



National Cyber Security Centre
Ministry of Security and Justice

Cyber Security Assessment Netherlands CSAN 2015



Cyber Security Assessment Netherlands CSAN 2015

National Cyber Security Centre

The National Cyber Security Centre (NCSC), in collaboration with the business community, government bodies and academics, is working to increase the ability of Dutch society to defend itself in the digital domain.

The NCSC supports the central government and critical infrastructure organisations by providing expertise and advice, response to threats and enhancing crisis management. In addition, the NCSC provides information and advice to citizens, the government and the business community relating to awareness and prevention. The NCSC thus constitutes the central reporting and information point for IT threats and security incidents.

The NCSC is part of the Cyber Security Department of the National Coordinator for Security and Counterterrorism (NCTV).

Collaboration and sources

In drawing up this report the NCSC gratefully used information provided by the following parties:

- The various ministries
- Military Intelligence and Security Service (MIVD)
- Defence Computer Emergency Response Team (DefCERT)
- AIVD
- National High Tech Crime Unit, Dutch National Police
- Public Prosecution Service
- Representatives of the critical infrastructure sectors and NCSC partner organisations
- National Coordinator for Security and Counterterrorism (NCTV)
- National Management Organisation for Internet Providers (Nationale Beheersorganisatie Internet Providers)
- Internet Standards Platform (Platform Internetstandaarden)
- Bits of Freedom
- ICT Netherlands
- Dutch Payments Association
- Confederation of Netherlands Industry and Employers (VNO-NCW)
- Scientific institutions
- Universities
- Experts in the field of cyber security

Their contributions, the substantive reviews as well as publicly accessible sources, information from the critical infrastructure and analyses from the NCSC, have made valuable contributions to the substantive quality of this assessment.

Table of contents

Summary	9
Introduction	15
1 Manifestations	17
2 Threats: actors	27
3 Threats: tools	35
4 Resilience: vulnerabilities	47
5 Resilience: measures	53
6 Interests	61
Appendix 1 » NCSC statistics	66
Appendix 2 » Sectoral assessment	72
Appendix 3 » Terms and abbreviations	76

Summary

The Cyber Security Assessment Netherlands (CSAN) is published annually by the National Cyber Security Centre and drawn up in close collaboration between public and private parties. The aim is to offer insight into developments, interests, threats and resilience in the field of cyber security over the period from April 2014 to April 2015.

The focus of the CSAN lies on the developments in the Netherlands, but important developments abroad have also been included. The CSAN is a factual description, with guidance based on insights and expertise from government departments, critical infrastructure sectors and the academic community. For this CSAN, the NCSC has renewed its collaboration with a large number of parties, both public parties (e.g. the police, intelligence and security services and the Public Prosecution Service), academic institutions and private parties (such as the critical infrastructure sectors).

Over the past few years, more attention has been paid to the dependence on IT. Countries attach increasing importance to the internet and IT becomes indispensable. More and more insight is gained into the number of incidents, which also allows for more targeted measures being taken to increase cyber security, for larger and smaller organisations. Phishing and cryptoware, however, continue to pose a threat to the Netherlands as a whole.

Core findings

Cryptoware and other ransomware constitute the preferred business model for cyber criminals

Criminals use cryptoware (ransomware) increasingly often in order to achieve their goals. Unlike other common malware, such as Remote Access Tools (RATs), criminals use cryptoware to block access to data using encryption. The willingness of people and organisations to pay the criminals results in high average proceeds per target for criminals. That is why they can make relatively large investments per infection. More advanced forms, for example aimed at web applications, have also been identified. The popularity of the use of ransomware and, in particular, cryptoware will further increase in the next few years.

Geopolitical tensions manifest themselves increasingly often in (impending) digital security breaches

States and other actors that seem to act in line with the interests of these states increasingly use digital attacks and cyber operations. The aim is to represent their interests and to influence geopolitical relations or developments. Digital attacks are an attractive alternative and addition to conventional military and espionage means. Their scope and impact are large and the costs and risks are low. In the past year, conflicts, attacks or political issues were often the reason for digital attacks. It is often difficult to trace back the actor who carried out the actual attack, and to determine the extent to which a state actor played a leading role in the attack.

