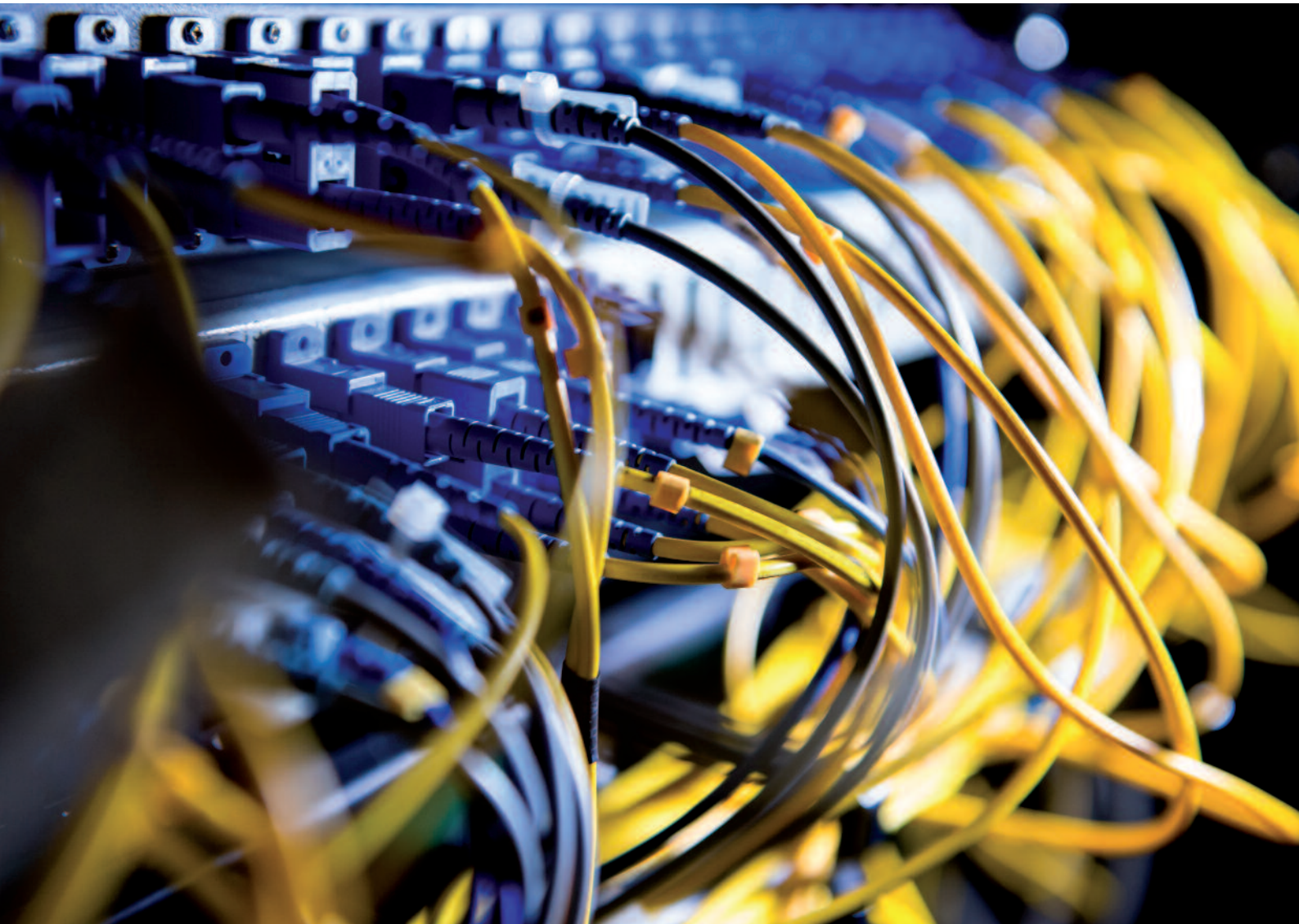
National Coordinator for Security and Counterterrorism
Ministry of Justice and Security

Cyber Security Assessment Netherlands

CSAN 2018



Publication details

The Cyber Security Assessment Netherlands (CSAN) 2018 offers insight into threats, interests and resilience in the field of cyber security in relation to national security. The CSAN is published annually by the National Coordinator for Security and Counterterrorism.

The National Coordinator for Security and Counterterrorism (NCTV) protects the Netherlands against threats that could disrupt society. Together with its partners within the government, the academia and the business sector, the NCTV ensures that the Dutch critical infrastructure is safe and remains so.

The National Cyber Security Centre (NCSC) is the central information hub and centre of expertise for cyber security in the Netherlands. The NCSC is working towards increasing Dutch society's resilience in the digital domain, and towards a safe, open and stable information society. The NCSC is part of the National Coordinator for Security and Counterterrorism.

The CSAN has been written by the NCTV and the NCSC based on insights and expertise from government services, organisations in the critical processes, the academia and other parties. The NCTV has gratefully used their expertise and information both during expert sessions and during validation.

Table of Contents

Attackers are successful due to a lack of basic measures

Cyber security under pressure

The Cyber Security Assessment Netherlands (CSAN) 2018 offers insight into threats, interests and resilience in the field of cyber security in relation to national security. The CSAN is published annually by the National Coordinator for Security and Counterterrorism and is written in cooperation with public and private partners.

Sabotage and disruption by nation-states are the most significant threats to national security

Nation-states are perpetrating an increasing number of digital attacks on other countries, organisations or individuals for geopolitical motives. Their objective is to acquire strategic information through espionage, to influence public opinion or democratic processes, or even to sabotage critical systems. Digital attacks by nation-states have been observed over the last year. It is of note that simple attack techniques have been successfully deployed and that Dutch IT infrastructure has been exploited to perpetrate attacks on other countries.

Major incidents show that the attackers do not anticipate or may even be willing to accept the collateral damage caused by their actions. Abroad, the collateral damage has resulted in social disruption and it has led to economic damage in the Netherlands. Vulnerability to espionage, disruption and sabotage is growing due to the dependence on foreign parties. In certain countries, foreign parties may be legally obliged to work in support of operations such as espionage or preparations for sabotage.

Professional criminals are continuing to develop in the digital field. The threat is increasing as a result. Tools that allow less well-equipped attackers to easily perpetrate digital attacks are being supplied through a professional criminal service sector.

Attackers continue to be successful due to a lack of basic measures

The digital resilience of the Netherlands is under pressure. Organisations are being successfully attacked using simple methods. As the recent period has shown, incidents could have been prevented and damage mitigated with basic measures. Many organisations fail to implement these measures. Among other things, shortcomings in configurations and the failure to implement security updates in a timely fashion mean that attackers are successful.

Resilience is under further pressure from the increasing complexity and connectivity of the IT landscape and in some cases by too little attention to cyber security. At the same time, insecure products and services lower the threshold for attackers. Across the globe, there have been various instances of supply chains being exploited to perpetrate attacks. This has also led to damage in the Netherlands.

The sustained functioning of society and the economy depends on cyber security

Cyber security is needed for the functioning of the highly digitised Dutch society and economy and as a barrier against digital threats. The consequences of attacks and systems failures can be severe and may even disrupt society. The costs and benefits of cyber security do not always lie with the same party; this is part of the reason why parties make concessions on the interests of digital security. This has associated risks at national level and can have far-reaching consequences. Confidence in the digital society is undermined by, among other things, successful digital attacks. Theft of valuable information can damage confidence in economic activity and could potentially damage the Dutch economy. Espionage, disruption and sabotage by nation-states undermine Dutch interests.

The digital threat is permanent. Cyber attacks continue to be profitable, low-threshold and involve little risk for attackers. Within the context of recent geopolitical developments, nation-states are expected to continue using such digital attacks and may even opt to do so on a greater scale. In combination with far-reaching and increasing digitisation of society, this fits in with the move towards a further increase in the risk of social disruption.

Reader's guide

The CSAN 2018 offers insight into threats, interests and resilience in the field of cyber security in relation to national security. Cybersecurity is the entirety of measures to prevent damage caused by disruption, failure or misuse of ICT and to recover should damage occur.[1] Such damage may consist of any or all of the following: reduced reliability of ICT, limited availability and violation of the confidentiality and/or integrity of information stored in the ICT systems.

The CSAN has been written based on insights and expertise from government services and organisations in critical processes, the academia, and other parties. The developments are described in a qualitative form. Where available in a reliable form, they are substantiated by a quantitative foundation or reference to sources.

Monitoring threats, interests and resilience is a continuous process, with the CSAN being one of the annual results. Matters that have not or have barely changed with respect to the previous editions of the CSAN have been described in brief or not at all. The analysis in the CSAN is based on the triangle of threat, interest and resilience. These three factors together determine the risk.

The questions central to the CSAN 2018 are:

- What are the threats that could impair the confidentiality, integrity, and availability, of information, information systems or information services, or impaired them in the reporting period May 2017 to April 2018 inclusive? What are the threats that pose the most significant risk to national security?
- What are the potential consequences for national security if identified threats manifest themselves?
- What combinations of vulnerabilities and tools manifested themselves globally in the reporting period May 2017 to April 2018 inclusive and (could) be used in the Netherlands?
- To what extent is the Netherlands and the national security of the Netherlands resilient against tools that have been or could be used and the manifestation of the threats?
- To what extent can underlying causes or factors that form the basis of the threat assessment be identified?

Chapter 1 sets out the key issues, the underlying causes and factors that form the basis for the threat assessment. Chapter 2 explains the threat in more detail and clarifies it. The interests of society and national security are set out in Chapter 3. The fourth chapter contains the annual overview of the reporting period May 2017 to April 2018 inclusive and aims to explain the most relevant developments. The resilience of the Netherlands is covered in the fifth and final chapter. Finally, the appendices provide an overview of the incidents handled by the NCSC and an explanation of the abbreviations used.

Figure 1 **Interest, threat and resilience model**

Cyber attacks are usually profitable, low-threshold and involve little risk for actors

1 Key issues

The threat assessment is based on six key issues which mutually affect each other. A cyber attack is usually profitable, low-threshold and involves little risk for the actor. The easy accessibility of attack tools and the use of insecure products and services are reasons for this low threshold. Conflicts of interest lead to concessions on resilience. The increasing complexity and connectivity put resilience under further pressure. Finally, foreign producers and service providers have a positive as well as negative effect on resilience.

Cyber attacks are usually profitable, low-threshold and involve little risk for actors

Regardless of the motive – personal, economic, ideological or geopolitical – for many years now a cyber attack has been a profitable way for actors to achieve a variety of objectives. The continually growing digitisation increases the potential damage an actor can affect by means of a digital attack and increases the benefit they can achieve from it.

Many forms of digital attacks can be perpetrated at a low threshold as a result of the fundamental causes set out below. As a result an attacker does not, by any means, need to personally have significant capabilities for an attack. Even actors who do have these capabilities can often make do with simple forms of attack.

In many cases, a digital attack can be perpetrated with little risk. There is a chance of an attack remaining undetected for a long time. If the attack is discovered, attribution to and detection of the actors is complex.[2] Even if attribution is possible, in many cases this remains without consequences, certainly in the case of state or state-sponsored actors. A turning point does appear to have been reached in governments' publicly attributing digital attacks. Various countries have attributed attacks to other countries.

Attack tools are easily accessible through attack facilitators

Digital attacks can be perpetrated at a low threshold using the services of attack facilitators. These service providers make infrastructure, tools and techniques for digital attacks available for hire. This allows less-experienced or more poorly equipped actors to perpetrate digital attacks. The low-threshold accessibility of attack tools leads to an increase in the threat.

Insecure products and services are the Achilles' heel of cyber security

Digitally insecure products and services are a fundamental cause of many incidents.[3] Insecure products and services lower the threshold because they make it easier for attackers to successfully perpetrate attacks. The lack of security can occur because suppliers do not or no longer provide updates or these updates are not easy to install. Even if they are available, they are not always used by organisations. There is very little economic stimulus for producers to produce secure hardware and software. Because of this, there is a conflict of interest between on the one hand the producers' economic interests and the cyber security interests of society on the other hand.

Conflicts of interest lead to concessions

In a broader sense too, conflicts of interest lead to concessions on cyber security interests. Members of the public, businesses, sectors and the government will always have to conduct a balancing exercise. After all, cyber security measures cost time and money, scarce resources that could also be used elsewhere. Occasionally, the interest of digital security is a direct extension of other interests; conflicts arise occasionally. They arise within organisations, conflict between ease-of-use for the individual and the cyber security interest, for example, but they also arise between organisations. One of the reasons for this is an unequal division of costs and benefits.

Increasing complexity and connectivity puts resilience under pressure

The greater the complexity and connectivity, the more challenging it becomes to realise a resilient digital infrastructure. On the one hand, the organic growth and relative long service life of systems

lead to a more complicated landscape. On the other hand, the increasing use of shared facilities, such as cloud services, in the form of individual building blocks, means that it is more difficult to maintain oversight. Where in the past services were set up within an organisation, now they are often contracted-in from various parties and implemented externally. Control of the IT landscape remains within the organisation, while the implementation becomes fragmented across a number of parties. This situation creates new dependencies and increases the scope for attack.

The digital infrastructure is complex, not all essential components are equally robust and there is a high dependence on individual components. Developers and suppliers use certain software generically as building blocks for their own work. Some popular protocols for data exchange via the Internet are decades old and are not resistant to contemporary attacks.

Foreign producers and service providers have positive as well as negative effects on resilience

Dutch organisations are highly dependent on a limited number of foreign suppliers of products and services. Although these companies have more resources at their disposal to arm themselves against attacks, the social impact of disruptions is significant because many different services depend on a small number of providers.

In addition to being disrupted, the products or services from foreign suppliers can also be compromised by actors without the knowledge of this supplier. Furthermore, producers and service providers are subject to the laws and regulations of the country in which they have a branch. Governments abroad could force them into some form of cooperation on, for instance, political, military or economic intelligence operations. If governments decide to accept products and services from their own country or allies only, this will lead to fragmentation of the Internet.

Nation-states pose the most significant digital threat

2 Threats

The digital threat is permanent. Digital attacks by state actors with the objective of espionage, influencing, disruption and sabotage, form the most significant digital threat to national security. In addition, the activities of cybercriminals have a major impact. There seems to have been no fundamental change to the threat landscape over the past year. However, it does seem to have become more diverse as result of a number of shifts, some of which originated several years ago. The threat matrix in this chapter shows the complete threat assessment. In addition, the most striking elements of the threat assessment are examined.

The lines between actors are blurring

The number of actors perpetrating digital attacks has increased over the past few years.[4] There are also actors currently active in the digital domain who had no meaningful role in years gone by.[5] It is relatively easy for them to employ capabilities because of the increasing accessibility of tools for perpetrating digital attacks.

To make the threat assessment clearer, a distinction is made between various categories of attackers, each of which has their own working methods and motives (see the threat matrix). In practice, the lines between the various actors are becoming less apparent.[6] For instance, different groups of actors can use the same tools and techniques. One of the reasons for this is the trickle-down effect, where high-quality attack techniques become widely known or fall into the wrong hands. An example from 2017 is the tools that are attributed to the American National Security Agency (NSA) which were leaked by the Shadow Brokers hacker group. A specific tool (ExternalBlue exploit) was then used in the WannaCry attack.[7]

Another example of the blurring of the lines are the seemingly technical similarities between the Petya ransomware and the NotPetya sabotage software. The media reported examples of actors attacking another hacker group and making off with their proceeds.[8] Nowadays, attack tools are spreading across the entire spectrum of attackers, from nation-states to criminals. The lines between actors continue to blur, partly as a result of various groups of actors collaborating, actors intentionally impersonating someone else, or by creating false leads to other actors.[1]

Identifying the actor behind a digital attack, which is referred to as attribution, is even more complex when the actors are difficult to separate from each other. The level of sophistication of an attack and the tools that were used are factors affecting the number of leads for identifying the actor. The blurring of lines between actors results in a greater probability of incorrect attribution, possibly with major consequences, such as for instance further escalation in a conflict situation.[9]

1 A recent example of a false flag operation is a cyber attack on the organisers of the Olympic Games in South Korea, where the impression was created that the attack came from North Korea. As a result of the attack, the Olympic Games website went down, and broadcasting channels were not working. In open sources, the attack was attributed to Russia, possibly motivated by their exclusion from the Olympic Games due to the doping scandals.

Threat matrix

The threat matrix provides insight into the threats originating from various actors against various targets. The table is not exhaustive and does not contain all threats that are imaginable, but limits itself to the threats where it is estimated that actors have sufficient intention and tools or where activities have been observed previously. The threat matrix has undergone a number of conceptual changes in relation to previous years. On the one hand, critical processes and providers have been added as separate target categories. On the other hand, the actor typology has been modified.[II] The following threats can be distinguished:

- Disruption: the intentional, temporary impairment of the availability of information, information systems or information services.
- Sabotage: the intentional, very long term impairment of the availability of information, information systems or information services, possibly leading to destruction.
- Information manipulation: intentionally changing information; impairing the integrity of the information.
- Information theft: impairing the confidentiality of information by copying or removing information.
- Espionage: impairing the confidentiality of information by state or state-sponsored actors copying or removing information.
- System manipulation: impairing information systems or information services; targeting the confidentiality or integrity of information systems or information services. These systems or services are then used to perpetrate other attacks.
- Breakdown/failure: impairment of the integrity or availability as a result of natural, technical or human failures.
- Leak: impairment of confidentiality as result of natural, technical or human failures.

	Government	Critical	Private organisations	Members of the public
Nation-state/ state-sponsored	Espionage Information manipulation	Sabotage Disruption Espionage	Espionage System manipulation	Espionage
Criminals	Disruption System manipulation Information theft	Disruption System manipulation	Information theft Information manipulation Disruption System manipulation	Information manipulation Disruption System manipulation Information theft
Terrorists	Sabotage	Sabotage		
Hacktivists	Disruption Information manipulation	Disruption Information manipulation	Disruption Information theft Information manipulation	
Cyber vandals and script kiddies	Disruption Information theft	Disruption Information theft	Disruption Information theft	Information theft
Insiders	Information theft Disruption	Information theft Disruption	Information theft Disruption	
Unintentional acts	Breakdown/failure Leak	Breakdown/failure Leak	Breakdown/failure Leak	Leak

This threat matrix is based on the actor typology in: M. de Bruijne, M. van Eeten, C. Hernandez Ganan, W. Pieters, Towards a new cyber threat actor typology. A hybrid method for the NCSC cyber security assessment (TU Delft 2017). Various criminal actors have been combined because there was no characteristic distinction in terms of threat. The state and state-sponsored actors distinguished in the method have been combined due to insufficient information to be able to make a distinction.

Nation-states pose the most significant digital threat

Nation-states digitally attack other countries, organisations or individuals, primarily for geopolitical motives. Their objective is to acquire strategic information (espionage), to influence public opinion or democratic processes (influencing), to disrupt critical systems (disruption) or even to destroy them (sabotage). A number of digital attacks by nation-states have been identified over the last year. They had an impact on national security.[10]

Digital attack tools being widely used

Digital attack tools are now a fixed component of the range of tools that nation-states can employ to protect their geopolitical interests. There are very few inter nation-state conflict situations where digital tools are not employed. Economic interests also play a role in this. Apart from these conflicts, nation-states participate in economic espionage, to improve the competitive position of their economy for example or to quickly acquire innovative knowledge. The greater willingness of nation-states to use digital tools is paired with an increase in the impact of digital attacks.[11] Cyber attacks can have a major impact and cause wide-ranging collateral damage[12] (examples are WannaCry and NotPetya).

