **J. Bouman**, 22 December 2022. [Online]. Available: https://twitter.com/JonathanBouman/status/1603158320365420544.

[47] **NCSC**, *"ICT-beveiligingsrichtlijnen voor webapplicaties,"* 1 September 2015. [Online]. Available: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties.

[48] **Microsoft**, *"What are the Microsoft SDL practices?,"* [Online]. Available: https://www.microsoft.com/en-us/securityengineering/sdl/practices. [Accessed 7 December 2022].

[49] **Microsoft**, *"Defend your users from MFA fatigue attacks,"* 28 September 2022. [Online]. Available: https://techcommunity.microsoft.com/t5/

microsoft-entra-azure-ad-blog/defend-your-users-from-mfa-fatigue-attacks/ba-p/2365677.

[50] **Microsoft**, *"Conditional Access authentication strength (preview),"* 12 Januari 2023. [Online]. Available: https://learn.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-strengths.

[51] **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.

[52] **American Hosptial Association**, *"Agencies alert health care sector to commonly exploited cyber vulnerabilities,"* 7 Oktober 2022. [Online]. Available: https://www.aha.org/news/headline/2022-10-07-agencies-alert-health-care-sector-commonly-exploited-cyber-vulnerabilities.

[53] **2022**, *"Dreigingsbeeld Statelijke Actoren 2 November 2022,"* 28 November 2022. [Online]. Available: https://www.rijksoverheid.nl/documenten/rapporten/2022/11/28/tk-bijlage-dreigingsbeeld-statelijke-actoren-2.

[54] **M. N. AIVD**, *"Dreigingsbeeld statelijke actoren,"* 3 Februari 2021. [Online]. Available: https://www.rijksoverheid.nl/documenten/rapporten/2021/02/03/dreigingsbeeld-statelijke-actoren.

[55] **FireEye**, *"Beyond Compliance: Cyber Threats and Healthcare,"* 2020. [Online]. Available: https://content.fireeye.com/cyber-security-for-healthcare/rpt-beyond-compliance-cyber-threats-and-healthcare.

[56] **ICRC**, *"Cyber-attack on ICRC: What we know,"* 16 Februari 2022. [Online]. Available: https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know.

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

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

[59] **NCSC**, *"Factsheet Bescherm domeinnamen tegen phishing,"* 28 Oktober 2015. [Online]. Available: https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-bescherm-domeinnamen-tegen-phishing.

[60] **CIRCL**, *"typosquatting finder,"* [Online]. Available: https://typosquatting-finder.circl.lu/.

[61] **ICThealth**, *"Factsheet NVZ: 28% poliklinische zorg is digitaal,"* 26 Juli 2022. [Online]. Available: https://icthealth.nl/nieuws/factsheet-nvz-28-poliklinische-zorg-is-digitaal/.

[62] **NVZ**, *"NVZ Factsheet digitale zorg,"* Juni 2021. [Online]. Available: https://nvz-ziekenhuizen.nl/sites/default/files/2022-10/NVZ%20Factsheet%20Digitale%20Zorg%20juni%202021.pdf.

[63] **Zorgenablers**, *"Remote Consultation,"* 24 November 2021. [Online]. Available: https://zorgenablers.nl/remote-consultation/.

[64] **Zorg Enablers**, *"Remote Monitoring,"* 23 11 2022. [Online].

Available: https://zorgenablers.nl/remote-monitoring/.

[65] **VGZ**, *"Explosieve groei opschaling digitale zinnige zorg,"* 2021. [Online]. Available: https://www.cooperatievgz.nl/cooperatie-vgz/nieuws-en-media/nieuwsoverzicht/explosieve-groei-opschaling-digitale-zinnige-zorg.

[66] **M&I/Partners**, *"Domotica-leveranciers in perspectief,"* 2022. [Online]. Available: https://mxi.nl/uploads/files/publication/domotica-leveranciers-in-perspectief-2022.pdf.

[67] **CISA**, *"Protecting Against Cyber Threats to Managed Service Providers and their Customers,"* 11 Mei 2022. [Online]. Available: https://www.cisa.gov/uscert/ncas/alerts/aa22-131a.

[68] **Bleepingcomputer**, *"BIG sabotage: Famous npm package deletes files to protest Ukraine war,"* 9 Januari 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/big-sabotage-famous-npm-package-deletes-files-to-protest-ukraine-war/.

[69] **Bleepingcomputer**, *"Dev corrupts NPM libs 'colors' and 'faker' breaking thousands of apps,"* 9 Januari 2022. [Online]. Available: https://www.bleepingcomputer.com/news/security/dev-corrupts-npm-libs-colors-and-faker-breaking-thousands-of-apps/.