Phishing is often used in targeted attacks and can barely be recognised by users

Phishing ('fishing' for login and other user data) plays a key role in carrying out targeted digital attacks. Users are hardly able to recognise phishing e-mails in targeted attacks. A successful phishing campaign gives attackers access to internal networks of organisations and the information stored on these networks. Means to make authentic e-mail recognisable as such (e.g. digital signatures, Sender Policy Framework (SPF), DomainKeys Identified Mail (DKIM) and Domain-based Message Authentication, Reporting and Conformance (DMARC)) are only used in practice to a limited extent. This ensures that phishing continues to be a low-threshold and effective method of attack for attackers.

Availability becomes more important as alternatives to IT systems are disappearing

Important social processes come to a standstill if the corresponding IT systems and analogue alternatives are unavailable. The phasing out of analogue alternatives to IT systems therefore makes the availability of these systems even more important. This is especially true if these IT systems support important social processes such as transport, financial transactions or energy supply. The measures that banks have taken against DDoS attacks show that it is possible to take effective measures in order to increase availability of digital facilities. However, organisations often wait to take such measures until IT systems have already experienced availability problems.

Vulnerabilities in software are still the Achilles heel of digital security

Software is a crucial part of our digital infrastructure, because software opens up the possibilities of hardware and the ever growing amount of data. Software suppliers in 2014 again released thousands of updates in order to repair vulnerabilities in their software. Organisations sometimes do not install updates due to the obstacles they encounter when installing them. As long as the updates have not been installed, parts of their network will continue to be vulnerable. Such vulnerabilities allow actors penetrating networks via phishing or zero-day

Key questions

The key questions of this CSAN 2015 are:

- What events or what activities by which actors could affect IT interests, what tools do they use and what are the developments in this respect? (threats)
- To what extent is the Netherlands resilient to vulnerabilities in IT, could these lead to an impact on IT interests and what are the developments in this respect? (resilience)
- Which Dutch interests are being adversely affected and to what degree, by restrictions of the availability and reliability of IT, breach of the confidentiality of information stored in IT or damage to the integrity of that information, and what are the developments in this respect? (interests)

Insight into threats and actors

Table 1 provides insight into the threats that the various actors have posed over the period between April 2014 and April 2015 to the targeted 'governments', 'private organisations' and 'citizens'. Criminal organisations and state actors continue to pose a threat to these three target categories. This threat has become more specific. For most organisations, the manifestations of less advanced actors form a smaller part of the total than before. In some cases, the red colour conceals that a high threat level can increase as well. The paragraphs on criminals and state actors in Chapter 2 discuss this in more detail.

Manifestations

Growth in number of incidents with ransomware and cryptoware continues

The rise of ransomware and cryptoware in 2013 continued in 2014 and 2015, also in the Netherlands. Ransomware and cryptoware is malware that holds IT systems 'hostage' by making them unavailable and demands a ransom. Cryptoware also encrypts the data that is stored. Various cryptoware variants caused many incidents over the past period. Infections were caused by, for example, Cryptolocker, CryptoFortress, Cryptowall and CTB locker. In the Netherlands, organisations are often affected by such infections.

DDoS attacks continue to take place, but measures prevent disruptions more often

DDoS attacks remain a concern in the Netherlands. After the wave of DDoS attacks in early 2013, service providers have invested in measures to prevent these attacks. Frequent and serious DDoS attacks on websites of governments and private organisations are still being detected. The origin of the problems is therefore still in place. As a result of the increased attention to anti-DDoS measures, however, services are often not disrupted.