The use of third parties

Nation-states can use or exploit other parties when preparing or perpetrating digital attacks. These parties do not have to be aware of the exploitation. Nation-states can buy advanced attack tools so they do not have to invest in developing them themselves.[13] Nation-states can also 'contract out' the preparations and perpetration of digital attacks to a third party.[14] Finally, they can exploit the products and services of a third party to perpetrate attacks. This is how the actor behind the NotPetya attack compromised the M.E.Doc software company to distribute malware through legitimate updates.

In addition attackers can, sometimes using a simple method, employ legitimate tools, system properties or the properties of (cloud) services to penetrate their victim's systems.[15] When doing so, actors exploit the trust consumers have in IT products. These attacks are often difficult to detect.

Significant damage from NotPetya

On 27 June 2017, the world was shocked by the rapid spread of malware which appeared to take files hostage. Kaspersky Lab called the malware NotPetya (or New Petya, Nyetya, ExPetr).[16] The name refers to the ransomware which was distributed in May 2016 under the name Petya. Many parties originally believed that there were similarities. In the end, the NotPetya malware proved to be significantly different to Petya or WannaCry (which was distributed in May 2017).

NotPetya is based on the ExternalBlue exploit which is attributed to the NSA.[17] A patch had already been available for this in March 2017.[18] What in the first instance appeared to be ransomware, turned out to be wiperware (software that erases data) because there was no opportunity to actually recover the files held hostage.[19]

The malware quickly spread through various countries, including the Ukraine (with 80% of the infections[20]), France, Denmark, England and the United States.[21] In the Ukraine, government systems failed, the Metro stopped running, Kiev airfield suffered difficulties and there were problems in the electrical power plants.[22] Maersk, a Danish maritime transport company which also has a branch in the port of Rotterdam also suffered in the NotPetya attack. In the end, Maersk suffered some €300 million losses worldwide as a result of the attack[23] and had to reinstall the software on 45,000 computers.[24] The Dutch parcel carrier TNT Express also had problems as a result of infected computers.[25]

Following investigation, it turned out that the malware had been distributed through a software update for M.E.Doc accounting software originating from the Ukraine.[26] The supply chain for the accounting software was compromised as a result. The software was able to spread quickly and circumvent security barriers if the latest patches for the EternalBlue exploit had not been installed.

The NotPetya attack was attributed to Russia by the United States, Denmark and the United Kingdom, among others.[27] The motive would have been to destabilise the Ukraine, as happened in the past with the distribution of what is known as BlackEnergy malware.[28] This would tie-in with the geopolitical tensions between Russia and the Ukraine.

Use of simple techniques

State actors have a great deal of expertise and are capable of perpetrating advanced attacks. Despite this, it has become apparent that nation-states make widespread use of simple attack techniques. For instance, according to public reports Russia makes widespread use of (spear) phishing.[29] The same applies to North Korea, which also distributes malware by email.[30] In 2017, China used a simple exploit of LinkedIn to approach people in Germany and then recruit them.[31] Just like other actors, nation-states realise that simple techniques are very effective.[32] An attacker attempts to entice targets into revealing sensitive or confidential information, which can then be used for a follow-on attack or for other purposes.

The widespread use of simple attack techniques by state actors demonstrates that they are sufficiently targeted and effective. Barriers can be erected against the simple attack techniques which make potential targets of attacks less vulnerable and less interesting. Measures which should be part of the 'basic hygiene' of IT systems and IT networks, a basic level of cyber security, increase the resilience to digital attacks considerably, even if attacks by state actors are involved.[33] This reduces the probability of and the impact of this threat.

Attackers accept collateral damage or do not anticipate it

A number of attacks had a major impact across the globe. In addition to NotPetya, WannaCry spread across 150 countries[34] in May 2017 with a major economic and social impact. For instance, in the United Kingdom the processes of a large number of hospitals were disrupted. Other nations attributed these attacks to state actors. Attackers appear to accept that collateral damage is caused, by the infection of the supply chain or by using a worm that is capable of self-distribution for example, or do not anticipate this collateral damage[35]. These techniques run the risk of an uncontrolled spread.

From the perspective of national security, uncontrolled attacks that are difficult to predict and have a destructive effect have the potential to create a society-disrupting impact. This is particularly the case when critical processes are hit, whether or not by accident as collateral damage, and certainly if several systems or processes are involved.

Supply chains increase vulnerability

Over the past year, various attacks have used a supply chain to distribute malicious software. One of the most prominent examples is NotPetya, which was distributed through an update to Ukrainian accounting software. This method of attack has a number of advantages for actors. First, the use of a trusted supplier as the distribution source ensures that the target's security measures can be circumvented by and large. Secondly, actors are also able to decide exactly who is infected, from one specific target up to and including all customers of a specific supplier. Thirdly, when an attack takes place via a supply chain, deciding who the intended target was is complicated. This makes attribution more difficult.

Dutch organisations are highly dependent on a limited number of foreign suppliers of products and services. Although these companies have more resources at their disposal to arm themselves against attacks, the social impact of disruptions are significant because many different services depend on a small number of providers.[36]

In addition to disruption, products or services from foreign suppliers can be compromised by actors with or without the knowledge of the supplier. Producers and service providers are an attractive target for actors because of the supply chains. In addition, producers and service providers are subject to the laws and regulations of the country in which they are established and governments abroad could force them into some form of cooperation in, for example, espionage or preparations for sabotage. This is a risk to national security. Within that framework, the government has informed the House of Representatives that Kaspersky antivirus software is being phased out from central government as a preventative measure. Businesses and organisations with critical services and processes and businesses that fall under the Defence Contracts General Security Requirements (*Beveiligingseisen Defensie Opdrachten*, *ABDO*) have been advised to do the same.

This year, it has been revealed that supply chain attacks are effective and destructive. The spread and impact of such attacks are difficult to predict, certainly when actors accept that the attack could hit other targets. It is expected that actors will use this method more frequently.[37]

Actors interested in personal data

Stolen and leaked personal data played a striking role during the reporting period.[38] A wide range of actors (state, criminal, hacktivist) are interested in personal data. Parties who have the data are attacked to acquire this data; they include service providers, public authorities and educational institutions. Personal data can be used for criminal activities such as credit card fraud and identity theft and can also be used for espionage activities. Examples of this have also been identified in the Netherlands.[39]

In addition, errors or malfunctions lead to personal data leaks such as, for instance, storing data in publicly accessible cloud applications.[40] This is a problem in the Netherlands too, in 2017, for instance, 10,000 data leaks were reported to the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens*, *AP*).[41] What is important in this respect is that some personal data such as date of birth and citizen service number cannot be changed. This makes reducing the impact of a leak of this data more difficult.

The threat from terrorists and hacktivists is stable

A number of points in the threat assessment are stable. For example, the threat from terrorists and hacktivists remains unchanged. Jihadists have been active on the Internet for many years now, in the propaganda and fundraising fields for instance, but until now they have not perpetrated any terrorist attacks using digital tools. They have the ambition, but this has not been converted into concrete intentions or the development of expertise and capabilities.[42] For terrorist groups, committing physical attacks remains the priority or they are easier to perpetrate. Hacktivist are active, in website defacements and data theft for instance, but at this moment they do not pose a threat that has an impact on national security either.[43]

Attack facilitators increase the accessibility of methods of attack

Attack facilitators are a special category in the cyber domain. They do not perpetrate digital attacks themselves but do play a role in the threat.[44] On the one hand, these are criminals who trade stolen information such as credit card details or personal data for financial profit. They sell information which can then be used for an attack. On the other hand, they are actors who realise facilities for attackers, by leasing botnets for example. Information and attack tools can be bought for relatively small amounts on both the open and the more hidden parts of the Internet. In this way, these products and services allow actors with limited capabilities to perpetrate digital attacks. The facilitators lower the threshold and increase the accessibility of attack tools.

DDoS attacks in the Netherlands, January 2018

In January 2018, the Netherlands suffered DDoS attacks on various government and financial institutions which resulted in customers being unable to access them temporarily. The Tax and Customs Administration, DigiD and a number of banks were affected. The media speculated about the actor behind the attack.[45]

While the DDoS attacks continued and the various financial institutions were difficult to access temporarily, a new investigation was conducted. On 1 February 2018, an 18-year-old man from North Brabant was arrested on suspicion of perpetrating the DDoS attacks.[46] According to his statement, he was able to perpetrate the attacks by paying €40 for a so-called stresser,[47] a system that can be engaged to test the capacity of systems.

Actors who provide services to cybercriminals are devoting greater attention to improving the provision of service. Cybercrime-as-a-service[II](CaaS) has existed for some time now[48] but has become more widely accessible. The tools that are leased are versatile and advanced and their numbers are growing significantly.[49] The connection of an increasing number of everyday devices to the Internet, the Internet of Things (IoT), plays a role in this development. Countless IoT devices are infected with malware, to create botnets that can be used multifunctionally, among other purposes. The sector displays similarities with the traditional supply and demand market where factors such as price differences, quality and the level of service provision play an important role and where tasks are specialised.

Developments over the past year have revealed that the CaaS sector is continually innovating and developing new, lucrative ways of earning revenue. This is apparent from, among other things, the continuous further development of products and services, an example of which is ransomware. It is not new, but is being further developed continuously. Cryptomining and cryptojacking[III] are relatively new developments.[50] This application focuses on earning revenue by using the processing power of computers to mine for crypto currencies. This is first of all by hacking Wi-Fi networks[51], computers[52] and websites[53], and secondly by giving website users a choice between adverts or crypto mining.[54] One of the parties is Coinhive[55] which offers crypto mining code as a service to website owners. Cryptojacking is an attractive revenue model for criminals, which incurs few risks.

The cybercriminal service sector appears to be becoming more professional by making tools more widely accessible.[56] This development leads to an increase in the threat, which in the long term can damage confidence in the economy and the digital infrastructure.

II The description cybercrime-as-a-service refers to the tradition of service providers to put 'as-a-service' after the name of their product. For instance, normal market services are supplied as platform-as-a-service and software-as-a-service.

III Cryptojacking is when cryptomining software is used without permission.

Failure and breakdowns

In addition to attacks by actors, incidents occur by accident which also pose a threat to systems and the information contained on them, i.e. failures and breakdowns. These threats can have a significant impact. For instance, in early April 2018, there was a major breakdown at Eurocontrol, the organisation responsible for coordinating the routes of passenger aircraft in Europe.[57] The breakdown resulted in delays to 10% of the flights. According to a report[58] from March 2018 by the US Federal Communications Commission (FCC), the biggest interruption of American telephone services was caused by a software error. On 4 October 2016, the American telephone network had to contend with an 84 minute long breakdown.[59] More than 100 million telephone calls were blocked. On 29 April, a major breakdown at Schiphol led to heavy traffic at the airport and on the access roads. Flights were delayed or cancelled.[60]

Closing remarks

The digital threat is permanent. Digital attacks by state actors with the objective of espionage, influencing, disruption and sabotage constitute the most significant threat. In addition, the activities of cybercriminals have a major impact. There seems to have been no fundamental change to the threat landscape over the past year. However, it has become more diverse as result of a number of shifts, some of which originated several years ago. Cyber attacks continue to be profitable, low-threshold and involve little risk for attackers. Within the context of recent geopolitical developments, nation-states are expected to continue using such digital attacks and may even opt to do so on a grander scale.

Cyber security is essential for society, the economy and national security

3 Interests

Cyber security is essential for the functioning of the Dutch society and the Dutch economy, both of which are highly digitised. Despite its importance as a barrier against digital threats, parties sometimes make decisions that compromise the interests of digital security. Such decisions can affect national security: after all, a chain is only as strong as its weakest link. This chapter describes the importance of cyber security.

Cyber security is essential for the functioning of society and the economy

According to the report 'The Economic and Social Need for More Cybersecurity' (*De economische en maatschappelijke noodzaak van meer Cybersecurity*), the Netherlands has developed into one of the most IT intensive economies in Europe, owing to our outstanding digital infrastructure. Digitisation presents enormous opportunities to society and the economy but the digital world must remain secure and trusted. Just as we need flood protection, so too the Netherlands must continue to have effective digital defences in place.[61]

In the coalition agreement, the government emphasises the importance of digitisation and cyber security. The government wants the Netherlands to be a European leader in the digital field. Preconditions for this are a secure digital infrastructure and cyber security.[62] The Bureau for Economic Policy Analysis asserts that the economic importance of cyber security is increasing as a result of digitisation.[63] Digital security is therefore necessary for the functioning of our society and economy and for exploiting opportunities.

Digital security is also important to the global Internet and to international legal order. Countries are highly dependent upon each other precisely because the digital domain has a cross-border nature. For instance, misuse of digital infrastructure in the Netherlands by Dutch or foreign actors results in problems in other countries. Those countries could hold the Netherlands accountable. Conversely, the Netherlands may have problems with actors in other countries. In addition, the Internet has developed into a global public good, the public core of which has to be protected.[64] The Netherlands, with its open and globalised economy and free society benefits from a free, open and secure Internet, including in countries outside of Europe.[65]

Cyber security required for national security

Five security interests[66] have been defined for national security (see table 2). If one or more of those security interests are severely impacted, this could have a disruptive effect on society.[67] This is certainly the case if critical processes are disrupted or fail. For example critical processes protect us against flooding, keep our food fresh and our water pure. Electricity and heating, the functioning of payment transactions, road, water and air traffic and the maintenance of public order and security are also factors that should be considered.[IV]

IV Twenty-six processes have been designated as critical. For details see: 'Resilient critical infrastructure' ('Weerbare vitale infrastructuur'), NCTV, 2016 (https://www.nctv.nl/organisatie/nationale_veiligheid/vitale_infrastructuur/index.aspx).

Table 2 **The five national security interests**

Territorial security	The unimpeded functioning of the Netherlands as an independent state in the widest sense, or the territorial integrity in a narrow sense. *This concerns both the physical territory and corresponding infrastructure and the image and reputation of our country.*
Physical safety	The unimpeded functioning of people in the Netherlands and its surroundings. *This concerns people's health and well-being. The criteria are numbers of fatalities and seriously injured people and a lack of basic needs such as food, power, drinking water and adequate accommodation.*
Economic security	The unimpeded functioning of the Netherlands as an effective and efficient economy. *This concerns both economic damage (costs) and the vitality of our economy (for example a serious increase in unemployment).*
Ecological security	The unimpeded continued existence of the natural living environment in and around the Netherlands. *This concerns violations of nature, the environment and ecosystems.*
Social and political stability	The unimpeded continued existence of a social climate in which individuals can function without being disturbed and groups of people enjoy living together within the benefits of the Dutch democratic system and values shared therein. *This concerns violations of freedom to act, the democratic system, the core values of our society, and the occurrence or otherwise of large-scale social unrest and accompanying emotions (fear, anger, grief).*

Source: National Safety and Security Strategy

Critical processes are highly digitised and therefore vulnerable to digital threats. Analogue alternatives are disappearing.[68] The Council for the Environment and Infrastructure (*Raad voor de leefomgeving en infrastructuur, Rli*) has indicated that the Dutch electricity supply is becoming increasingly intertwined with digital technology. Pre-programmed or self-learning technology is making decisions relating to storage, supply and consumption. The Rli mentions risks such as cyber attacks and breakdowns as result of, for example, software errors or unforeseen behaviour of autonomous systems. Breakdown or failure of the electricity supply can lead to accidents with personal injury, material or financial damage. Moreover, social unrest can occur in the event of a protracted power outage.[69]

The fact that cyber incidents can affect security interests is apparent from, for example, the National Security Profile which presents a summary of potential disasters and threats that could disrupt the Netherlands. It contains four cyber scenarios[V], assessed against the consequences for national security. The impact of two scenarios, 'Impairment of the foundation of the Internet' and 'Cyber disruption of the critical sector' are assessed as severe and the impact of the 'Government cyber espionage' and 'Cyber attacks on high-quality payment transactions' as considerable.[VI] [70]

Two examples in the latest AIVD Annual Report are illustrative in this respect. The AIVD finds that to an increasing extent activities are taking place where the objective is to facilitate the digital sabotage of critical infrastructure in Europe.[71] This development at least has an impact on territorial security and possibly on physical, economic and ecological security, as well as social and political stability. The AIVD also reports that terabytes of confidential data were stolen in 2017 during digital break-ins at various European multinationals and research institutions in the energy, high-tech, and chemical sectors. This represents a substantial economic value. Such persistent digital attacks are a threat to the economic earning capacity of the Netherlands[72] and thereby impair economic security.

The consequences of cyber incidents cannot be determined unequivocally

The major complexity and interconnectedness of the digital domain and the physical domain make it difficult to determine the consequences of cyber incidents. For instance, digital attacks often comprise different stages where one or more components of an information system are affected and as a result of this, in some cases, physical systems such as flood defences can be impaired.

Because many of these stages and the effectiveness of the measures taken are uncertain, there is a high degree of uncertainty about the impact of digital attacks.[73] Other factors, which could have a mutual effect too, also contribute to the impact.[VII] For instance, the consequences of structural, systematic and long-term digital espionage by a state actor on top sectors in the Netherlands are different to those of one-off and short-term spying on an individual top sector company in a top sector. Both come under the

V A scenario is a fictional situation which describes a possible disaster, threat or crisis. A scenario is constructed from a specific combination of a cause, actor, motive, target, nature of impairment, degree of penetration and duration.

VI There are five impact categories, in ascending order of impact: limited, considerable, severe, very severe, and catastrophic.

'digital espionage' threat, but the nature and scale of the consequences are different.

Despite these complications, reports on the financial consequences of incidents appear regularly. Such reports are written on the basis of certain assumptions, categories of consequences, or impact criteria, working methods, delineation in terms of scope, time and geographic area. This makes it difficult to compare reports, if not impossible. The Bureau for Economic Policy Analysis says that relatively little is known about the damage caused by cybercrime[VIII] [74] and companies like McAfee and CSIS mention various complicating factors for estimating the damage caused.[75]

The consequences of cyber incidents cannot, therefore, be determined unequivocally. The number of variables to be taken into account when doing so is far too high. Moreover, assumptions also have to be made about the possible interaction between variables. Chain effects can also occur. A disruption of the IT in the electricity system can disrupt all kinds of critical process and thereby result in all kinds of consequences. The fact that the consequences cannot be determined unequivocally partly limits better awareness of digital risks. This can be an impediment to optimally considering the interests of digital security in relation to other interests.

Cyber incidents can have major consequences, with the potential to disrupt society

Up until the time of writing, the Netherlands has been spared a large-scale cyber incident that is disruptive to society. Potentially, under different circumstances, a number of cyber incidents in the past could have turned out very differently, as in the case of the security leak at DigiNotar in 2011.[76] WannaCry (June 2017) could perhaps have had a society-disrupting impact, if the outbreak had occurred at the start instead of at the end of the working week and if the so-called 'kill-switch' which rendered the malware harmless had not been discovered by a security expert.