[70] **ITPro**, *"Open source packages with millions of installs hacked to harvest AWS credentials,"* 24 Mei 2022. [Online]. Available: https://www.itpro.co.uk/security/hacking/367776/open-source-packages-hacked-to-harvest-aws-credentials.

[71] **Kaspersky**, *"DDoS attacks in Q3 2021,"* 7 November 2022. [Online]. Available: https://securelist.com/ddos-report-q3-2022/.

[72] Overzicht cyberincidenten, 2022. [Online]. Available: https://www.datalekt.nl/home/overzicht-cyberincidenten/.

[73] **M. Ulikowski**, *"dnstwist,"* 2022. [Online]. Available: https://github.com/elceef/dnstwist.

[74] **FBI**, *"Hacktivists Use of DDoS Activity Causes Minor Impacts,"* 4 November 2022. [Online]. Available: https://www.ic3.gov/Media/News/2022/221104.pdf.

[75] **Enisa**, *"ENISA Threat Landscape for Ransomware Attacks,"* 29 Juli 2022. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-ransomware-attacks.

[76] **CIS**, *"CIS Benchmarks,"* [Online]. Available: https://www.cisecurity.org/cis-benchmarks/. [Accessed 14 December 2022].

[77] **R. Janssen, H. Prins, A. van Hout, J. Nauta, M. Hettinga, L. van der Krieke and S. Sytema**, *"Videoconferencing in Mental Health Care,"* in eTELEMED 2015 : The Seventh International Conference on eHealth, Telemedicine, and Social Medicine, 2015.

[78] *"U.S. Declares Start of Russia's Invasion of Ukraine, Introduces Sanctions; "Cyber Shields Up," Says CISA,"* The American Hospital Association, 23 Februari 2022. [Online]. Available: https://www.aha.org/advisory/2022-02-23-us-declares-start-russias-invasion-ukraine-introduces-sanctions-cyber-shields.

Glossary

2FA
(See Two-Factor Authentication)

Attack
Action in which someone deliberately tries to disable or bypass security to get into a digital system.

Attacker
Someone who deliberately tries to disable or bypass security to get into a digital system.

Attack Surface
The part of IT systems that an attacker can reach to target their attacks.

Actor
Person, group or organisation that threatens to attack a digital system. Examples are: script kiddie, hacktivist, malicious employee, hostile state (state actor) or a cybercriminal (criminal actor).

Administrator
Administrator of a computer system or computer network. This person has more rights compared to an ordinary user. For example, he can adjust settings and he determines what users in a computer network are allowed to do and what not.

API
Application Programming Interface. A program that allows applications to communicate with each other without people controlling it. Commonly used methods over the Internet are, for example, SOAP and REST.

APT
Advanced Persistent Threat, i.e. the constant threat from an advanced adversary. These are in particular hostile states (state actors). Cyberattacks are used where the attacker is in an information system for a longer period of time, without being noticed. Or he tries to access certain information in the system in all sorts of ways for a long time. The attacker often wants to use this to steal information or to shut down the network at a certain point. An APT differs from an ordinary threat by the attacker's motive, tenacity and sometimes also the chosen means.

Artificial intelligence (AI)
Also called AI. Technology that allows a system to mimic human thinking so that it can independently perform certain human tasks.

BEC
Business E-mail Compromise, or an incident where the attacker has penetrated an organisation's mail environment. The attacker can use this access to steal confidential information or to carry out new attacks, supposedly on behalf of (someone representing) an organisation. An example of this is CxO fraud.

Botnet
A network of computer systems that perform malicious tasks on their own, such as sending spam or carrying out a DDoS attack. A command-and-control server controls this network.

CEO fraud (also known as CxO fraud)
Form of fraud in which an attacker sends emails to a finance department purporting to be on behalf of a company's CEO or CFO. The attacker wants to convince or pressure an employee of the financial department to transfer money.

CISM
Certified Information Security Manager.

CISO
Chief Information Security Officer.

Code injection
A certain type of attack on an insecure part of an application. In doing so, the attacker changes something in the code of the system that causes the program to work differently. Example of a injection code is SQL-injection.

Credentials
The data that allows a user or other computer system to prove to a computer system that it is who it says it is. For example, a user name in combination with a password or a code sent through an SMS text message.

Cross site scripting
Common flaw in a website that could allow an attacker to access data or functionality not intended for them.

CVE
Cybersecurity Vulnerabilities and Exposures - list of public vulnerabilities. (https://cve.mitre.org/cve/).

Cybersecurity
The set of measures to reduce relevant risks to an acceptable level.
The measures can be aimed at preventing cyber incidents or at discovering cyber incidents, limiting the damage or making it easier to recover after an incident.