Espionage attacks, which become more and more frequent, start with spearphishing

In the past year, the Netherlands was dealing much more often with digital espionage attacks that posed a threat to national security and economic interests. Research conducted by the AIVD and MIVD showed that, in 2014, Dutch government institutions were often the target of advanced digital espionage attacks. Most of these attacks were carried out using spearphishing e-mails containing attachments infected with malware or links to malware websites.

Table 1 Threat matrix

Source of the threat	Targets		
	Governments	Private organisations	Citizens
Professional criminals	Theft and publication or selling of information ↘	Theft and publication or selling of information	Theft and publication or selling of information
	Manipulation of information	Manipulation of information	Manipulation of information
	Disruption of IT	Disruption of IT	Disruption of IT
	IT takeover	IT takeover ↘	IT takeover
State actors	Digitale spionage	Economic espionage	Digital espionage
	Offensieve cybercapaciteiten	Offensive cyber capabilities ↗	
Terrorists	Disruption/takeover of IT	Disruption/takeover of IT	
Cyber vandals and script kiddies	Theft of information	Theft of information	Theft of information ↗
	Disruption of IT	Disruption of IT	
Hacktivists	Theft and publication of information obtained	Theft and publication of information obtained	↘
	Defacement	Defacement	
	Disruption of IT	Disruption of IT	
	IT takeover	IT takeover ↘	
Internal actors	Theft and publication or selling of information	Theft and publication or selling of information	
	Disruption of IT	Disruption of IT	
Cyber researchers	Receiving and publishing information	Receiving and publishing information	
Private organisations		Information theft (industrial espionage)	Commercial use, abuse or 'resale' of information
No actor	IT failure	IT failure	IT failure



Change compared to
CSAN-4

Low	Medium	High
<p>No new trends or phenomena of threats have been observed.</p> <p>OR</p> <p>(Sufficient) measures are available to remove the threat.</p> <p>OR</p> <p>No incidents worth mentioning have occurred during the reporting period.</p>	<p>New trends or phenomena of threats have been observed.</p> <p>OR</p> <p>(Limited) measures are available to remove the threat.</p> <p>OR</p> <p>Incidents have occurred outside of the Netherlands, a few small ones in the Netherlands.</p>	<p>There are clear developments which make the threat expedient.</p> <p>OR</p> <p>Measures have a limited effect, so the threat remains substantial.</p> <p>OR</p> <p>Incidents have occurred in the Netherlands.</p>

Threats: actors

The biggest threat continues to be posed by professional criminals and state actors

The digital skills of criminals continue to develop. Last year saw, for example, several digital attacks by criminals which were notable for their good organisation, accurate implementation and technical sophistication. Moreover, more countries carry out digital attacks on or via the infrastructure of Dutch organisations. The biggest digital espionage threat is posed by foreign intelligence services.

Terrorists do not yet pose a serious threat, but their capabilities are, however, growing

Although the potential of terrorist actors in the digital field is growing, they do not yet pose a serious threat due to their limited technical capabilities. There are no indications of a specific threat against the Netherlands. In the context of digital attacks carried out by terrorists, the biggest threat is currently posed by jihadism. So far, digital attacks with jihadist motives in the Netherlands were limited to small-scale attacks that required little knowledge and manpower.

Conflicts, attacks and incidents provide a context for digital attacks

Various actors use national and international conflicts, attacks and incidents as a reason to carry out digital attacks. In the past year, for example, many digital attacks and cyber operations were observed which can be placed in a geopolitical context, such as the malware attacks related to the conflict in the Ukraine. It is often very difficult to link these attacks to parties. Both state actors and activist hackers with patriotic motives have the intentions and tools to carry out these attacks.

Threats: Tools

Dissemination of cryptoware is a lucrative criminal activity

The proceeds generated by criminals using cryptoware are high. Approximately 10 percent of Dutch reporting parties say they have paid criminals in order to regain access to files. The proceeds probably amount to several hundreds of euros per person per payment. The relevant criminals do their best to expand their market by looking for other means to infect (such as SD cards, USB sticks and network sources) and by using other encryption methods (for example by corrupting systems over a long period).