In these cases, the Netherlands escaped a disruption of society more or less as a result of fortuitous circumstances. It is precisely the total dependence on digital resources that would make it possible for a cyber incident to inflict damage which disrupts society. Examples include a conflict between other nation-states or conflict between a nation-state and the Netherlands. This is illustrated by the government of the United Kingdom (among others) has accused Russia of the NotPetya attack. Although the primary target was the Ukraine, other organisations in other countries, including the Netherlands, were affected.[77] The consequences could disrupt society, especially in the case of a conflict where the state actor has already undertaken the first steps towards digital sabotage. As a result of WannaCry and NotPetya, the European Council has also concluded that incidents and attacks could have major implications.[78]

Conflicts of interest lead to concessions

Cyber security measures are needed as a barrier against digital threats. At the same time, members of the public, businesses, sectors and the government will always need to conduct a balancing exercise. After all, cyber security measures cost time and money, two scarce resources that can also be deployed elsewhere. Occasionally, the interest of digital security is a direct extension of other interests; occasionally, however, there are conflicts between the various interests.

These conflicts arise within organisations, such as the conflict between ease-of-use for individuals and the interest of cyber security, but they also arise between organisations. The commercial interest of a business may be contrary to the social interest. One of the causes of these conflicts of interest is an unequal division of costs and benefits. Costs and benefits do not always lie with the same party, as is manifested in various situations. For example:

- digitally insecure products and services, the commercial interests of products versus the cyber security interest of society;
- the costs of measures to an organisation versus the benefits to other organisations or the collective;
- balancing the continuity of a process against the implementation of measures;
- the inconvenience a measure brings to individual users versus the added value of this measure to an organisation;
- the wider social interest of cyber security versus the specific interest of intelligence agencies and law inforcement;
- international conflicts of interest.

Digitally insecure products and services

Suppliers of hardware and software let other, mainly commercial, interests prevail over the social interest of digital security. For instance, the Cyber Security Council (*Cyber Security Raad, CSR*) for Internet of Things applications observed that there is little stimulus

VII The relevant factors are: a) the type of threat, b) the type of actor or event, c) the targets affected, d) the type of information system affected (process control system, office automation, website etc.), e) the nature of the information (for example the digital crown jewels of the company), f) the degree of penetration (organisation, sector, sectors, a number of provinces, etc.), g) the (potential) duration, h) the degree to which a cyber attack takes place structurally and systematically and i) the degree to which the consequences occur in the short or long term.

VIII According to the Bureau for Economic Policy Analysis, which is based on the CSAN, cybercrime includes crimes such as online-shopping fraud which fall outside of the scope of this CSAN.

for producing and maintaining secure hardware and software. Time-to-market and low cost prices are more important than quality to the majority of manufacturers, and companies do not put sufficient effort into meeting their obligations.

The result is the explosive proliferation of insecure devices and applications that are connected to each other and which pose a threat to our digital security and privacy.[79] The commercial interests of these producers and the cyber security interest of society constitute a conflict of interest.

Individual balancing of interests can lead to collective damage

The conflict of interest described in the previous paragraph does not only apply to all product and service suppliers, it also applies to all other organisations in the digital domain. They too have to balance the costs and benefits of cyber security measures. The benefits constitute a reduction in the impact of an incident or from completely preventing an incident; damage is mitigated or prevented.

The balancing of interests by an organisation will be determined by, among other things, the costs and benefits to the organisation itself and this organisation's insight into the risks. At the same time, an organisation's failure to implement measures can lead to damage to other organisations or result in damage to society. For instance, if an organisation does not have its software updates in order, this organisation's IT infrastructure can be exploited to attack other organisations. Here too, an organisation's commercial considerations can be contrary to the interests of another organisation or the interest of the collective.

Continuity of the process versus implementation of measures

A specific situation applies with respect to control systems. These are systems that manage and control physical processes and activities. Examples of these include industrial control systems (ICS) in manufacturing plants, control systems for medical equipment in hospitals, and so on.

Sometimes it is necessary to shut down processes temporarily to implement security measures such as updates. This has consequences in terms of continuity and also costs money. Moreover, updates can have an unwanted impact on the functioning of processes and therefore have to be assessed in advance.

So, updates are needed in terms of process continuity (as well as confidentiality and integrity) on the one hand, but on the other hand, continuity or functionality can be impaired temporarily by those updates. An organisation may choose to cancel or postpone updates but if things go wrong, there can be major consequences for other organisations.

Cyber security sometimes results in reduced ease-of-use

Cyber security sometimes reduces ease-of-use. The use of individual usernames and passwords for accounts and two factor authentication increases security for the organisation but in practice it requires additional effort on the part of the user. An organisation responsible for a critical process could, therefore, decide to use the same username and the same password and not to use two factor authentication. Once actors have managed to acquire those details, they have access to all of the systems which are associated with the account, which can have serious consequences. The costs of measures (reduced ease-of-use) fall to individual users, the benefits to organisations, or even to companies.

Tensions between the social cyber security interest and intelligence and law inforcement interests

Tensions may arise in some cases between the wider social cyber security interest and the specific interests of intelligence agencies and law inforcement. Public authorities, companies and members of the public are using encryption increasingly often to protect the confidentiality and integrity of communications and stored data. At the same time encryption, when used by criminals for instance, is a barrier to obtaining information that is needed by law inforcement and intelligence and security services.[80]

Another case in point is the way operational services deal with what is known as zero day vulnerabilities. Agencies at home and abroad can, in the interest of their national security, deploy zero-day vulnerabilities to investigate threats. Not reporting (zero-day) vulnerabilities means the producers cannot provide solutions. This occasionally causes major risks to society, because others can also discover and exploit such vulnerabilities. The (coordinated) disclosure to producers and suppliers of vulnerabilities provides an opportunity to resolve them, making it impossible to exploit these vulnerabilities.[81]

International conflicts of interest

At an international level, there have been divisions between various countries about the approach to the cyber domain. Differences of opinion have arisen on the application of international law, standards of behaviour in cyberspace and dependence on and access to digital resources. An example of this is the obligation some countries impose on software suppliers, including antivirus companies, to provide insight into source codes, justified by the need to check for possible 'backdoors' for purposes such as espionage.

The downside of this is that countries could also gain insight into any vulnerabilities which they could exploit themselves.[82] Possible misuse impairs confidence in that software. If governments decide to accept products and services from their own country or allies only, this will result in fragmentation of the Internet.

Cyber security: a chain is only as strong as its weakest link

Decisions compromising the interests of cyber security that are taken by individual parties can have consequences for all of Dutch society and the economy, and could eventually result in damage to national security. Such a decision by an individual party may be optimal for that party but the sum of all decisions taken is certainly not always optimal for the greater whole.[83]

In cyber security too, a chain is only as strong as its weakest link. The large-scale exploitation of a vulnerability in a single device could, for example, have major implications for the functioning of critical processes. A vulnerability in transformers for solar panels produced by a market leader exposed in the press in 2017 is a case in point. According to the researcher, a large number of transformers could remotely and simultaneously be switched off using this vulnerability. Such large-scale switching off could lead to disruption of the power supply in large parts of Europe.[84] The Council for the Environment and Infrastructure has also warned that the stability of the entire electricity system is being undermined primarily by components that are not under public ownership.[85]

Closing remarks

Cyber security is needed for the functioning of the highly digitised Dutch society and economy, and as a barrier against digital threats. This applies to national security in particular. The consequences of cyber incidents cannot be determined unequivocally. Still, those consequences could be considerable, certainly under particular circumstances. Despite the importance of cyber security as a barrier against digital threats, parties sometimes make decisions that compromise the interests of digital security, simply because they have other interests as well. In some cases, those decisions could impair national security: after all, a chain is only as strong as its weakest link and the costs and benefits do not always lie with the same party.

Two developments contribute to the continuous need for digital security. Wide-ranging digitisation has been going on for years and the end is not yet in sight. Ever-more processes critical to society are being digitised; analogue alternatives are disappearing and ever-increasing volumes of information are being processed digitally.

The deployment of new technological developments such as robotisation, e-health and intelligent transport systems are creating entirely new forms of information as a result of which the volume of information will increase even further. Consequently this development, the number of potential vulnerabilities is increasing.

Additionally, within the context of recent geopolitical developments, account must be taken of the fact that state or state-sponsored actors will remain instrumental in perpetrating digital attacks, will use more complex methods or will use them on a greater scale. As a result, cyber security continues to be necessary for the functioning of society.

Chain dependencies and supply chains increase vulnerability

4 Annual overview

The annual overview shows that nation-states are increasingly using digital espionage and perpetrating sabotage attacks against organisations across the globe. Configuration shortcomings make attacks possible and various incidents demonstrate that chain dependency is a considerable risk to digital security. Researchers are discovering vulnerabilities and attack techniques which have the potential to cause large-scale damage, but these are not yet beyond the laboratory. Email continues to be a popular tool for phishing or spear phishing, and for distributing malware. In addition to the use of known malware variants, such as ransomware, criminals appear to have embraced cryptojacking as a new tool for earning revenue.

Nation-states are using malware against vulnerabilities in the critical infrastructure

The highly developed IT infrastructure in the Netherlands remains attractive as a transit port for digital attacks. The Dutch infrastructure is being exploited for attacks on third countries.[86] The AIVD has established that nation-states are increasingly perpetrating both targeted and random digital attacks on organisations worldwide. The intelligence service is increasingly seeing activities that are aimed at facilitating the sabotage of critical infrastructure in Europe (in the future) because other countries have established a foothold in certain systems.[87]

In September 2017, security company Symantec reported on new attacks by a group known as Dragonfly.[92] This campaign, also known under the name Havex, Crouching Yeti, Koala Team and Energetic Bear, focused on exploring the operational environment of energy companies and installing backdoors. This involved espionage, possibly to later facilitate sabotage. The researchers detected attacks in the US, Turkey, and Switzerland which had been being perpetrated since 2015. According to Symantec, the campaign had the potential to target energy companies with sabotage in the future, although they could not confirm with certainty that this was indeed the ultimate objective.

More details are known about the malware that caused the power cuts in the Ukraine earlier

In the previous reporting period, a cyber attack on the power grid in the Ukraine led to a loss of power. In June 2017, security company ESET released a research report on the malware that may have been used in this attack.[88] The malware that was used, referred to by the name of Industroyer by the researchers, can communicate with the industrial control systems (ICS) that are used for purposes such as controlling power grids. However, the malware can also be used against other organisations in other industries and other countries and possibly against the Netherlands.[89] An important precondition to allow the malware to be used is that the attacker must have access to the target's network.

The attack was also analysed by researchers from security company Dragos, who named the malware CrashOverride.[90] They attributed the attack to the Russian actor group Electrum. This group was said to have been closely associated with the Sandworm actor group, which had already been working on espionage campaigns against companies and institutions in the Ukraine and various sectors in Europe and the United States, including the energy sector, government, telecommunications and academia for a number of years.[91] According to the researchers, system manipulation (influencing the power grid) was the only objective of the malware and not, therefore, espionage, unlike earlier campaigns by this actor.

The malware that was used was suitable for sabotaging ICS, but was mainly used for digital espionage in practice. The group used two exploit kits (LightsOut and Hello) and various remote access tools (RATs) (Havex, Karagany and Oldrea). In March 2018, researchers from the security company Cylance suggested that compromised Cisco routers were also used in attacks by this actor.[93]

In October 2017, the American US-CERT reported attacks by advanced actors on critical infrastructure which were linked to the Dragonfly campaign.[94] The attackers focus on poorly secured points and small networks to penetrate the networks of major organisations in the energy sector. There are two types of targets. The initial targets are organisations on the outside, trusted suppliers with less well-secured networks, for example. Attackers use the networks of the trusted suppliers as a base of operations to attack their final target.

Analysis by US-CERT revealed that where two factor authentication was not used, the login details that were obtained by the attackers, at those locations were used to gain access to the victims' network. The attackers targeted the ICS infrastructure and conducted reconnaisance operations in the network. There are currently no indicators that targets in the Netherlands were attacked in this campaign. In March 2018, the American government attributed these attacks to Russia.[95]

This illustrates a remarkable development in the reporting period: the public attribution of cyber attacks to specific countries. For instance, the Ukrainian secret service SBU, the United States, and the United Kingdom also accused Russia of involvement in the NotPetya attack.

Triton/Trisis malware targeting security systems

In December 2017, malware was discovered that can reprogram Schneider Electric Triconex Safety Instrumented Systems. These safety controllers are used as backup in the safety of, for example, chemical or nuclear industrial processes including when problems occur with the normal control system. These Triconex-systems are used in thousands of manufacturing plants worldwide. In March 2018, there was renewed attention for this malware; the New York Times reported that the malware may have been used in an attempt to sabotage a petrochemical plant in Saudi Arabia.[96] The malware appeared to be capable of modifying a control system, according to the New York Times, with the objective of sabotage and causing an explosion. A bug in the malware seems to have prevented an explosion. Due to the high level of sophistication of the attack it was associated with a state actor. The National Cyber Security Centre is not aware of any Triconex malware infections in the Netherlands.

In the previous reporting period, the 'Shadow Brokers' hacker group published hacking tools believed to originate from the American intelligence services.[97] The tools that received most attention were EternalBlue and EternalRomance – which exploit the SMB file sharing protocol on Windows systems to compromise those systems – and DoublePulsar, a backdoor that can be installed on infected systems to execute various malicious code. The use of these exploits has become publicly visible during this reporting period and has inflicted much damage.

At the beginning of May 2017, the WannaCry malware spread across globe through misuse of the vulnerabilities exploited by EternalBlue. It severely affected many organisations. The impact in the Netherlands was limited. The organisations affected include the Spanish Telefónica company, FedEx and the British National Health Service (NHS). Further spreading was limited because a security researcher discovered what is known as a kill-switch in the malware and triggered it.

Actors use tools to target vulnerabilities in the supply chain

In June 2017, the large-scale NotPetya[IX] digital attack affected organisations across the globe. The attack, which was known by other names including PetrWrap, GoldenEye and ExPtr, also resulted in various victims in the Netherlands. The initial attack vector appeared to be the M.E.Doc company's accounting software: attackers were able to use stolen log-in details to add malicious code to an update to the software.

Following infection, the malware spreads as a worm within the organisations affected. Although it manifested as ransomware, research revealed that decryption was not possible in practice. This means that NotPetya actually only focused on erasing files, where the only solution to an infection was restoring backups. The malware used components from various sources, such as the EternalBlue exploit which had been used previously in WannaCry. Various security companies claimed that NotPetya specifically targeted the Ukraine. In addition to the Ukrainian Secret Service SBU, the United States and the United Kingdom accused Russia of involvement in the cyber attack.[98]

IX The recent NotPetya malware is derived from the existing Petya ransomware virus from 2016. However, the original author claimed not to be responsible for the current variant. This is why the current malware was named NotPetya.

2017: the year of the cryptoworm

In May, hundreds of thousands of computers across the world were infected by WannaCry.[99] In June, thousands of computers mainly in the Ukraine, Russia, and Western Europe (including the Netherlands) were infected with the NotPetya malware.[100] There was also an outbreak of the BadRabbit ransomware in the Ukraine, Russia, Turkey, and Germany.[101] Each of these campaigns used exploits that had not been released previously. Unlike many other ransomware campaigns, where users had to click a malicious link or open an infected attachment to become infected, this campaign used what is known as a worm to distribute the malware.

These global ransomware attacks demonstrate how dangerous and disastrous a cryptoworm can be, even if a vulnerability for which a patch has been available for a long time is exploited. In comparison with previous large-scale ransomware campaigns it was mainly the global scale of the infection and the financial damage that was inflicted that was notable. In the Netherlands, this was mainly caused by NotPetya. Container transporter Maersk estimated the losses as a result of this attack to be 200 to 300 million dollars.[102]

In August and September 2017, the popular CCleaner clean up software was infected with the Floxif Trojan.[103] This malware was injected into the program during the development process, as a result of which it found its way into the official version and the program's digital signature was valid. Initially, Avast reported that malicious code had not actually been executed on any infected systems despite the infected software being downloaded over two million times at the time.

Further research by the Cisco Talos security company revealed that it was a targeted attack. Of the 700,000 systems that made contact with the command and control server, a second phase infection, which was well hidden in the system, was detected on at least 20 systems. The victims were major companies in the technology sector. According to Cisco Talos, no second phase infections were detected in the Netherlands.

Important vulnerabilities exposed, exploitation can be expected

A number of technical vulnerabilities came to light during the reporting period that had the potential to cause damage on a major scale and which therefore generated a great deal of interest but little or no exploitation of them was observed. The attack techniques required to be able to exploit the vulnerabilities were often complex or certain conditions had to be met which made it difficult to use them on a large scale, such as the need to be physically close to the target. It is expected that these vulnerabilities that are currently difficult to exploit, but which could be of value to attackers, will be exploited in future.

In July 2017, a vulnerability was revealed in the Broadcom Wi-Fi chips that are used in telephones and other devices produced by manufacturers including Samsung, Google, and Apple. An attacker could exploit this vulnerability to gain control of the device, execute code on the Wi-Fi chip and obtain access to decrypted Wi-Fi traffic.[104] This vulnerability is known as Broadpwn.

Two months later, researchers found a similar vulnerability in the Broadcom Wi-Fi chips, where the researchers also published the exploit code which an attacker could use to execute code on the Wi-Fi chip.[105] Exploitation of the vulnerability using this exploit code only appears possible if a user connects to a new Wi-Fi network. This requires an attacker to be in physical proximity to the victim. The vulnerabilities were disclosed to Apple and Google and resolved in a coordinated way in new versions of their iOS and Android operating systems. This allowed devices for which the manufacturers are still issuing updates to be patched.

In October 2017, researchers at the Catholic University of Leuven published a report on attack techniques to which every device that uses Wi-Fi based on WPA or WPA2 encryption could be vulnerable, the so-called Krack attack.[106] Because the attacker has to be physically in proximity to the Wi-Fi network they wish to attack, the attack techniques are difficult to use efficiently on a large scale.

In January 2018, researchers revealed that two new families of vulnerabilities, Spectre and Meltdown, had been discovered in modern processors. An attacker exploiting these vulnerabilities can obtain confidential information by executing program code on the victim's computer.[107] A number of suppliers have announced or already released patches as a result of the vulnerability being announced.

The publication of proof-of-concept code to exploit these vulnerabilities did not a directly result in an increased risk because not everyone can perpetrate such complex attacks.[108] The expectation is that these vulnerabilities will be exploited in the future. In May 2018, a new vulnerability was discovered with a similar effect to Spectre.[109]

In March 2018, researchers at the security company CTS Labs launched a website about 13 serious vulnerabilities and backdoors they claimed to have discovered in AMD processors, known as AMDflaws.[110] The media quickly expressed doubts about the legitimacy of CTS labs, partly because AMD researchers were only informed of the vulnerabilities 24 hours prior to publication.[111] Eventually, AMD confirmed that the vulnerabilities did exist and they were working on patches. However, they indicated that the vulnerabilities posed a limited risk because they could only be exploited if an attacker had already compromised the system and had administrator rights.[112]

In May 2018, researchers at the Free University of Amsterdam revealed the GLitch vulnerability. This is a new way of perpetrating what is known as Rowhammer attacks via a computer's graphic processor (GPU).[113]

Many data leaks as a result of configuration shortcomings and a lack of security measures

Major data leaks are still commonplace

Data from data leaks can be used for spear phishing or for direct identity theft. The scale of the data leaks that were discovered and reported in this reporting period and the level of confidentiality of leaked information are once again noteworthy. In most cases, these aspects were caused by a failure to configure properly or a failure to resolve discovered vulnerabilities in due time. The damage caused by a data leak is difficult to establish, because there is often no indication of the scale of any misuse.