CxO Fraud
See CEO fraud.

DDoS
Distributed Denial-of-Service. Attacks in which digital services are rendered inaccessible to users. DDoS services can be easily and cheaply terminated through the internet (dark web) and often make use of so-called botnets consisting of IoT devices.

Defacing
Defacing a website to post your own message. Often used by hacktivists.

Digital security
The undisturbed functioning of information and process control systems, information processed and stored by them and services and processes dependent on them.

Digital process
A process that is carried out in whole or in part by the complex and interrelated interaction between people and many components such as hardware, software and/or networks. This term also includes fully automated processes, such as process control systems.

Disruption
An obstacle in the availability, integrity or confidentiality of information (processing). In other words: failure of digital processes or parts thereof.

Endpoint security
Security of end systems (PCs, laptops, tablets, etc.) - not limited to antivirus, but also, for example, data-leak protection (DLP).

Exploit
Method (program or code) hackers use to exploit a vulnerability.

Hacking
'Hacking' is when an actor has managed to breach the security and perform actions on the system for which the actor is not authorised.

Hacktivist
Someone who carries out digital attacks to promote a certain ideology.

Immutable back-up
A backup file that cannot be changed so that an attacker cannot encrypt it.

Incident
An event that compromises the availability, authenticity, integrity or confidentiality of data stored, transmitted or processed or of the services offered by or through network and information systems.

Initial access
The attacker gains initial access to the victim, often an account of an employee of an organisation within a specific application or on a specific server. To this end, tools are used that automatically scan for weaknesses in systems. (Spear)phishing is also widely used.

Malware
Malicious software that attackers put on a digital system in order to access it remotely, destroy it or steal information. Malware is a contraction of the English 'malicious' and 'software'.

Multi-factor authentication (MFA)
See two-factor authentication (2FA).

Outage
A situation in which one or more digital processes are disrupted due to natural or technical causes or due to human error.

Patch
New version of software or firmware by the manufacturer. Fixes known vulnerabilities, possibly provides new security and additional features.

Phishing
Attack in which the attacker tricks someone into providing important information, such as login details or credit card details. Phishing often happens through emails. But attackers also do it over the phone, text or app message.

Privileged Access /account
Account on a digital system that gives more rights to do certain things. For example, files and settings change. In Windows systems this account is called the administrator or administrator, in Unix and Linux systems the root.

Responsible disclosure
Action whereby one or more discovered vulnerabilities are responsibly disclosed. Usually, the vulnerability is first reported to the owner of the system where it was found so that the vulnerability can be fixed.

Risk
The chance that a threat will lead to a cyber incident and the impact of the cyber incident on interests, both in relation to the current level of digital resilience.

SaaS (Software-as-a-Service)
A form of outsourcing services. With SaaS, software is offered as an online service. In the same way we also speak of, for example, IaaS (Infrastructure as a Service), PaaS (Platform as a Service) and DRaaS (Data Recovery as a service).

SBoM
Software Bill of Materials (SBoM). A list of which version of components are included in the software.

Security by design
Enforcing, both technically and organisationally, careful handling of data from the design phase of a system.

Spear phishing
A phishing attack targeting a specific person. Sometimes the attack is also specially adapted for this person. This makes it very difficult to identify the phishing attack.

State actor
A country that uses digital means of attack for espionage and sabotage and/or for spreading disinformation.

Threat
A cyber incident that may occur or a combination of simultaneous or consecutive cyber incidents.

Two-factor authentication (2FA), also known as multi-factor authentication (MFA)
A method to determine whether a user or digital system is who or what he says he is. You use different ways to do this. For example, a password and a code that the user receives by SMS text message. Or a combination of a fingerprint and a password.

Vulnerability scan
Vulnerabilities Scan - An automated check that detects vulnerabilities in a system.

Wiper software
A variant of malware that damages or deletes essential files on a computer, causing the computer to stop working.

Zero-day attack
Attack or method of attack that exploits a vulnerability (the zero-day vulnerability) that is not yet known to others (such as a vendor or user), resulting in no patch is available yet.

Acknowledgment

We thank everyone who contributed to the production of this Cybersecurity Threat Assessment for Healthcare, including a number of reviewers of healthcare institutions, CISOs from various healthcare institutions and suppliers.

We also owe a special thanks to the **Financial ISAC and TNO** for using their model, which is based on the FAIR (Factor Analysis of Information Risk) framework (https://www.fairinstitute.org).

And finally, we would like to thank **Artiënne Buissant des Amorie** of Artgen for drawing up the threat assessment.

Questions or remarks?
info@z-cert.nl
033 737 06 09

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

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