Phishing, or spearphishing in particular, is the most frequently used tool for targeted attacks

The parties who carried out various targeted attacks that were discovered in the past period often succeeded in their efforts by making use of spearphishing, with a phishing e-mail being sent to one person or a limited group of persons. Apart from spearphishing, actors also still use classic phishing as a tool. The Netherlands is a particularly popular target for phishers. This may have to do with the relatively good economic situation and the strong euro.

Malvertising continues to pose a danger to internet users

Advertisements have been incorporated in many websites, which sometimes have a high number of visitors. One malicious ad may therefore have a large impact in a short period of time. If a user opens a website that contains a malicious ad, this will often result in all kinds of vulnerabilities in the user's system being exploited fully automatically, so without any further user interaction. Nowadays, cyber criminals also abuse advertisement networks to attack specific user groups. They use on-line advertising auctions to this end.

Resilience: vulnerabilities

Publicity campaigns for vulnerabilities make prioritising more difficult

The past reporting period shows a development with much more publicity regarding technical vulnerabilities. Various sectors have reported that these publicity campaigns involve a risk: due to the great deal of attention that is paid to individual vulnerabilities, the issues of the day may divert attention from structural solutions. In that case, management will not always make decisions based on the correct information and will receive the impression that security officers are insufficiently prepared.

Raising awareness alone will not help prevent phishing

The quality of phishing texts has become even better. Individual users can hardly be blamed for falling victim to them. Technical measures to prevent phishing are, however, still used up to a limited extent. For example, less than 10 percent of government domain names are protected against phishing attacks using the open standards DKIM, SPF and DMARC.

Resilience: measures

Security of open source software comes at a price

The Heartbleed vulnerability showed that open source software is not automatically safer, even if it is used frequently. The publicity surrounding this bug resulted in large internet companies joining forces in April 2014 in the Core Infrastructure Initiative. The initiative invests in the open source basic infrastructure of the internet and improves the basic security of the internet. However, it currently only covers a small part of the open source projects responsible for the infrastructure of the internet. This kind of financing is not available for other projects.

Recruitment in cyber security: many vacancies, few people

The labour market for cyber security professionals has, for some time now, been characterised by a large difference between the supply of and demand for (technical) cyber security professionals. The number of vacancies is increasing; the government has also

actively recruited staff members in this area over the past period. Organisations often experience difficulties in filling job vacancies. This applies to technical cyber security positions in particular.

Detection capacity is essential for the discovery of advanced attacks

Advanced attacks, so-called Advanced Persistent Threats (APTs), are difficult to detect. These attacks, aimed at organisations in various sectors, often circumvent existing security measures. It often takes months or years before the attacks are discovered, which may result in a serious extent and impact of the damage for the organisations affected. Although an increasing number of organisations have special software to protect them against APTs, it appears that the prevention of such attacks is mostly unexplored territory for many organisations.

Interests

New areas of application result in vulnerabilities and debate

More IT is installed in cars, aircraft and other means of conveyance. This requires attention for the security of this IT. For a security problem in an entertainment system should not affect the operation of the vehicle. A lack of security may, in such a case, even have fatal consequences. Such risks may also arise if the software used contains bugs, a licence expires or a network service is no longer available. Security often has no priority in the development of such new applications.

Interests of critical infrastructure are large but stable

The interests protected by the critical infrastructure remain large but show little change. Consultations with representatives of organisations in those sectors have made this evident. Although the security of information and systems each time creates new challenges, the underlying motivations for security have hardly changed.

Alternatives to IT systems are disappearing

If IT systems that support social processes are not available, it is, in a growing number of cases, no longer possible to rely on analogue alternatives. The availability of these IT systems thus becomes more important: failure is not an option. At the same time, the underlying technology is more complex than with analogue systems. Moreover, these systems can be attacked more easily if they can be accessed via the internet.