In September 2017, the credit rating agency Equifax announced a data leak that possibly involves 143 million Americans. In October 2017 and March 2018, Equifax reported that attackers had stolen the data of another 4.9 million Americans.[114] [115] An Apache Struts vulnerability was at the root of the data leak, which was exploited reasonably quickly after the discovery and issue of a patch. The complexity involved in patching meant that the vulnerability was not resolved in a timely matter. The attack cost Equifax 87.5 million dollars in the third quarter of last year.[116]

In November 2017, it was revealed that the Uber taxi app had concealed a major hack in 2016 where the data of 57 million people was made public.[117] In December, an announcement followed that the data of an estimated 174,000 Dutch passengers and Uber drivers had been stolen.[118] Uber appeared to have accidentally put the keys providing access to the Amazon cloud that contained all the personal information of passengers and Uber drivers on GitHub. This was discovered and reported to the company.

Following consultation, Uber eventually decided to pay the individual who reported the leak 100,000 dollars on condition that they signed an agreement in which they committed to erasing all the data. Uber decided not to report this data leak because, according to them, it fell under their normal coordinated vulnerability disclosure (CVD) program. Eventually, the lawyers involved in reaching this decision were fired when the incident became public and many people expressed concerns about it.[119]

In the same month, it was revealed that, as a result of a data leak, the energy consumption of all Dutch households could be obtained by postcode and house number on an energy supplier's website.[120]

In February 2018, German security company Kromtech discovered an incorrectly configured Amazon S3 bucket, a type of cloud storage server.[121] The server held more than 119,000 scanned documents, including identity documents. The leak was resolved the day after it was discovered. In April 2018, it was revealed that the scanned identity documents and address details of 3,000 Dutch citizens from the period 2009–2012 were amongst them.[122] Allegedly, this included the identity documents of Department of Defence employees.

Over 10,000 data leaks reported to the Dutch Data Protection Authority in 2017

The number of data leaks reported to the Dutch Data Protection Authority increased by over 70% in 2017 compared with the previous year, from 5,849 to 10,009. Just as in 2016, most of the reported data leaks originated from organisations in the health and welfare sectors (3,105 reports), public administration (2,000) and financial services (1,984). Almost half of the data leaks (47%) reported in 2017 concerned personal data that was sent to an incorrect recipient. Lost or stolen devices, data carriers, or documents were the cause in 14% of the total number of data leaks reported.

In most cases, the data involved name and address details, sex, date of birth and citizen service number. The size of the reported data leaks varied. In 80% of the cases, it was a data leak where the data of 1 to 100 people was leaked, in 17% it was the data of 101 to 5000 people, in 2% of the cases the data of 5001 to 100,000 people was leaked and in less than 1% more than 100,000 people had been affected.[123]

DDoS attacks via publicly accessible systems

The number of DDoS attacks worldwide rose in the first three quarters of 2017. It was quieter in the last three months of the year.[124] [125] [126] Politically motivated DDoS attacks, by hacktivists for instance, still receive regular attention,[127] although they appear to have little social impact. In the previous reporting period, IoT botnets made large scale misuse of the Internet of Things to carry out DDoS attacks. In this reporting period, it has become clear that other types of systems can also be used to execute large-scale DDoS attacks if they are not secured or are insufficiently secure.

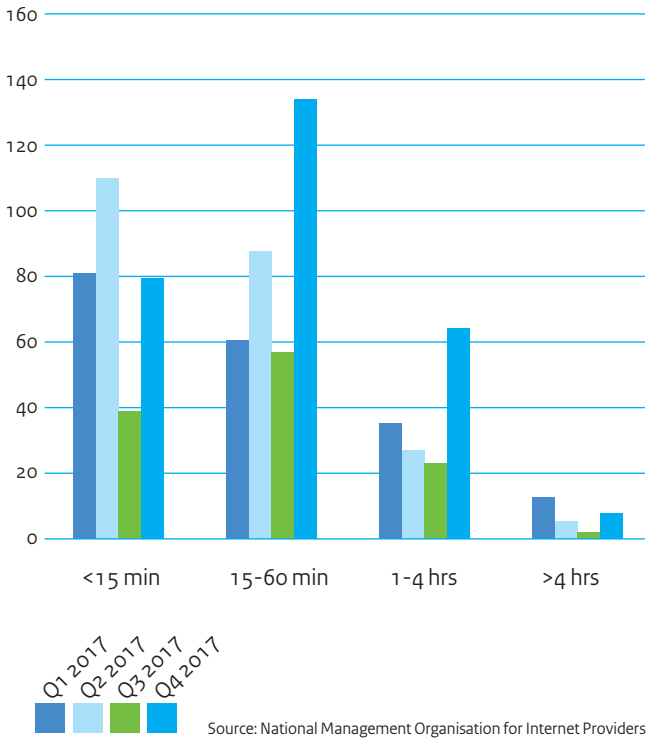
In February 2018, publicly accessible memcached systems were used in DDoS attacks.[128] Memcached systems are intended to temporarily store small amounts of data from other sources, such as databases and APIs, to make websites faster. The systems do not require authentication for communications and were not developed to be publicly accessible. It was reported that at the time of the attacks, there were approximately 3,000 publicly accessible memcached systems in the Netherlands.

Scenarios where these memcached systems are used to conduct amplification attacks are possible. In these attacks, the attacker ostensibly sends a request on behalf of the target by falsifying its IP address. Because the responses are longer than the request, an attacker can use relatively little bandwidth to set up a larger attack on that target. A publicly accessible system with a very high amplification factor, such as an unprotected memcached system, presents attackers with an attractive tool for carrying out attacks.

DDoS attacks are becoming increasingly complex, because they are coming from an increasing number of types of sources, which could be located anywhere in the world and can hit multiple targets simultaneously. Examples are insecure IoT devices, open memcached systems or 'booter sites' where DDoS attacks can be bought with only a little money.[129] [130] In March 2018, it was revealed that GitHub had been hit by a DDoS attack of 1.35 TB per second, the most powerful DDoS attack recorded up until that time, in January of that year. Memcached systems were also used in this attack.[131]

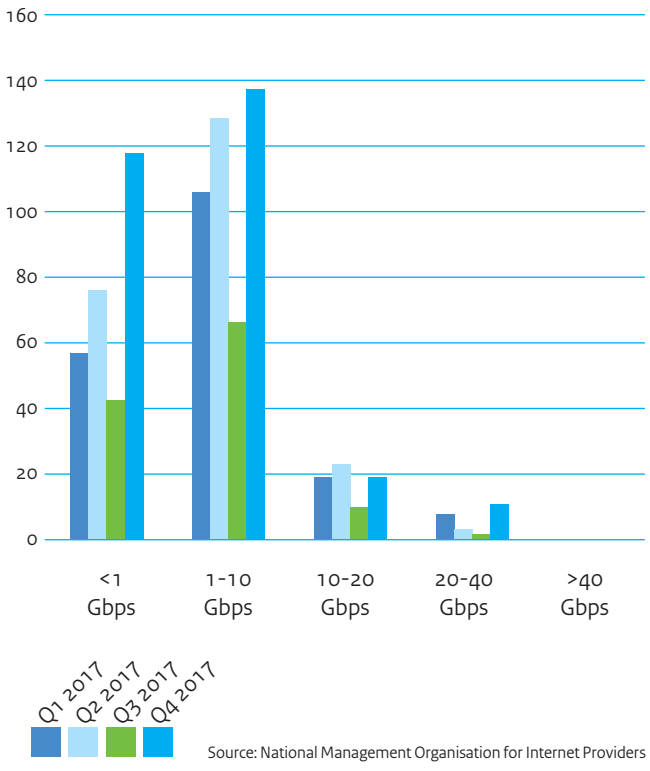
In 2017, the National Management Organisation for Internet Providers (*Nationale Beheersorganisatie Internet Providers, NBIP*), handled 826 DDoS attacks. Just as in 2016, the size of more than half of the attacks handled was between 1 and 10 Gbps. In 2017, more than 40% of the attacks lasted between 15 and 60 minutes. More than 3% of the attacks lasted longer than 4 hours.

Figure 2 **Duration of DDoS attacks**



Source: National Management Organisation for Internet Providers

Figure 3 **Size of DDoS attacks**



Source: National Management Organisation for Internet Providers

Email continues to be a popular tool for perpetrating digital attacks

Various actors use phishing or spear phishing as the first stage of a digital attack

Phishing is often the first stage of a cyber attack[132] and because it succeeds in many cases,[133] the tool is used by all kinds of actors. Email is used as a tool to establish a foothold in systems for espionage and sabotage purposes. Over 90% of malware infections are from email.[134] Once attackers have gained access to the network, they seek specific commercial information or they explore how the organisation's digital infrastructure is set up.

Renewed attention to email spoofing

Attackers sometimes use 'email spoofing' in phishing or spear phishing and the distribution of malware by email. During the reporting period, researchers revealed how people can send email that appears to originate from @tweedekamer.nl.[135] Other domains also appear to be vulnerable to this type of exploitation, such as @aivd.nl and @defensie.nl.[136] In the United States, thousands of the federal government's domains are being spoofed. The media attributes this to state actors.[137] Although it is not a new phenomenon, there are still many organisations that fail to implement measures such as the SPF, DKIM and DMARC standards. However, the fact that security measures can be circumvented came to light in 2017 when 'Mailsploit' vulnerabilities were revealed which still allow someone else's email address to be successfully used as the sender, despite security measures.[138]

The traditional form of phishing using spam still exists, but it is no longer the only form in the current threat landscape. The number of targeted spear phishing attacks continues to grow.[139] By targeting rich individuals in particular, or individuals with access to financial accounts, or the sensitive data of businesses or public authorities, attackers are hoping for greater financial gains from widespread and random spam campaigns.

State actors are using spear phishing for digital espionage

The AIVD has acknowledged a slight increase in economic espionage by state actors in Europe in comparison with 2016.[140] In March 2018, the American Department of Justice released details of charges against nine Iranians. They are accused of stealing 31 TB of documents and data from more than 140 American universities, 30 American companies, 5 American government organisations and more than 176 universities in 21 other countries, including the Netherlands.

The attackers are alleged to have used the login details of employees stolen using spear phishing emails to facilitate the theft, which would have taken place between 2013 and 2017.[141] The suspects were linked to the Mabna Institute, an Iranian company set up in 2013 with the explicit aim of illegally obtaining access to non-Iranian academic sources through computer hacking. The attackers would have been looking for research details, scientific data, industrial secrets, and intellectual property.

According to the FBI, the institute was contracted in by various components of the Iranian government, including the Islamic Revolutionary Guard, one of the various entities responsible for gathering intelligence. The FBI alleges the attackers stole data for the Iranian government and they offered the stolen data via two Iranian websites (megapaper.ir and gigapaper.ir).

The number of reports of phishing was reasonably stable worldwide between May and September 2017 and bears little difference to the average number of reports in the previous reporting period.[142] [143] [144] Right at the end of 2017, Microsoft detected a considerable number of phishing emails.[145] During this reporting period, the main manifestations of digital attacks that were observed were cases of phishing or spear phishing being used by criminals and state or state-sponsored actors. According to the Verizon telecommunications company, the latter two used phishing in 70% of their digital attacks.[146]

A significant increase in phishing websites misusing well-known Dutch brands

Some of the phishing emails lured victims to phishing websites, with an imitation version of a bank website for instance, where criminals attempted to obtain their login or credit card details. Analysis by the foundation for Internet Domain Registrations in the Netherlands (*Domeinregistratie Nederland, SIDN*) reveals that over the past year, the number of phishing sites that misuse well-known Dutch brands has increased by over 40%.[147] According to security company Webroot, an average of 1.4 million unique phishing websites are set up every month.[148] The many 'phishing kits' software packages that can be obtained (sometimes free of charge), which allow new phishing websites to be set up quickly and easily, will have played an important role in this respect.[149] One of the tactics used by actors to appear legitimate and secure, is furnishing the sites with a TLS certificate.[150]

Developments in the field of malware

A decrease has been detected in exploits for Adobe Flash player and vulnerabilities in Internet Explorer, while Microsoft Office exploits have increased.[151] In 2017, many of the documents that contained an exploit for Microsoft Office also contained a phishing component, in case the target had already patched that vulnerability. According to security company Kaspersky Lab, more than 90% of the detected malicious Office documents contained exploits for two specific vulnerabilities.[X] [152]

Large numbers of emails containing banking malware distributed in the Netherlands

In December 2017, analysts at security company Fox-IT in the Netherlands observed the distribution of a large number of phishing emails with a link to a downloadable zip file. Recipients who opened the attachment were infected with the Zeus Panda malware. Its objective was to obtain login details for Internet banking and credit card information. Although the emails that were sent did not appear to be very professional, and contained spelling mistakes for example, some 48,000 people clicked the link. The number of infections was lower, because the link was clicked 11,000 times from a Windows-based computer, the only platform upon which the malware worked.

The malware that was used was not new, but unique to this phishing campaign is that the criminals had also used web shops in addition to banks in their attack. The malware not only tried to obtain the victims' login and credit card details when visiting a banking website but also when visiting a web shop.

Although malware remains the most common digital threat,[153] the AIVD has observed that nation-states are increasingly misusing legitimate software functionalities and bona fide suppliers to gain access to specific victims.[154] Dutch organisations in the private sector, the critical infrastructure and governments are also targets in this respect. This makes the use of malware superfluous, which makes prevention and detection of such attacks more difficult.

Cryptojacking more attractive and more notable

Crypto currencies work on the basis of cryptographic principles and are mined by cryptomining: performing complex calculations.[155] More and more often, criminals are attempting to make money through cryptojacking, where they use the computing power of the computer systems of unsuspecting third parties for cryptomining.[156] The reason for this is that the value of cryptocurrencies has risen in recent years. In addition to criminals, there are instances where internal actors can pose a threat, when they use their employers' systems for cryptomining for their own personal gain.[157] [158] [159]

Criminals try to obtain the use of as many systems as possible, by infecting them with cryptomining malware for instance, and thus make them part of a botnet. Researchers at security company Proofpoint have followed the Smominru botnet which infected more than 526,000 Windows machines with cryptomining malware.[160] [161] When it did so, just as with WannaCry, the previously leaked EternalBlue and DoublePulsar vulnerabilities were used. The botnet is said to have made the criminals more than two million dollars.

In addition to more traditional computer systems, IoT devices are also being used to mine for cryptocurrencies.[162] Although they often have limited computing power, the large number of devices that are vulnerable to publicly accessible exploits still makes them an attractive target for cryptojacking by criminals.[163]

X CVE-2017-0199 or CVE-2017-8759.

Cryptomining malware has also been found on industrial control systems

In February 2018, security company Radiflow reported that they had encountered cryptomining malware in a network with industrial control systems for the first time. Monero mining malware was discovered in the network of the customer, a wastewater processing facility in Europe, during normal monitoring activities.[164] The malware was found on a number of servers, including an HMI (Human Machine Interface). These computers were indirectly connected to the Internet, to facilitate remote monitoring. According to the security company, it would appear that one of these computers was used to visit a website that was infected with the malware. Subsequently, the other servers were infected through the internal network.

An increasing number of websites are allowing their visitors to mine for cryptocurrency.[165] [166] [167] A JavaScript file that runs automatically when a visitor opens the relevant website is used for this. Cryptomining via websites appears to have become more professional since the end of 2017. One of the parties behind this is Coinhive,[168] a company that provides this code as a service to website owners. Coinhive presents it as an alternative to displaying advertisements on the website. In exchange for a commission of 30% of the return, this company provides the code that ensures that the computers of all visitors to the website are used to mine for cryptocurrency.[169] In many cases, visitors are not explicitly asked for permission.[170] This method of working has been observed on both 'questionable' websites such as the Pirate Bay,[171] a torrent website, and on legitimate video streaming services[172] [173].

Because cryptomining takes place in the background, it can be a long time before it is discovered.[XI] It is plausible that the growing popularity of cryptojacking is related to the enormous increase in the value of many cryptocurrencies. According to the Cisco Talos security company, an attacker who is using 2,000 systems (which is easily achievable according to the experts) could make around 500 dollars a day or 182,500 dollars a year. The researchers have seen botnets with millions of infected systems, which in theory could therefore make over 100 million dollars a year.[174]

Cryptojacking attacks appear to have increased in this reporting period, while the number of ransomware infections fell in the second half of 2017. A number of sources have established a relationship between the decrease in ransomware and the increase in cryptojacking.[175] [176] [177] In addition to the relative invisibility of the attack, an advantage of cryptojacking in relation to ransomware is that it makes money without the victims having to do anything for this, such as paying bitcoins in exchange for access to the system. It is still too early to be able to say with certainty that a shift from ransomware to cryptomining malware is actually taking place. According to security company Malwarebytes, the use of both increased in the first quarter of 2018 by 27% and 28% respectively but espionage malware continues to be the most popular.[178]

Closing remarks

During the reporting period, it was once again observed that criminals, nation-states and state-sponsored actors cause the most damage. The tools that were used were largely recognisable from previous years. For instance, email was the most widely used tool by far for phishing and spear phishing and for distributing malware.

A development with respect to criminals is that there has been an increase in the use of cryptojacking for financial gain. In addition, they are still making money by using or selling stolen information. Nation-states are increasingly perpetrating both targeted and random digital attacks on organisations worldwide. In addition to espionage, these attacks focus on disruption or sabotage of critical infrastructure.

Many incidents, such as data leaks and DDoS attacks, were facilitated by configuration errors or technical shortcomings in software or systems. In a number of large-scale digital attacks affecting organisations worldwide, it has become clear that chain dependency poses a significant risk to software security.

XI The computer could become slow because some of the computing power of the infected computer is used to mine for cryptocoins. This could be an indication to the user that something is wrong.

Basic measures very often not implemented, resilience under pressure

5 Resilience

The digital resilience of the Netherlands is under pressure. Many organisations fail to implement basic measures. Doing so could have prevented incidents or mitigated damage. The crown jewels of organisations are being successfully attacked without the use of advanced methods. Resilience is under further pressure from the increasing complexity and connectivity of the IT landscape and in some cases as a result of scant attention being paid to cyber security. The resilience assessment is generic and not specified for organisations.

Organisation-specific assessment of resilience is not possible

It is not possible to make a specific assessment of the resilience of organisations in the Netherlands to the threats as identified in this CSAN. There is simply no clear picture as to what measures have been taken by organisations. New vulnerabilities crop up on regular basis, cyber actors are evolving and unforeseen disruptions and outage can occur as a result of, for instance, the fragility of the Internet. Measures that currently result in an acceptable level of resilience could prove to be insufficient based on new insights.

Measures are usually available but are not always implemented

Implementing basic measures ensures that the cyber security within an organisation is brought up to a certain level. These measures provide protection against a wide range of attacks carried out by various actors. Incidents have revealed that organisations do not always implement basic measures.