Introduction

The topic of cyber security is given an ever more prominent position in the Netherlands. This year, the Netherlands hosted the international Global Conference on Cyber Space. It allowed the Netherlands to present itself as a frontrunner in the field of cyber security. At the same time, incidents with hacked databases and vulnerabilities in the infrastructure of governments and companies underlined the everyday importance of cyber security. Worldwide prominent incidents, such as the Sony hack and the hack of American bank JPMorgan Chase, resulted in increased media attention. In public opinion, there seems to be a growing perception of cyber crime and hacking as threats. It is still by no means certain whether the actual problems are growing.

In the year 2015, the increasing dependence on internet applications translates into access to internet-related services being evident, and thus being indispensable. It is now unthinkable that IT has no role to play in all kinds of everyday activities, such as financial transactions, travel and communication.

The central role of the internet and IT now also extends to the geopolitical level. The increased dependence on IT translates into an increased pressure to get a grip on the same internet in terms of politics.

The Cyber Security Assessment Netherlands (CSAN) is published annually by the National Cyber Security Centre and is drawn up in close collaboration with a large number of parties, both public parties (e.g. the police, intelligence and security services and the Public Prosecution Service), academic institutions and private parties (critical infrastructure).

The CSAN offers insight into the developments, interests, threats and resilience in the field of cyber security over the past year. It is aimed at policymakers in government and the critical infrastructure sectors to help enhance the digital resilience of the Netherlands or to help improve current cyber security programmes.

The key questions of the CSAN 2015 are:

- What events or what activities by which actors could affect IT interests, what tools do they use and what are the developments in this respect? (**threats**)
- To what extent is the Netherlands resilient to vulnerabilities in IT, could these lead to an impact on IT interests and what are the developments in this respect? (**resilience**)
- Which Dutch interests are being adversely affected and to what degree, by restrictions of the availability and reliability of IT, breach of the confidentiality of information stored in IT or damage to the integrity of that information, and what are the developments in this respect? (**interests**)

The first chapter, Manifestations, provides an overview of cyber security breaches over the past year. The following chapters analyse these developments and answer the key questions.

This CSAN builds on previous assessments and also refers to them. However, this report is an independent document. The reporting period of CSAN 2015 runs from April 2014 through April 2015. The focus lies on developments in the Netherlands, but important developments abroad have also been included.

The CSAN is a factual description, with guidance based on insights and expertise from government services and the critical infrastructure sectors themselves. It describes developments in a qualitative form and, where available in a reliable form, it provides a quantitative foundation and/or reference to sources. Monitoring developments is a continuous process with the CSAN being one of the annual results. Matters which have not or have hardly changed in respect of the previous editions have been described in brief or not at all.



1 Manifestations

The image of 2014 was largely defined by a number of major incidents resulting in large amounts of data becoming public knowledge. Examples are the hacks at Sony in November 2014 and TV5MONDE in March 2015. Moreover, geopolitical developments (such as the conflict in the Ukraine or the rise of ISIS) were the cause of many manifestations. There were also frequent reports of extortion by criminal organisations. This was clearly shown by the growing number of infections with different forms of cryptoware.

This chapter provides an overview of the most important manifestations in the area of cyber security over the past reporting period. A manifestation occurs when interests are harmed as a threat manifests itself and resilience is inadequate in order to remove the threat. This allows a malicious actor to actively use a vulnerability in a system, but manifestations may also occur due to errors made by users and administrators or due to technical disruptions.

Disruption of IT

Companies and public organisations have become increasingly dependent on IT systems for their primary processes. The same applies to citizens and their daily lives. As a result, the adverse effects of a failure of these systems increase every year. For attackers, the deliberate disruption of IT is therefore an important tool to inflict harm on opponents or competitors or to extort companies and individual citizens.

Ransomware and cryptoware

The rise of ransomware and cryptoware in 2013 continued in 2014 and 2015, also in the Netherlands. Ransomware and cryptoware is malware that holds IT systems ‘hostage’ by making them unavailable and demands a ransom. Cryptoware also encrypts the data that is stored. Various cryptoware variants caused many incidents over the past period. Infections were caused by, for example, Cryptolocker, CryptoFortress, Cryptowall and CTB locker. In the Netherlands, office IT environments are often hit by such infections. This is shown by, for example, meetings with representatives of the critical infrastructure sectors. Infections at, for example, the municipalities of Dronten¹, Lochem² and The Hague³ made the news. The Directorate-General for Public Works and Water Management⁴ also became a victim of cryptoware. Most infections do not make the news, but many organisations have been hit by infections over the past period. Infections usually occur as staff members read private e-mails at work.⁵ Messages they receive there contain malware or include a link to malware. Cryptoware hits both public and private organisations, including healthcare institutions⁶ and SMEs⁷. Some companies pay the ransom demanded in order for the infected files to be restored.⁸

1 <https://www.security.nl/posting/422471/Ransomware+verstoorde+dienstverlening+Dronten>

2 <http://www.lochem.nl/bestuur-organisatie-nieuws/nieuws/nieuwsoverzicht/artikel/gemeente-lochem-getroffen-door-computervirus/>

3 <https://www.security.nl/posting/406204/Computers+gemeente+Den+Haag+besmet+via+valse+PostNL-mail>

4 <http://tweakers.net/nieuws/102028/computers-rijkswaterstaat-zijn-besmet-met-ransomware.html>

5 Information from various ISACs.

6 Information from the ISAC for the healthcare sector (20 March 2015).

7 <http://www.computable.nl/artikel/nieuws/security/5242994/1276896/cryptowarevirus-raakt-vooral-het-mkb.html>

8 <https://www.security.nl/posting/422024/Tientallen+Nederlandse+bedrijven+betalen+ransomware>

The business case for criminals therefore continues to exist.

The total number of cryptoware infections is difficult to determine. According to the American security company Dell SecureWorks, the Cryptowall variant alone infected around 625,000 computer systems worldwide in five months' time in mid-2014.⁹ It is reported that 1000 to 5000 systems were infected in the Netherlands. 'Old-fashioned' Kovter ransomware, which sends a message to users that illegal material has been downloaded and that prosecution can be bought off by paying a fine, infected more than 40,000 computers per day at its peak in mid-2014.¹⁰






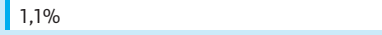
used to a limited extent and has so far not been detected in the Netherlands. Sabotage attacks on ICSs are highly exceptional in the Netherlands.¹²

The 2014 annual report of the German BSI reports sabotage at a blast furnace company in Germany. The attackers penetrated the company's office network through spearphishing. This network allowed them to gain access to the operational control network of

the blast furnace. By damaging a furnace, they managed to stop production for some time. It is unknown who is behind this attack.

Casus Coinvault

The Dutch police has investigated various cryptoware attacks.¹¹ In cooperation with Kaspersky Lab, the police discovered and further investigated a number of servers of the criminals who carried out one of these attacks, which makes use of Coinvault malware. This investigation showed that the three investigated servers were jointly responsible for 2081 infections with Coinvault (see below).

Server	Number of infections	Infections NL	Ransom payment
#1	718	 48%	 1,3%
#2	826	 45%	 2,1%
#3	537	 56%	 1,1%

A striking feature of the malware is that the victim was Dutch in almost half of the cases. This malware variant contains many Dutch links. Apart from the many Dutch victims of the ransomware, Coinvault uses Dutch plug-ins, there is a help desk page in perfect Dutch and the criminals refer to a Dutch bitcoin exchange in order to make payment.

An estimated 1.5 percent of victims actually pay in order to get files back. A side note on this is that this percentage was measured at the time when the servers were seized. The attack campaigns were probably active for one or two weeks at that time.