During the reporting period there were many incidents where basic measures could have mitigated the damage or even prevented the incidents. Manifestations with major consequences, such as WannaCry and BadRabbit, exploited known vulnerabilities. The security updates for these vulnerabilities had been available for months, but had clearly not been installed.[179] In other cases, vulnerabilities were not (or not yet) known, but basic measures would have formed a barrier or mitigated the consequences.

The impact of worms such as WannaCry, NotPetya and BadRabbit for instance, could have been reduced by, among other things, the basic measure of segmentation. The outbreaks of both WannaCry (12 May 2017) and NotPetya (27 June 2017) exploited the EternalBlue vulnerability, while critical security updates had been available for supported systems since March. The inability to implement basic measures results in reduced resilience. That effect can be seen in the roll-out of business telephones for instance. Suppliers of Android telephones are vague about the period within which they make the security updates available. If organisations do not make explicit agreements about updates with their supplier, there is a very real risk of the product being outdated as soon as it is taken into use.

Configuration errors also lead to incidents. For instance, details of energy contracts of Dutch households became publicly available online because incorrectly configured S3 buckets, which are used for data storage, had become accessible. Incorrectly configured memcached servers have been exploited to execute major DDoS attacks. Traditional attack methods, including phishing, are used to compromise the crown jewels of organisations.

The fact that cyber attacks remain undetected for a long time can also indicate that basic measures are not properly in place. Research has revealed that companies, governments and organisations in Europe often only discover that they have been the victim of a cyber attack months later.[180] Organisations' crown jewels are being successfully attacked without the use of advanced tools.

There are various reasons why organisations do not always implement known basic measures.[XII] They sometimes fall within, at other times outside an organisation's sphere of influence. An example is the growing shortage of cyber security specialists on the labour market.[181] [182] It may be assumed that in the coming year, organisations will still not implement all basic measures unless there is reason to do so, for instance a cyber incident that the organisation has fallen victim to. This lack of basic measures limits the resilience of organisations.

Resilience under further pressure

The greater the increase in complexity and connectivity, the more complicated it becomes to realise a resilient digital infrastructure. On the one hand, organic growth and the relative long service life of systems produce a more complicated landscape. On the other hand, it is more difficult to maintain a clear overview because of the increased use of shared facilities such as cloud services in the form of individual building blocks.

Where in the past services were set up within an organisation, they are now contracted-in from numerous parties and implemented externally. Control of the IT landscape remains within the organisation, while the implementation becomes fragmented across various parties. The use of various service providers and cloud services creates new dependencies and increases the scope for attack.

The digital infrastructure is complex, not all essential components are equally robust and there is a high degree of mutual dependence between components. Developers and suppliers use certain software generically as building blocks for their own work. This is often software that is developed by cooperative partnerships of volunteers. They often lack the capabilities or resources for maintaining or testing the quality of the software. Some popular protocols for data exchange via the Internet are decades old and are not resistant to contemporary attacks. Improved versions of old Internet standards (such as IPv6, or HTTPS) are being adopted slowly, as a result of which the drawbacks to the old versions (IPv4 and HTTP) will continue to be an issue for some time.

Vulnerabilities in supply chains and the way in which they can or have been exploited are referred to in various parts of this CSAN.[XIII] Cyber incidents in some parts of the chain can also result in cyber incidents elsewhere in the chain. A complicating factor is that every supplier makes choices about the importance that they assign to cyber security. What is optimal for the supplier can be suboptimal for the customers that they serve.[XIV] Conversely, a party may have organised its business properly but can still have problems as a result of an incident at the supplier. It is not easy for an individual party to find a solution to vulnerabilities in the supply chain.

The annual review describes some fundamental vulnerabilities that came to light during this reporting period. Although they have mainly been exploited in a laboratory setting, exploitation outside of the laboratory certainly cannot be excluded. Due to issues of complexity and connectivity, it is far from easy to determine where vulnerabilities are located in an organisation's infrastructure and which chain suppliers have vulnerabilities. If solutions are already known, it may take some time for them to be released and there is a risk of a vulnerability being overlooked. Implementing measures, if they do exist, is therefore troublesome and time-consuming.

As a result of this increasing complexity and connectivity, it is difficult for organisations to predict which vulnerabilities will be exploited in the future and which corresponding measures to combat them should be implemented straight away. Organisations will be confronted with surprises such as unexpected incidents and chain effects. These uncertainties, the so-called 'unknown unknowns', are the result of the complexity of the digital infrastructure.

Resilience of organisations: a game of cat and mouse

Although the threat assessment has not changed fundamentally, cyber actors have been innovating. For instance, they take advantage of newly discovered vulnerabilities. The makers of WannaCry are an example of this trend: relatively shortly after the vulnerability became public, they were able to exploit it on a large scale.

For a long time now, collecting money using money mules has been a vulnerable component of criminal operations. Ransomware makes collecting money less vulnerable and the relatively new cryptojacking makes collecting money more robust. There is also a professional sector of products and services available at a low threshold which can be used to perpetrate digital attacks, and this sector is also innovating.

It is likely that cyber actors are also evolving and adapting to the measures implemented within organisations. For instance, state actors who in principle could use advanced knowledge and tools prefer to use less advanced and simpler tools. Depending on the

XII A number of reasons for this are set out in the section on Conflicts of interest lead to concessions (Chapter 3).

XIII See Foreign producers and service providers have positive as well as negative effects on resilience (Chapter 1), Supply chains increase vulnerability (Chapter 2) and Chapter 4.

XIV See the section entitled Conflicts of interest lead to concessions (Chapter 3).

perceived interest, actors will use more time, money and resources to achieve the intended goals. For example, during the reporting period it was noted that cyber actors exploit vulnerabilities in supply chains.[XV]

Conversely, organisations also adapt their cyber security measures to cyber incidents. This is why, after the initial outbreak of WannaCry, Microsoft saw the need to issue the MS17-010 patch for unsupported Windows versions too and why organisations implement measures when they have suffered a ransomware infection.

Closing remarks

It is not possible to make a specific assessment of the resilience of organisations in the Netherlands to the threats as identified in this CSAN. Time and again, cyber incidents reveal that many organisations fail to implement basic measures. With respect to the current threat, these organisations are almost defenceless against malicious parties and could also become the unintended victim of cyber attacks on, via or against others.
Incidents could have been prevented or the damage mitigated if these basic measures had been implemented. Organisations' crown jewels are being successfully attacked without the use of advanced methods. Resilience is under further pressure from the increasing complexity and connectivity of the IT landscape and in some cases from scant attention being paid to cyber security. Cyber actors are playing cat and mouse with organisations. The digital resilience of the Netherlands is under pressure.

XV See the paragraph entitled Supply chains increase vulnerability (Chapter 2).

Appendices

Appendix 1
NCSC statistics

This appendix offers a summary of the reported vulnerabilities, security advisories and incidents that have been handled by the NCSC. It also contains a summary of activities within the National Detection Network (*Nationaal Detectie Netwerk*). Incidents are recorded and kept up to date using a registration system; this system comprises the source of all of the graphs below. The number of reported vulnerabilities increased substantially in the past reporting period. However, the number of other reports fell slightly.

The NCSC facilitates the submission and processing of reports within the framework of Coordinated Vulnerability Disclosure, (CVD reports) for both its own infrastructure and for that of the Dutch central government and a number of private parties. It also issues security advisories to its members and handles cyber security incidents. In addition, the NCSC is working on expanding the National Detection Network (NDN). Statistics on these topics have been calculated for this reporting period (May 2017 to April 2018 inclusive) and they are presented below. Comparing these statistics to previous reporting periods allows trends and developments to be revealed.

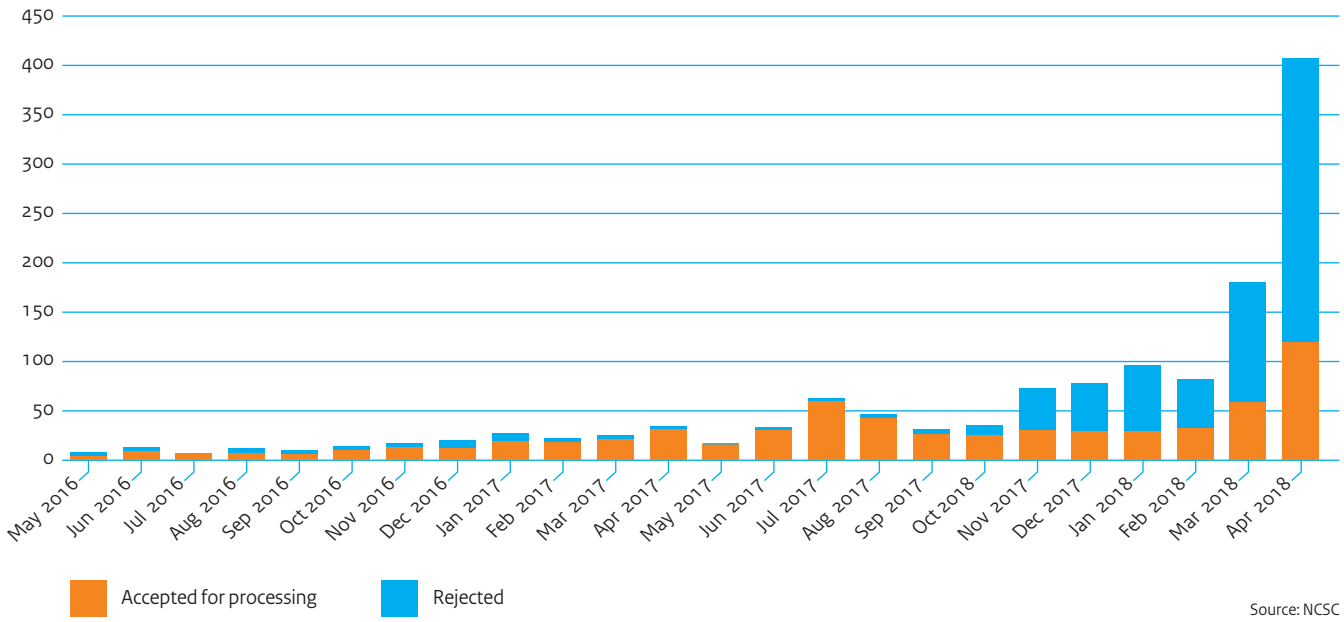
Vulnerability reports

During the reporting period, the NCSC received a total of 1,140 Coordinated Vulnerability Disclosure reports. Previously, such reports were known as Responsible Disclosure reports. On average 95 reports were received each month. These were reports for its own systems as well as for other Dutch central government systems and third-party systems. This includes reports that have resulted in the coordinated resolution and publication of newly discovered vulnerabilities in hardware and software. In some cases duplicate reports were filed for the same vulnerability by two or more researchers. As a result, the total number of reports does not match the total number of vulnerabilities.

There were 194 CVD reports in the previous reporting period. This means there was almost a sixfold increase in the current period, which can be explained by the substantial rise in the number of reports from abroad, mainly from India. Communications with a number of these reporters revealed that reporting a vulnerability and receiving a reward for it (often a T-shirt) is a way of demonstrating their cyber security knowledge to potential employers.

Figure 4 shows the number of CVD reports per month for the past two reporting periods. The numbers show an explosive growth, which has mainly taken place in the past six months. This figure also shows the relationship between reports that were or were not accepted for processing. Not only has the total number of reports increased, the percentage of reports being rejected has also grown. Six-hundred and forty (56%) were rejected in the last period, whereas forty-three (28%) were rejected in the previous period. There are various reasons for rejecting a report. If a report is made on behalf of an organisation outside the NCSC's constituency, it is rejected with a recommendation to first contact that organisation directly. A report is also rejected if, upon further investigation, it turns out that there is no vulnerability or that the security risk is negligible. In addition, a report can be rejected if the same vulnerability in the same system has been reported previously.

Figure 4 Number of CVD reports per month

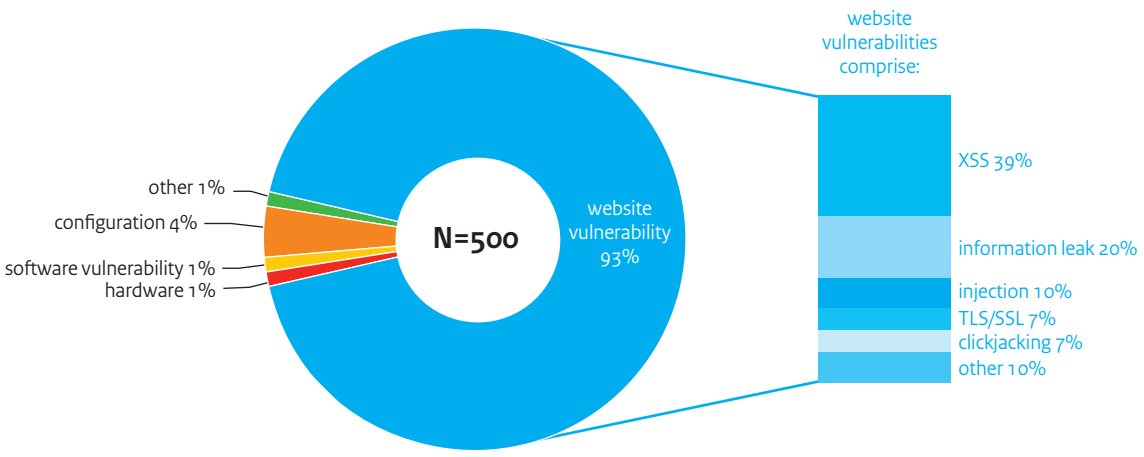


Source: NCSC

Figure 5 shows the various types of CVD reports. The majority (93%) of all reports concern a vulnerability in a website, a web application, or infrastructure on which web applications run. Examples of such reports are weak TLS parameters, cross-site scripting (XSS), SQL-, XML- and HTML injection and information leaks. An example of the latter is a vulnerability through which it is possible to view a configuration file. Only 4% of all reports relate to configuration errors in hardware and software. Relatively few reports are about vulnerabilities in software or hardware (excluding web servers and web applications).

Unlike the previous CSAN, only reports that were accepted for processing have been included here. We have chosen to do this because the number of rejected reports would otherwise distort this figure.

Figure 5 Types of CVD reports



Source: NCSC

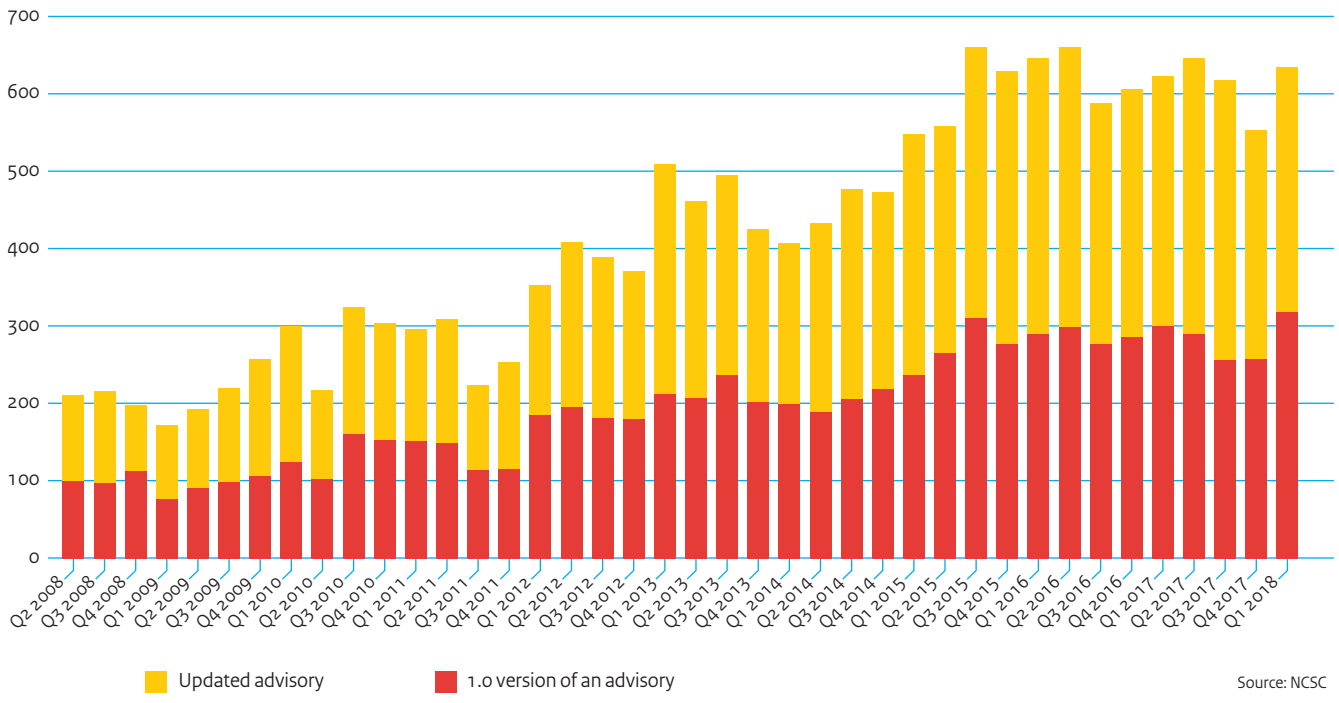
Security advisories

The NCSC publishes security advisories for software and hardware vulnerabilities or perceived threats. A security advisory describes the problem at hand, what systems may have been affected and what should be done to prevent a vulnerability being exploited.

Figure 6 shows the number of security advisories that the NCSC published per quarter between the second quarter of 2008 and the first quarter of 2018. Here, a distinction is made between new security advisories (with version number 1.0) and updates to existing security advisories. In total, the NCSC published 1,100 new security advisories during the past reporting period, which is about 7% less than the year before. The number of updates to existing security advisories also fell slightly to 1,289, representing a decrease of approximately 4%.