Sabotage

Digital sabotage attacks cause websites to be unavailable or unusable for some time. The most common forms of such sabotage are DDoS attacks and defacements. These will be discussed later in this chapter. The social unrest and costs for the parties concerned may be extensive. Such attacks, however, usually do not result in permanent damage to the information systems that are attacked, but there are also more serious forms of sabotage. Wiper malware deletes data, possibly resulting in loss of information. Malware that manipulates industrial control systems (ICSs) may cause damage to linked production or control systems. Wiper malware is

(Distributed) Denial-of-Service incidents

DDoS attacks remain a concern in the Netherlands. After the wave of DDoS attacks in early 2013, service providers have invested in measures to prevent these attacks. Frequent and serious DDoS attacks on websites of governments and private organisations are still being detected. The origin of the problems is therefore still in place. Thanks to the increased attention to anti-DDoS measures, the delivery of services is less often disrupted. In early 2015 however, the Rijksoverheid.nl website was unavailable for several hours due to a DDoS attack.

9 <http://www.secureworks.com/cyber-threat-intelligence/threats/cryptowall-ransomware/>

10 http://landing.damballa.com/rs/damballa/images/Damballa_Q2_2014_State_of_Infection.pdf

11 <https://www.politie.nl/nieuws/2015/april/13/11politie-zorgt-voor-doorbraak-in-recente-cryptoware-aanval.html>

12 Source: AIVD/MIVD

Sony Pictures Entertainment hack

In November 2014, it appeared that Sony had been a victim of an extensive digital attack. Intellectual property and confidential information were stolen on a large scale and a considerable part of its office environment was sabotaged.

The hacker group Guardians of Peace (GOP) claimed to be responsible for these attacks. This group demanded, among other things, that Sony withdraw *The Interview*, a film on a plot to kill the North Korean leader Kim Jong-un. The United States of America hold North Korea responsible for this attack.¹³ North Korea denies any involvement.

Digital attack on TV5MONDE

In early April 2015, the French international television station TV5MONDE became a victim of a digital attack that seemed to come from the hacker group called 'CyberCaliphate', which sympathises with ISIS.¹⁴ This group is also held responsible for the defacement of US CENTCOM (see paragraph 'Defacements' on page 18). Due to the attack, eleven television channels, the Facebook page and the website of the station were unavailable for several hours. The attack was seen as a retribution against France for their participation in the fight against ISIS.

Two months later, researchers of security company FireEye revealed that the attack looked like the work of a Russian hacker group known as APT28.¹⁵ According to the researchers, the hackers use the jihadist group as a cover for their work. This example shows how difficult the attribution of digital attacks is.¹⁶

The popular weblog 'geenstijl.nl', which is hosted by the same company, was hit by the same attack.¹⁷ During the reporting period, the police received 67 reports of DDoS attacks. Most of these reports were filed by organisations.

Educational institutions often fall victim to DDoS attacks. For instance, the A12 Regional Training Centre was hit by this type of attacks on several occasions.¹⁸ Schools in Almere¹⁹ and Winschoten²⁰ also became a victim. It appeared that the schools' own students were responsible for the attacks. Since at many schools the role of IT in the teaching process is increasing, such disruptions are a growing problem for teachers and students. In the reporting period, popular Dutch websites, such as the news website nu.nl²¹ and the public transport information service 9292.nl²², were hit by DDoS attacks that reduced their availability. The perpetrators and the motive of such attacks usually remain unknown.

DDoS attacks can be used easily by actors. An effective DDoS attack can be carried out with little money or knowledge. This contrasts sharply with the distorting effect of the attacks. If a service is unavailable for hours or days, this may cause serious problems.

The threat posed by DDoS attacks differs among organisations within the government and the critical infrastructure sectors in the Netherlands. Some organisations face DDoS attacks on an almost continuous basis (several attacks per week), while other organisations face attacks only sporadically (a few times per year) or almost no attacks at all. The difference in threat per sector is also shown by Akamai's report titled 'State of the Internet Q1 2015'.²³ According to this report, most DDoS attacks (including the most serious ones) focus on companies in the gaming industry (35.3 percent of the attacks) and the software/technology industry (25.2 percent of the attacks), while, for example, government institutions are hardly hit (1.8 percent of all attacks). However, this does not make DDoS attacks a problem of the past.