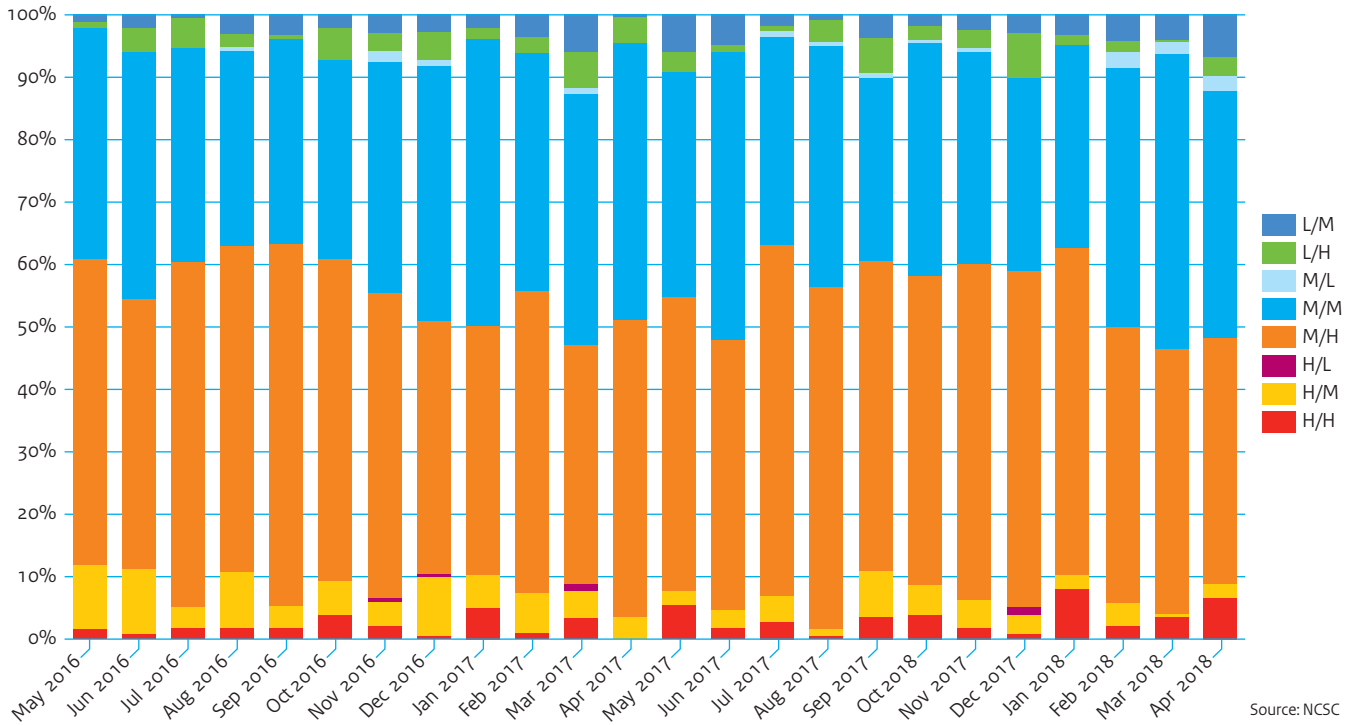
The NCSC security advisories are classified according to two elements. Firstly, the NCSC determines the likelihood that the vulnerability will be exploited. Secondly, it determines the damage that occurs when the vulnerability is exploited. Based on a number of aspects, a level is estimated for both criteria (likelihood and damage) : High (H), Medium (M) or Low (L). For example: if there is a high likelihood that a particular vulnerability will be exploited, but the expected damage caused by the exploitation is low, the corresponding security advisory will be classified as H/L. Figure 7 shows the relationships between these levels for all published advisories (including updates) per month for the last two reporting periods.

Figure 6 **Number of security advisories per quarter (Q2 2008 – Q1 2018)**



Source: NCSC

Figure 7 **Classification of advisories per month (May 2016 – April 2018)**



Source: NCSC

Damage from vulnerabilities

Every security advisory comes with a description of the possible damage that malicious parties could inflict if the advisory is not followed-up on. Table 3 shows the percentage of advisories per damage description for the past three reporting periods. Here we can see that largest proportion of security advisories (51%) still relates to denial of service (DoS), followed by remote execution of random code with user rights (37%), access to sensitive data (33%), bypassing a security measure (19%) and escalation of privileges (17%). These were also the most common security advisories in the previous reporting period. An advisory often comes with several damage descriptions, resulting in a total percentage higher than 100%.

Table 3 **Percentage of security advisories per damage description CSAN2016 to CSAN2018**

Damage description	2016	2017	2018
Denial of Service (DoS)	56%	61%	51%
Remote code execution (user rights)	37%	42%	37%
Access to sensitive data	32%	32%	33%
Security bypass	25%	17%	19%
Privilege escalation	21%	19%	17%
Access to system data	13%	13%	14%
Cross-Site scripting (XSS)	9%	8%	9%
Manipulation of data	8%	10%	8%
Remote code execution (administrator/root rights)	6%	7%	6%
Authentication bypass	5%	3%	6%
Spoofing	5%	5%	4%
Cross-Site Request Forgery (XSRF)	2%	2%	1%
SQL injection	2%	1%	1%

Source: NCSC

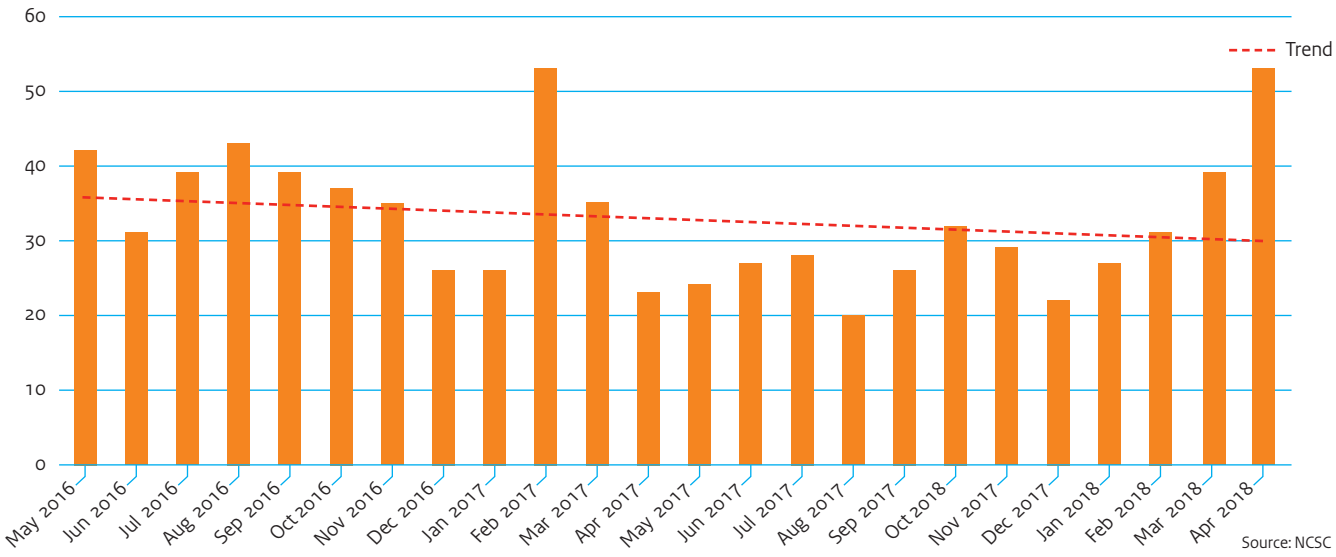
Cybersecurity incidents registered with the NCSC

The NCSC assists the Dutch central government and organisations in critical sectors in the handling of incidents in the field of IT security. In this role, the NCSC receives reports of incidents and vulnerabilities and also identifies incidents and vulnerabilities itself, based on various different detection mechanisms and its own research for example. At the request of national and international parties, the NCSC supports Dutch internet service providers in combating cyber incidents that originate from a malicious web server in the Netherlands, for example, or from infected computers in the Netherlands.

Number of incidents handled

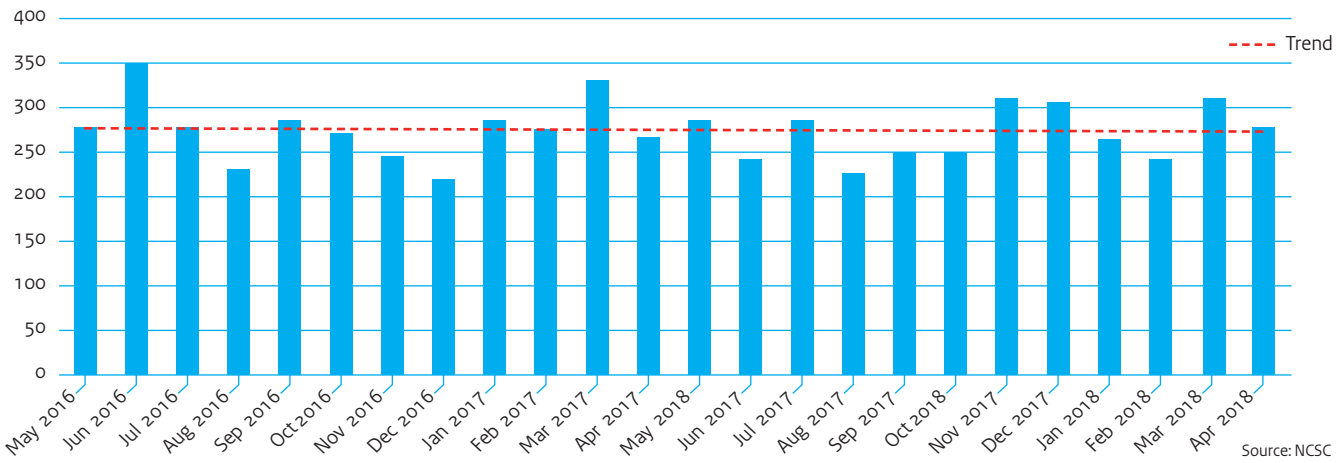
The number of incidents handled per month in the last two reporting periods is shown in figure 8. The automated checks and CVD reports are not included here. They are both shown in separate graphs in this appendix. A total of 358 incidents were reported in the past reporting period; approximately 30 per month. Four-hundred and twenty-nine were reported in the previous reporting period; approximately 36 per month. Compared with the previous reporting period, the major differences can be found in the number of reports of phishing (20% decrease) and malware infections (30% decrease). The decrease could be explained by the fact that organisations are reporting basic incidents less often because they are considered to be a 'going concern'. A consequence of the refinement of the NCSC's constituency as result of the Dutch

Figure 8 **Incidents handled (excluding automated checks and CVD reports)**



Source: NCSC

Figure 9 **Automated checks**



Source: NCSC

Data Processing and Cybersecurity Notification Obligation Act (Wet gegevensverwerking en meldplicht cybersecurity, WGMC) is that incidents at certain organisations are no longer reported to the NCSC. No reports were filed under the WGMC notification obligation during the reporting period.

Figure 9 shows the results of automated checks for the past two reporting periods. An average of 270 incidents were reported per month in the past period. That was an average of 275 in the previous period. A report may concern several infected systems within an organisation.

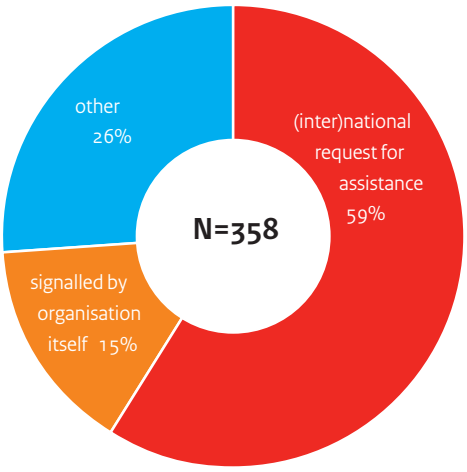
Distribution of incidents per report, category and handling

Figure 10 shows the distribution of incidents according to reporting type. This shows how an incident was reported to the NCSC. Most incident reports (59%) come from outside: from national or international sources. In 20% of all cases, it concerns signalling by the organisation itself. Examples include a warning from an organisation's own detection mechanism or a message from a public source. The remaining 21% of the reports concern information accepted as notification or other various reports.

Figure 11 shows the distribution of incidents per category. The NCSC has used the incident taxonomy specified by CERT.PT and ENISA for this distribution.[183] The inner ring shows the main categories, the outer ring shows the subcategories. Occasionally, a single incident may have more than one aspect which falls under various possible categories in the taxonomy. To prevent overlap, in these cases the NCSC has chosen to base the selection of single categories on the main or most important aspect of the incident concerned.

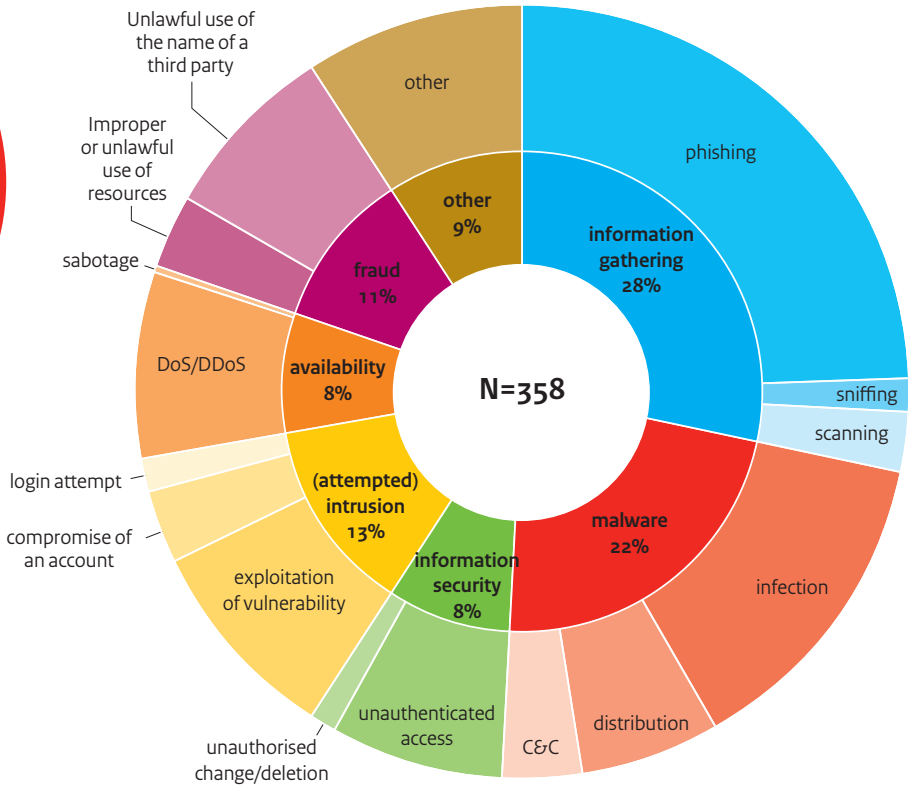
Over one quarter of the incidents (28%) appear to concern information gathering. The vast majority of these concern phishing. Malware incidents account for 22% of all incidents. The majority of these relate to malware infections. In 8% of all cases there was unauthorised access or exploitation of the vulnerability and 13% involved (attempted) intrusions. Here too, it mainly concerns exploitation of a vulnerability. Only 8% of all incidents related to availability. Almost all of these incidents were related to (D)DoS attacks or threats. Eleven percent of all incidents related to fraud. An example of this is the unlawful use of the name or logo of a third party. The remainder (9%) was due to various incidents, including sending spam.

Figure 10 **Incidents handled per reporting type**



Source: NCSC

Figure 11 **Incidents handled per category**



Source: NCSC

Compared with the distribution of incidents in the preceding reporting period, we can see a decrease in the percentages of both information security and (attempted) intrusions. This can largely be explained by the fact that, unlike previously, no CVD reports have been included in the graph. Given the large increase in CVD reports, they are now shown above in separate graphs.

Figure 12 shows the distribution of incidents by handling. Incident handling is independent of how the report was received or which category the incident falls into, and the figure only reflects the actions that were carried out. The NCSC provided remote support in 67% of all incidents. In 20% of all incidents, the NCSC issued a 'notice-and-take-down' (NTD) request. This is done if a malicious website, a phishing website for instance, must be taken off-line. If an incident turns out to be a false positive, or if information is accepted as a notification, the incident is registered as not having been handled. This was the case for 9% of all reports. The NCSC only provided on-site support in a few cases (3%). Generally speaking, these ratios are the same as in the previous reporting period.

Division of incidents between government and critical sectors

The NCSC supports both the Dutch central government and the critical infrastructure in security incidents. In addition, the NCSC acts as a point of contact for international requests for assistance concerning information security. Figure 13 shows the distribution of the number of incidents handled, divided into public, private and international parties. A total of approximately 38% of the incidents involved a public organisation and 42% involved a private organisation. The remaining 20% involved an international party. An example of this is the receipt of a malware report from a fellow CSIRT organisation in another country. A foreign organisation can also ask the NCSC to have a malicious website, which is hosted in Netherlands, taken off-line.

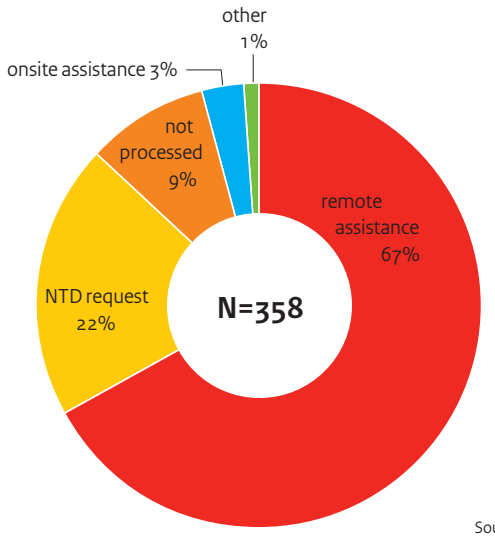
Figure 14 shows the distribution between incident categories per type of organisation. The bottom of each column shows the type of organisation the distribution concerns and the number of incidents it represents.

Approximately 20% of all incidents involved malware, regardless of the type of organisation. The difference is even greater for incidents in the 'gathering of information' category. Thirty-six percent of all cases involving an international party fall into this category. In practice, most of these incidents involved phishing campaigns. This figure also shows that (attempted) intrusion occurs more frequently in incidents in the private sector (17%) than when a public party (12%) or an international party (9%) is involved.

A similar distribution can also be seen with incidents involving information security. Such incidents are often related to unauthorised access to sensitive information or systems. This type of incident is more often reported from the public sector (14%) than from the private sector (5%) or an international party (4%). An example of this is the reporting of a website vulnerability that allows an attacker to view a customer database. Incidents involving an attack on the availability of an organisation are reported more often from the public sector (12%) than from the private sector (7%) or an international party (4%).

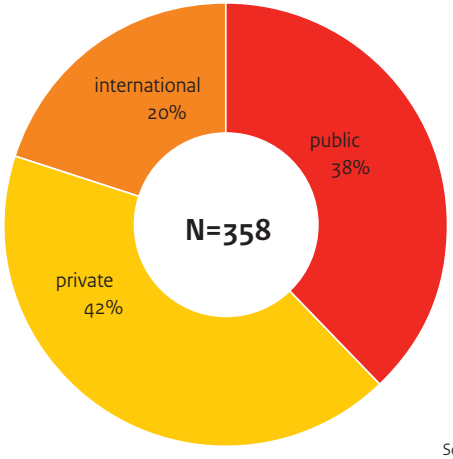
Where phishing is involved, a distinction is made between phishing campaigns focusing on obtaining login details, which fall under information gathering, and websites that are used in phishing campaigns which misuse the name, the logo or the corporate identity of third party without permission, which falls under fraud. Just as with information gathering, the fraud category is much more prevalent with international parties (17%) than with private parties (13%) or public parties (5%).

Figure 12 **Incidents handled, by handling**



Source: NCSC

Figure 13 **Incidents handled by type of organisation**



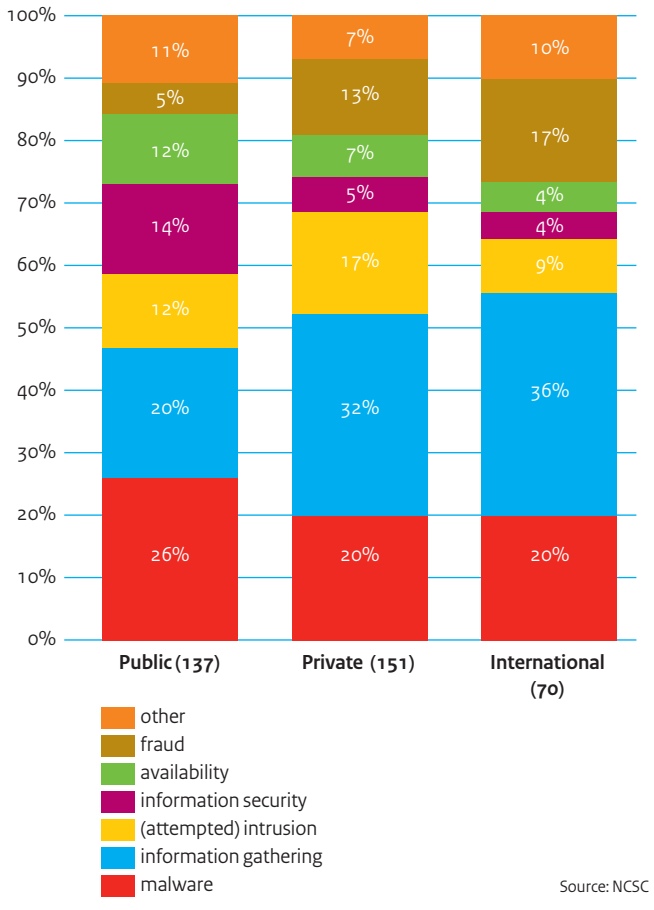
Source: NCSC

National Detection Network

The National Detection Network (NDN) is a collaboration allowing digital threats and risks to be detected more quickly and effectively. By sharing threat information, parties can implement suitable measures on their own initiative to mitigate or prevent possible damage.

Within the NDN, 'indicators of compromise' (IoCs) are shared with participating parties. An IoC is information that can help in identifying specific malicious behaviour on a system or in a network. In practice, this information often concerns IP addresses or domain names. If a shared IoC leads to the detection of malicious behaviour at a participating party, this is known as a 'hit'. A hit only indicates that behaviour has been observed that matches the shared information. However, it does not necessarily mean that a participating party has been compromised. If a defensive measure, such as a firewall, antivirus or intrusion detection system (IDS) prevents the malicious software or network traffic, this is recorded as a 'hit' even though no actual infection has taken place.

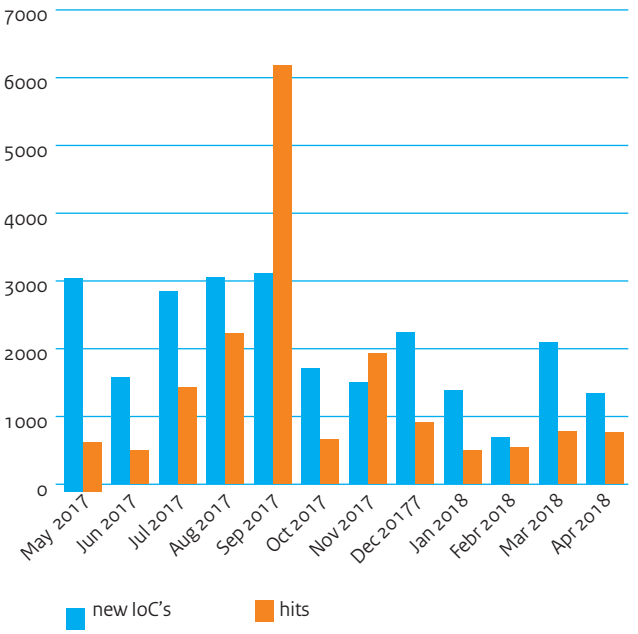
Figure 14 **Incident categories per type of organisation**



Source: NCSC

Figure 14 shows the number of new IoCs that have been actively shared within the NDN. It also shows the number of hits. In total, 25,049 new IoCs have been shared, approximately 2,087 a month. Only a small number of these are actually encountered. In total, 17,506 hits were observed, approximately 1,459 a month. There was a relatively large number of hits in September, as a result of a major phishing campaign.

Figure 15 **Active IoCs and Hits**



Source: NCSC

Appendix 2
Terms and abbreviations

0-day	See Zero-day vulnerability.
Attack	A digital attack is an intentional breach of cyber security.
Attack facilitator	A criminal who develops and exploits the tools and infrastructure to allow other actors to perpetrate digital attacks for a price.
Actor	Person, group or organisation that forms a threat.
AIVD	General Intelligence and Security Service (Algemene Inlichtingen- en Veiligheidsdienst).
AP	Dutch Data Protection Authority (Autoriteit Persoonsgegevens).
Authentication	Establishing the identity of a user, computer or application.
Availability	Availability means ensuring that users, authorised by virtue of their duties, have prompt and timely access to information and the related assets (information systems).
Bitcoin	A digital unit of currency, see crypto currency.
Botnet	A collection of infected systems that can be controlled centrally by actors. Botnets form the infrastructure for many types of Internet crime.
Breakdown	See outage or disruption.
Cloud service	IT infrastructure that is made available as a service via the Internet.
Confidentiality	Confidentiality means ensuring that information can only be accessed by those who are authorised to do so.
Criminal	An actor who perpetrates attacks with an economic or financial motive.
Cryptojacking	Using the computing power of systems (without the knowledge of the owner) to mine for cryptocurrency.
Cryptomining	Mining for cryptocurrency by performing cryptographic calculations.
Cryptocurrency	An umbrella term for digital currencies whereby cryptographic calculations are used as an authenticity feature and for transactions.

CVD	Coordinated Vulnerability Disclosure is the practice of responsibly reporting any security leaks found. Responsible disclosure is based on agreements that usually mean that a reporter will not share his or her discovery with third parties until the leak has been repaired, and the affected party will not take legal action against the reporter. This was previously known as responsible disclosure.
Cybercrime	A form of crime aimed at IT or the information processed by an IT system. There are various types of cybercrime: • in the narrow sense, a type of criminal activity which targets IT (high-tech crime); • a type of criminal activity where the use of IT is a prime consideration in its perpetration (cybercrime); • in a broad sense, any form of (traditional) criminal activity where IT is used (digital crime).
Cybercrime-as-a-service	Cybercrime-as-a-service is a method used in the underground economy in which actors can use the (paid) services of an attack facilitator to perpetrate attacks.
Cyber vandal	See script kiddie.
Cyber security	Cyber security is the entirety of measures to prevent damage caused by disruption, outage or misuse of IT and repair it should it occur. This damage could comprise impairing the availability, confidentiality or integrity of information systems and information services and information stored on them.
DDoS	Distributed Denial of Service is the name of a type of DoS whereby a particular service (a website for instance) is made inaccessible by bombarding it with heavy network traffic from a large number of different sources.
Defacement	A defacement is the replacement of a web page with a message that it has been hacked, possibly with additional messages of an activist, idealist or repugnant nature.
Disruption	The intentional, temporary impairment of the availability of information, information systems or information services.
DKIM	DomainKeys Identified Mail is a protocol that allows the sending mail server to place digital signatures in legitimate emails. The owner of the sending domain publishes legitimate keys in a DNS record.
DMARC	Domain-based Message Authentication, Reporting and Conformance is a protocol used by the owner of a domain to indicate what needs to be done with non-authentic emails from their domain. The authenticity of emails will initially be determined on the basis of SPF and DKIM. The domain owner publishes the desired policy in a DNS record.
DNS	The Domain Name System links internet domain names to IP addresses and vice versa. For example, the website 'www.ncsc.nl' represents IP address 159.46.193.36. In addition, a DNS record specifies how emails to that domain should be processed, among other things.
DoS	Denial of Service is the name for a type of attack that makes a particular service (a website for example) inaccessible to the customary users of that service. Websites are usually attacked by a DDoS attack.
Encryption	Encoding information to make it unreadable for unauthorised persons.
Espionage	Impairing the confidentiality of information by state or state-sponsored actors copying or removing information.
Exploit	Software, data or a series of commands that exploit a hardware or software vulnerability for the purpose of creating undesired functions or behaviour.

Exploit kit	A tool used to set up an attack by choosing from ready-made exploits, in combination with desired effects and method of infection.
Hacker/Hacking	The most conventional definition of a hacker (and the one used in this document) is someone who attempts to break into IT systems with malicious intent. Originally, the term hacker was used to denote someone using technology (including software) in unconventional ways, usually with the objective of circumventing limitations or achieving unexpected effects.
Hacktivist	Contraction of the words hacker and activist: actor who mounts digital attacks motivated by a certain ideology.
ICS	Industrial Control Systems are measurement and control systems used, for example, to control industrial processes or building management systems. ICSs collect and process measurement and control signals from sensors in physical systems and control the corresponding machines or devices.
Incident	An incident is an event where information, information systems or information services are disrupted, fail or are misused.
Information security	Information security is the process of establishing the required reliability of information systems in terms of confidentiality, availability and integrity, as well as implementing, maintaining and monitoring a coherent set of corresponding security measures.
Information theft	Impairing the confidentiality of information by copying or removing information.
Information manipulation	Intentionally changing information; impairing the integrity of the information.
Injection	A method of attack where user input is manipulated to contain data other than system commands. SQL injection is often used to influence communication between an application and the underlying database, to manipulate or steal data.
Insider	An internal actor who, with access to systems or networks from the inside, is a threat with the motive of revenge, monetary gain or ideology. An insider can also be hired-in or instructed from outside.
Integrity	Integrity entails guaranteeing the correctness and completeness of information and its processing.
IoT	The Internet of Things is a network of smart appliances, sensors and other objects (often connected to the Internet) that collect data on their environment, can exchange this data and make (semi-) autonomous decisions or take actions that affect their environment based on it.
IP	The Internet Protocol handles the addressing of Internet traffic so that it arrives at its intended destination.
Leak	Impairment of confidentiality as result of natural, technical or human failures.
Malware	Contraction of malicious software. Malware is used as a generic term for viruses, worms and Trojans, among other things.
MIVD	Military Intelligence and Security Service (Militaire Inlichtingen- en Veiligheidsdienst).
Outage	Impairment of integrity and availability as result of natural, technical or human failures.
Phishing	An umbrella term for digital activities with the object of tricking people into giving up their data. This information can be exploited for, for instance, fraud or identity theft.

Ransomware	Gijzelsoftware in Dutch. Type of malware that blocks systems or the information they contain and only makes them accessible again against payment of a ransom.
Sabotage	The intentional, very long-term, impairment of the availability of information, information systems or information services. In extreme cases, it leads to destruction.
Script kiddie	An actor with limited knowledge who draws on tools which have been devised and developed by others, for cyber attacks, to demonstrate vulnerabilities or as a challenge.
Spam	Unwanted email, usually of a commercial nature.
Spear phishing	Spear phishing is a version of phishing that is directed against a single person, or limited group of people, deliberately targeted for their position of access in order to achieve as big an effect as possible without being noticed.
SPF	Sender Policy Framework is a protocol used by the owner of a domain name to indicate which servers are allowed to send legitimate emails on behalf of his or her domain. The owner of the domain name publishes the list of authorised servers in a DNS record.
State-sponsored actor	An actor sponsored by a state actor.
State actor	Nation-states digitally attack other countries, organisations or individuals, primarily for geopolitical motives. Their objective is to acquire strategic information (espionage), to influence public opinion or democratic processes (influencing), to disrupt critical systems (disruption) or even to destroy them (sabotage).
System manipulation	Impairing information systems or information services targeting the confidentiality or integrity of information systems or information services. These systems or services are then used to perpetrate other attacks.
Terrorist	Actor with ideological motives who endeavours to realise social change, to spread fear among groups of the population or to influence political decision-making processes by using violence against people or by causing disruptive damage.
Tool	A technology or computer program used by an attacker to exploit or increase existing vulnerabilities.
Trojan	A type of malware that provides an attacker with secret access to a system via a backdoor.
Two-factor authentication	A method of establishing identity, requiring two independent proofs of an identity.
Vulnerability	Characteristic of a society, organisation or (parts of an) information system that allows an attacker to hinder and influence the legitimate access to information or functionality, or to access it without the proper authorisation.
Wiperware	A type of malware that commits sabotage by deleting data or making it permanently inaccessible.
Worm	A type of malware that automatically propagates itself to other systems.
Zero-day vulnerability	A zero-day vulnerability is a vulnerability for which no patch is yet available because the developer of the vulnerable software has not yet had time (zero days) to repair the vulnerability.

Appendix 3
Sources and references

1 National Cyber Security Agenda 2018.
2 Economic Impact of Cybercrime - No Slowing Down, McAfee & CSIS, February 2018, p 3 and Cyber Security Risk Assessment for the Economy (Risicorapportage Cyberveiligheid Economie), Bureau for Economic Policy Analysis (Centraal Planbureau), The Hague, 3 July 2017, pp 8–11.
3 ENISA Threat Landscape Report 2017. 15 Top Cyber-Threats and Trends, ENISA, January 2018, p 107.
4 General Intelligence and Security Service Annual Report 2017 (Jaarverslag AIVD 2017), DNI Worldwide threat assessment (2018).
5 General Intelligence and Security Service Annual Report 2017 (Jaarverslag AIVD 2017) p 8 et seq.
6 ENISA Threat Landscape Report 2017 (2018).
7 Crowdstrike 2018 Global Threat Report. Blurring the lines between statecraft and tradecraft.
8 Kaspersky, Spy wars: how nation-state backed threat actors steal from and copy each other, October 2017. Blurring lines, also in FireEye Looking ahead: cyber security in 2018 and DNI Worldwide threat assessment (2018).
9 FireEye Looking ahead: cyber security in 2018.
10 General Intelligence and Security Service Annual Report 2017 (Jaarverslag AIVD 2017).
11 DNI Worldwide threat assessment (2018).
12 MMC CYBER HANDBOOK 2018. Perspectives on the next wave of cyber.
13 https://citizenlab.ca/2014/02/mapping-hacking-teams-untraceable-spyware/, consulted on 7 May 2018.
14 M-trends 2018.
15 FireEye Looking ahead: cyber security in 2018.
16 https://www.kaspersky.com/blog/new-ransomware-epidemics/17314/, consulted on 9 April 2018.
17 https://www.kaspersky.com/blog/new-ransomware-epidemics/17314/, consulted on 9 April 2018.
18 http://www.wired.co.uk/article/what-is-eternal-blue-exploit-vulnerability-patch, consulted on 11 April 2018.
19 https://securelist.com/expetrpetyanotpetya-is-a-wiper-not-ransomware/78902/, consulted on 9 April 2018.
20 http://www.bbc.com/news/technology-40428967, consulted on 9 April 2018.
21 https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe, consulted on 9 April 2018.
22 https://www.theguardian.com/world/2017/jun/27/petya-ransomware-attack-strikes-companies-across-europe, consulted on 9 April 2018.
23 http://www.ictmagazine.nl/maersk-lijdt-rond-300-miljoen-schade-ransomware-aanval/, consulted on op 9 April 2018.
24 https://tweakers.net/nieuws/134473/maersk-herinstalleerde-45000-pcs-in-10-dagen-na-notpetya-aanval.html, consulted on 9 April 2018.
25 https://nos.nl/artikel/2180251-nieuwe-aanvallen-met-gijzelvirus-ook-pakketbezorger-tnt-getroffen.html, consulted on 11 April 2018.
26 http://blog.talosintelligence.com/2017/07/the-medoc-connection.html, consulted 9 April 2018.
27 https://www.wired.com/story/white-house-russia-notpetya-attribution/, consulted on 9 April 2018.
28 https://www.sentinelone.com/wp-content/uploads/2017/06/BlackEnergy3_WP_012716_1c.pdf, consulted on 12 April 2018.
29 The use of spear phishing by Russian actors has, for example, been extensively documented in F-Secure, The Dukes. 7 years of Russian cyberespionage.
30 For example, in 'Study reveals North Korean cyber-espionage has reached new heights', The Guardian 20 February 2018, consulted on 12 April 2018.

31 General Intelligence and Security Service Annual Report 2017 (Jaarverslag AIVD 2017); https://nos.nl/artikel/2207027-duitse-inlichtingenchef-china-rekruteert-via-linkedin.html, consulted on 30 March 2018.
32 ENISA Threat Landscape Report 2017 (2018) and Verizon 2018 Data Breach Investigations Report.
33 The 'Are you aware of the risks from cyber espionage?' brochure (Bent u zich bewust van de risico's van cyberspionage?) (General intelligence and security service, Military Intelligence and Security Service 2017) covers the basic measures that can be taken.
34 IBM X-Force Threat Intelligence Index 2018, 24.
35 DNI Worldwide threat assessment (2018).
36 Cyber Security Assessment Netherlands 2017.
37 Symantec 2018 cyber security predictions.
38 Crowdstrike 2018 Global Threat Report. Blurring the lines between statecraft and tradecraft; IBM X-Force Threat Intelligence Index 2018.
39 General Intelligence and Security Service Annual Report 2017 (AIVD Jaarverslag 2017).
40 https://www.nu.nl/internet/5206289/duizenden-nederlandse-identiteitsdocumenten-jarenlang-openbaar-datalek.html, consulted on 4 April 2018.
41 Press release by the Dutch Data Protection Authority. '10,000 data leaks reported in 2017' (Persbericht Autoriteit Persoonsgegevens, '10.000 datalekken gemeld in 2017'), 29 March 2018.
42 General Intelligence and Security Service Annual Report 2017 (Jaarverslag AIVD 2017); ENISA Threat Landscape Report 2017 (2018).
43 ENISA Threat Landscape Report 2017 (2018).
44 M. de Bruijne, M. van Eeten, C. Hernandez Ganan, W. Pieters, Towards a new cyber threat actor typology. A hybrid method for the NCSC cyber security assessment (TU Delft 2017).
45 https://nos.nl/artikel/2214400-zware-ddos-aanvallen-wie-wat-waar-en-waarom.html, consulted on 11 April 2018.
46 https://nos.nl/artikel/2215746-verdachte-ddos-aanvallen-banken-moeten-het-op-orde-hebben.html, consulted on 11 April 2018.
47 https://nos.nl/artikel/2215507-18-jarige-brabander-opgepakt-voor-recente-ddos-aanvallen.html, consulted on 11 April 2018.
48 Cyber Security Assessment Netherlands 2016 and Cyber Security Assessment Netherlands 2014.
49 https://www.bankinfosecurity.com/interviews/crime-as-service-top-cyber-threat-for-2017-i-3406, consulted on 29 March 2018.
50 Cyber Security Assessment Netherlands 2016 and Cyber Security Assessment Netherlands 2013, p 64.
51 https://nakedsecurity.sophos.com/2017/12/14/starbucks-wi-fi-hijacked-customers-laptops-to-mine-cryptocurrency/, consulted on 11 April 2018.
52 https://www.security.nl/posting/552971/Microsoft+detecteert+uitbraak+van+cryptomining-malware, consulted on 11 April 2018.
53 https://www.security.nl/posting/555742/Cryptominers+in+browser+steeds+lastiger+te+detecteren, consulted on 11 April 2018.
54 https://www.telegraph.co.uk/technology/2018/02/14/salon-website-asks-readers-mine-cryptocurrency/, consulted on 11 April 2018.
55 https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/, consulted on 30 March 2018
56 MMC CYBER HANDBOOK 2018. Perspectives on the next wave of cyber; ENISA Threat Landscape Report 2017 (2018).
57 https://www.independent.co.uk/travel/news-and-advice/eurocontrol-air-traffic-systems-failure-flights-cancelled-delays-a8286651.html, consulted on 9 April 2018.
58 https://www.documentcloud.org/documents/4427886-Level-3-FCC-report.html, consulted on 11 May 2018.
59 https://www.bleepingcomputer.com/news/software/software-bug-behind-biggest-telephony-outage-in-us-history/, consulted on 7 May 2018.
60 https://nos.nl/artikel/2229927-reconstructie-hoe-het-zondag-misging-op-schiphol.html, consulted on 3 May 2018.
61 The economic and social imperative for more cybersecurity. Effective Digital Defences (Nederland digitaal droge voeten), September 2016 (https://www.cybersecurityraad.nl/binaries/CybersecurityAdviesHernaVerhagen_tcm56-122110.pdf).
62 Confidence in the future. Coalition agreement 2017–2021 VVD, CDA, D66 and ChristenUnie, 2017 (https://www.tweedekamer.nl/sites/default/files/atoms/files/regeerakkoord20172021.pdf).
63 Cyber Security Risk Assessment for the Economy, (Risicorapportage Cyberveiligheid Economie), Bureau for Economic Policy Analysis, 3 July 2017 p 1 (https://www.cpb.nl/publicatie/risicorapportage-cyberveiligheid-economie), consulted on 28 March 2018.
64 The public core of the Internet. Towards a Foreign Internet Policy, Scientific Council for Government Policy (Naar een buitenlands internetbeleid, Wetenschappelijke Raad voor het Regeringsbeleid), Amsterdam: Amsterdam University Press, 2015.
65 Worldwide for a safe Netherlands. Integrated Foreign and Security Strategy 2018–2022, Ministry of Foreign Affairs, 2018 (Wereldwijd voor een veilig Nederland. Geïntegreerde Buitenland- en Veiligheidsstrategie 2018–2022, Ministerie van Buitenlandse Zaken, 2018) (https://www.rijksoverheid.nl/documenten/rapporten/2018/03/19/notitie-geintegreerde-buitenland--en-veiligheidsstrategie-gbvs).
66 https://www.nctv.nl/binaries/strategie-nationale-veiligheid-2007_tcm31-32502.pdf, consulted on 7 May 2018.
67 National Security Profile (Nationaal Veiligheidsprofiel) 2016, Bilthoven, 2016, p 9.
68 Cyber Security Assessment Netherlands 2015, p 64.
69 Electricity provision in the face of ongoing digitalisation (Stroomvoorziening onder digitale spanning), Rli, March 2018 (http://www.rli.nl/publicaties/2018/advies/stroomvoorziening-onder-digitale-spanning), consulted on 30 March 2018.
70 National Security Profile (Nationaal Veiligheidsprofiel) 2016, Bilthoven, 2016, pp 117–133.

71 AIVD Annual Report 2017 (Jaarverslag 2017, AIVD), March 2018, p 10 (www.aivd.nl/jaarverslag2017).
72 AIVD Annual Report 2017 (Jaarverslag 2017, AIVD), March 2018, p 8.9 (www.aivd.nl/jaarverslag2017).
73 National Security Profile (Nationaal Veiligheidsprofiel) 2016, Bilthoven, 2016, p 123.
74 Risk Report on the Cyber Security of the Economy (Risicorapportage Cyberveiligheid Economie), Bureau for Economic Policy Analysis, the Hague, 3 July 2017, p 3.
75 Economic Impact of Cybercrime - No Slowing Down, McAfee & CSIS, February 2018, pp 8–9.
76 NRC research: bringing down of central government computers only just averted (platgaan computers Rijk nét afgewend), NRC, 10 September 2011 consulted on 26 March 2018.
77 https://www.security.nl/posting/550347/Britse+overheid+beschuldigt+Rusland+van+NotPetya-aanval, consulted on 26 March 2018.
78 http://data.consilium.europa.eu/doc/document/ST-7925-2018-INIT/en, consulted on 11 May 2018.
79 Towards a safe, connected, digital society. Recommendation on the cybersecurity of the Internet of Things (IoT) (Advies inzake de cybersecurity van het Internet of Things (IoT)), Cyber Security Council, 11 February 2018 (https://www.cybersecurityraad.nl/binaries/CSR%20Advies%20IoT%20digitale%20oversie%20DEF%20NED_tcm56-298518.pdf), consulted on 5 April 2018.
80 Letter to Parliament on the Government Position on Encryption (Kamerbrief over Kabinetsstandpunt encryptie), 4 January 2016 (https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/kamerstukken/2016/01/04/tk-kabinetsstandpunt-encryptie/tk-kabinetsstandpunt-encryptie.pdf), consulted on 30 March 2018 and Cyber Resilience Playbook for Public-Private Collaboration, World Economic Forum, January 2018 (http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf), consulted on 6 April 2018.
81 Cyber Resilience Playbook for Public-Private Collaboration, World Economic Forum, January2018 (http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf), consulted on 6 April 2018 and Cyber Security Risk Assessment for the Economy (Risicorapportage Cyberveiligheid Economie), Bureau for Economic Policy Analysis, the Hague, 3 July 2017, p 2.
82 https://www.security.nl/posting/534770/Symantec+geeft+overheden+geen+toegang+meer+tot+broncode, consulted on 6 April 2018 and https://www.security.nl/posting/537021/McAfee+geeft+overheden+geen+toegang+meer+tot+broncode, consulted on 6 April 2018.
83 Cyber Resilience Playbook for Public-Private Collaboration, World Economic Forum, January 2018, p 6 (http://www3.weforum.org/docs/WEF_Cyber_Resilience_Playbook.pdf, consulted on 6 April 2018).
84 https://www.security.nl/posting/526657/Onderzoeker%3A+Lek+in+zonnepanelen+kan+stroomvoorziening+ontregelen, consulted on 7 May 2018.
85 http://www.rli.nl/publicaties/2018/advies/stroomvoorziening-onder-digitale-spanning, consulted on 30 March 2018.
86 Cyber Security Assessment Netherlands 2017.
87 https://www.aivd.nl/publicaties/jaarverslagen/2018/03/06/jaarverslag-aivd-2017, consulted on 30 March 2018.
88 https://www.welivesecurity.com/wp-content/uploads/2017/06/Win32_Industroyer.pdf, consulted on 13 April 2013.
89 https://nos.nl/artikel/2177859-waarschuwing-voor-industroyer-het-virus-dat-stroomnet-kan-platleggen.html, consulted on 13 April 2018.
90 https://dragos.com/blog/crashoverride/CrashOverride-01.pdf, consulted on 13 April 2018.
91 https://www.zscaler.com/blogs/research/analysis-sandworm-cve-2014-4114-0-day, consulted on 13 April 2018.
92 https://securityaffairs.co/wordpress/62782/hacking/dragonfly-2-0-campaigns.html, consulted on 13 April 2018.
93 https://threatmatrix.cylance.com/en_us/home/energetic-dragonfly-dymalloy-bear-2-0.html, consulted on 13 April 2018.
94 https://www.us-cert.gov/ncas/alerts/TA17-293A, consulted 13 April 2018.
95 https://www.us-cert.gov/ncas/alerts/TA18-074A, consulted on 13 April 2018.
96 https://www.nytimes.com/2018/03/15/technology/saudi-arabia-hacks-cyberattacks.html, consulted on 5 April 2018.
97 https://www.nctv.nl/binaries/CSBN2017_tcm31-267075.pdf, consulted on 13 April 2018.
98 http://www.bbc.com/news/uk-politics-43062113, consulted on 13 April 2018.
99 http://www.bbc.com/news/technology-39913630, consulted on 13 April 2018.
100 https://www.nytimes.com/2017/05/12/world/europe/uk-national-health-service-cyberattack.html, consulted on 13 April 2018.
101 https://securelist.com/bad-rabbit-ransomware/82851/, consulted on 13 April 2018.
102 https://www.techrepublic.com/article/notpetya-ransomware-outbreak-cost-merck-more-than-300m-per-quarter/, consulted on 5 April 2018.
103 https://www.forbes.com/sites/thomasbrewster/2017/09/18/ccleaner-cybersecurity-app-infected-with-backdoor/#4206ad12316a, consulted on 13 April 2018.
104 http://blog.exodusintel.com/2017/07/26/broadpwn/, consulted on 13 April 2018.
105 https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen/NCSC-2017-0838+1.00+Twee+kwetsbaarheden+ontdekt+in+Broadcom+WiFi-driver.html, consulted on 13 April 2018.
106 https://www.krackattacks.com/, consulted on 13 April 2018.
107 https://meltdownattack.com/, consulted on 13 April 2018.

108 https://www.ncsc.nl/actueel/nieuwsberichten/meltdown-en-spectre.html, consulted on 13 April 2018.
109 https://www.heise.de/ct/artikel/Super-GAU-fuer-Intel-Weitere-Spectre-Luecken-im-Anflug-4039134.html, consulted on 3 May 2018.
110 https://amdflaws.com/, consulted on 12 April 2018.
111 https://www.wired.com/story/amd-backdoor-cts-labs-backlash/, consulted on 13 April 2018.
112 https://blog.trailofbits.com/2018/03/15/amd-flaws-technical-summary/, consulted on 12 April 2018.
113 https://www.vusec.net/projects/glitch/, consulted on 3 May 2018.
114 https://www.bloomberg.com/news/articles/2017-10-02/urgent-equifax-2-5-million-more-americans-may-be-affected-by-hack, consulted on 5 April 2018.
115 https://investor.equifax.com/news-and-events/news/2018/03-01-2018-140531340, consulted on 5 April 2018.
116 https://investor.equifax.com/news-and-events/news/2017/11-09-2017-211550295, consulted on 5 April 2018.
117 https://www.nu.nl/internet/5017448/uber-verzweeg-datalek-van-57-miljoen-accounts.html, consulted on 30 March 2018.
118 https://www.nu.nl/internet/5046449/data-174000-nederlanders-gelekt-bij-uber-hack.html, consulted on 30 March 2018.
119 https://www.reuters.com/article/us-uber-cyber-payment-exclusive/exclusive-uber-paid-20-year-old-florida-man-to-keep-data-breach-secret-sources-idUSKBN1E101C, consulted on 5 April 2018.
120 https://www.nu.nl/internet/4989794/energieverbruik-alle-nederlandse-huishoudens-was-in-zien-datalek.html, consulted on 30 March 2018.
121 https://mackeepersecurity.com/post/fedex-customer-records-exposed, consulted on 5 April 2018.
122 https://www.nu.nl/internet/5206289/duizenden-nederlandse-id-bewijzen-jarenlang-openbaar-datalek.html, consulted on 5 April 2018.
123 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/01_2018-02-23_2017_jaarrapportage_algemeen.pdf, consulted on 30 March 2018.
124 https://www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/q2-2017-state-of-the-internet-security-report.pdf,cancelled, consulted on 6 April 2018.
125 https://www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/q3-2017-state-of-the-internet-security-report.pdf, consulted on 6 April 2018.
126 https://www.akamai.com/uk/en/multimedia/documents/state-of-the-internet/q4-2017-state-of-the-internet-security-report.pdf, consulted on 6 April 2018.
127 https://www.arbornetworks.com/blog/insight/hacktivism-political-protest-ddos-attacks-target-czech-republic-spain/, consulted on 13 April 2018.
128 https://www.ncsc.nl/actueel/nieuwsberichten/ncsc-waarschuwt-voor-misbruik-publiek-beschikbare-memcached-systemen-bij-ddos-aanvallen.html, consulted on 13 April 2018.
129 https://www.sidnlabs.nl/a/nieuws/een-proactieve-en-collectieve-ddos-bestrijdingsstrategie-voor-de-nederlandse-vitale-infrastructuur, consulted on 6 April 2018.
130 https://www.armor.com/app/uploads/2018/03/2018-Q1-Reports-BlackMarket-DIGITAL.pdf, consulted on 6 April 2018.
131 https://www.wired.com/story/github-ddos-memcached/, consulted on 5 April 2018.
132 http://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf, consulted on 11 April 2018.
133 https://businesstech.co.za/news/industry-news/206328/why-phishing-attacks-are-so-effective/, consulted on 11 April 2018.
134 http://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf, consulted on 11 April 2018.
135 https://nos.nl/artikel/2199450-na-apen-mailadressen-tweede-kamer-relatief-makkelijk.html, consulted on 30 March 2018.
136 https://www.ad.nl/politiek/iedereen-kan-mailen-namens-de-aivd~a0200b89/, consulted on 30 March 2018.
137 https://www.cyberscoop.com/russians-foreigners-spoofing-gov-email-dmarc-proofpoint/, consulted on 30 March 2018.
138 https://tweakers.net/nieuws/132585/apple-mail-outlook-2016-en-veel-andere-mailclients-zijn-kwetsbaar-voor-spoofing.html, consulted on 30 March 2018.
139 https://nos.nl/op3/artikel/2176061-hang-op-klik-weg-of-bel-je-oom.html, consulted on 5 April 2018.
140 https://www.aivd.nl/publicaties/jaarverslagen/2018/03/06/jaarverslag-aivd-2017, consulted on 5 April 2018.
141 https://www.justice.gov/opa/pr/nine-iranians-charged-conducting-massive-cyber-theft-campaign-behalf-islamic-revolutionary, consulted on 24 March 2018.
142 http://docs.apwg.org/reports/apwg_trends_report_h1_2017.pdf, consulted on 30 March 2018.
143 http://docs.apwg.org/reports/apwg_trends_report_q3_2017.pdf, consulted on 30 March 2018.
144 https://www.nctv.nl/binaries/CSBN2017_tcm31-267075.pdf, consulted on 30 March 2018.
145 https://info.microsoft.com/rs/157-GQE-382/images/EN-US_CNTNT-eBook-SIR-volume-23_March2018.pdf, consulted on 5 April 2018.
146 http://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_en_xg.pdf, consulted on 11 April 2018.
147 https://www.sidn.nl/a/veilig-internet/aantal-phishingsites-met-nederlandse-topmerken-ruim-40-toegenomen-, consulted on 11 April 2018.

148 https://www-cdn.webroot.com/8415/0585/3084/Webroot_Quarterly_Threat_Trends_September_2017.pdf, consulted on 12 April 2018.
149 https://www.imperva.com/blog/2018/01/our-analysis-of-1019-phishing-kits/, consulted on 11 April 2018.
150 https://info.phishlabs.com/blog/quarter-phishing-attacks-hosted-https-domains, consulted on 12 April 2018.
151 https://kasperskycontenthub.com/securelist/files/2017/12/KSB_statistics_2017_EN_final.pdf, consulted on 4 April 2018.
152 https://kasperskycontenthub.com/securelist/files/2017/12/KSB_statistics_2017_EN_final.pdf, consulted on 5 April 2018.
153 https://www.enisa.europa.eu/publications/enisa-threat-landscape-report-2017, consulted on 5 April 2018.
154 https://www.aivd.nl/publicaties/jaarverslagen/2018/03/06/jaarverslag-aivd-2017, consulted on 5 April 2018.
155 https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-3.html, consulted on 29 March 2018.
156 https://pages.checkpoint.com/global-cyber-attack-trends-2017.html?utm_source=research&utm_medium=cp-website&utm_campaign=CM_WR_18Q1_WW_Threat_Intelligence_Trends_Report_2017_H2, consulted on 11 April 2018.
157 http://www.bbc.com/news/world-europe-43003740, consulted on 11 April 2018.
158 https://www.bitsonline.com/australian-meteorology-staffers-questioned-sneaky-mining-operation/, consulted on 11 April 2018.
159 https://www.nu.nl/cryptovaluta/5154917/bedrijf-mocht-werknemer-niet-staande-voet-ontslaan-minen-bitcoins.html, consulted on 11 April 2018.
160 https://blog.malwarebytes.com/cybercrime/2018/02/state-malicious-cryptomining/, consulted on 11 April 2018.
161 https://www.proofpoint.com/us/threat-insight/post/smominru-monero-mining-botnet-making-millions-operators, consulted on 11 April 2018.
162 https://press.avast.com/cybercriminals-could-build-cryptomining-armies-using-vulnerable-iot-devices-at-mobile-world-congress-2018, consulted on 11 April 2018.
163 http://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html, consulted on 11 April 2018.
164 https://www.darkreading.com/attacks-breaches/radiflow-reveals-first-documented-cryptocurrency-malware-attack-on-a-scada-network/d/d-id/1331017?piddl_msgorder=asc, consulted on 5 April 2018.
165 https://arxiv.org/pdf/1803.02887.pdf, consulted on 4 April 2018.
166 https://www.symantec.com/blogs/threat-intelligence/browser-mining-cryptocurrency, consulted on 5 April 2018.
167 https://blog.checkpoint.com/2018/01/15/decembers-wanted-malware-crypto-miners-affect-55-businesses-worldwide/, consulted on 5 April 2018.
168 https://krebsonsecurity.com/2018/03/who-and-what-is-coinhive/, consulted on 30 March 2018.
169 https://medium.com/pcmag-access/why-hackers-love-cryptocurrency-miner-coinhive-e808c1b527fb, consulted,consulted on 13 April 2018.
170 https://tweakers.net/nieuws/135735/opt-in-variant-van-coinhive-cryptominer-wordt-nauwelijks-gebruikt.html, consulted on 12 April 2018.
171 https://wccftech.com/the-pirate-bay-cryptojacking-mine-monero/, consulted on 30 March 2018.
172 https://www.theguardian.com/technology/2017/dec/13/video-site-visitors-unwittingly-mine-cryptocurrency-as-they-watch-report-openload-streamango-rapidvideo-onlinevideoconverter-monero, consulted on 5 April 2018.
173 https://arstechnica.com/information-technology/2018/01/now-even-youtube-serves-ads-with-cpu-draining-cryptocurrency-miners/, consulted on 11 April 2018.
174 http://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html, consulted on 11 April 2018.
175 https://cloudblogs.microsoft.com/microsoftsecure/2018/03/13/invisible-resource-thieves-the-increasing-threat-of-cryptocurrency-miners/, consulted on 11 April 2018.
176 https://www.forbes.com/sites/jasonbloomberg/2018/03/04/top-cyberthreat-of-2018-illicit-cryptomining/#420b1f905ae8, consulted on 11 April 2018.
177 http://blog.talosintelligence.com/2018/01/malicious-xmr-mining.html, consulted on 11 April 2018.
178 https://www.malwarebytes.com/pdf/white-papers/CTNT-Q1-2018.pdf, consulted on 11 April 2018.
179 https://www.theregister.co.uk/2017/05/13/wannacrypt_ransomware_worm/, consulted on 2 May 2018.
180 https://www.telegraaf.nl/nieuws/1905093/cyberaanval-pas-na-half-jaar-ontdekt, consulted on 12 April 2018.
181 https://www.uwv.nl/overuwv/Images/factsheet-arbeidsmarkt-ict.pdf, consulted on 11 May 2018.
182 https://fd.nl/economie-politiek/1251379/noodklok-over-nederlandse-braindrain-bij-cybersecurity, consulted on 7 May 2018.
183 https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy, consulted on 7 May 2018.

Publication
National Coordinator for Security and Counterterrorism (NCTV)
PO Box 20301, 2500 EH The Hague, The Netherlands
Turfmarkt 147, 2511 DP The Hague, The Netherlands
+31 70 751 5050

More information
https://english.nctv.nl/
info@nctv.minvenj.nl
@nctv_nl

August 2018