The intensity of DDoS attacks shows a slight worldwide increase. In early 2015, for example, an Indian network provider was hit by a short attack with a peak of 334 Gbps.²⁴ Up to that point, this was the most intensive DDoS attack worldwide.

GitHub is a popular website on which open source software is developed and distributed collaboratively. In March 2015, the website was hit by an extensive DDoS attack from Chinese IP addresses.²⁵

¹³ Source: AIVD/MIVD.

¹⁴ <http://www.ibtimes.com/french-tv-network-tv5monde-hit-pro-isis-cybercaliphate-hackers-1875314>

¹⁵ <http://www.buzzfeed.com/sheerafrenkel/experts-say-russians-may-have-posed-as-isis-to-hack-french-t#.hkaK8DKGK>

¹⁶ See also: Chapter 2, Actors.

¹⁷ https://www.security.nl/posting/418103/Storing+Rijksoverheid_nl+veroorzaakt+door+DDoS-aanval

¹⁸ <http://www.gelderlander.nl/regio/de-vallei/ede/opnieuw-cyberaanval-op-netwerk-roc-a12-1.4791497?ls=pl>

¹⁹ <http://www.omroepflevoland.nl/nieuws/121705/almere-leerlingen-leggen-computersysteem-plat>

²⁰ <http://nis.rtvnoord.com/artikel/artikel.asp?p=141973>

²¹ <http://www.automatiseringgids.nl/nieuws/2015/08/nu.nl-plat-door-ddos-aanval>

²² <http://tweakers.net/nieuws/95475/reissite-9292-kampt-al-een-dag-met-ddos-aanval.html>

²³ <http://www.stateoftheinternet.com/downloads/pdfs/2015-internet-security-report-q1.pdf>

²⁴ <http://www.arbornetworks.com/news-and-events/press-releases/recent-press-releases/5405-arbor-networks-records-largest-ever-ddos-attack-in-q1-2015-ddos-report>

²⁵ <http://www.networkworld.com/article/2903317/microsoft-subnet/largest-ddos-attack-in-githubs-history-targets-anticensorship-projects.html>

This attack was partly routed via Dutch IT infrastructure.²⁶ The attacks were aimed at two development projects of software to be used to circumvent Chinese censorship measures.

When, in early 2015, shortly after the attack on the satirical French magazine Charlie Hebdo in France, 19,000 websites went off-line, people easily concluded that this was a DDoS attack carried out by jihadists.²⁷ After a few days, however, the cause appeared to be a human error at hosting provider Oxalide.²⁸

Defacements

Every day, hundreds of websites worldwide are hit by defacements; in the Netherlands, too, dozens of websites are affected every day.²⁹ In almost all cases, this is due to so-called mass defacements, in which large numbers of web servers are scanned for vulnerabilities. If a vulnerability is discovered, the attacker will place an eye-catching message on the website, stating that it has been hacked. In many cases, this is an ideological message. Targeted defacements are carried out as well, with the relevant organisation being of ideological or political significance to an attacker. As far as we know, such targeted attacks were not carried out on Dutch websites during the past year.

The attack on Charlie Hebdo was followed by defacements of French websites in particular. The Anonymous action #OpCharlieHebdo led to a counteraction #OpFrance.³⁰ Front pages of dozens of French websites displayed Islamic texts.

The pro-Palestinian hackers of AnonGhost have been extremely active in defacements over the past period. Ideological messages were shown on websites of the United Nations³¹ and various Israeli organisations,³² but, for example, also the websites of Air France³³ and American Express.³⁴

Another popular type of defacement is the hacking of social media accounts. Attackers retrieve log-in data, for example through phishing. The consequences for the information security of

organisations are limited, because the attackers do not attack the organisations' network. However, reputational damage may be considerable. This type of attack is especially popular among ideologically motivated attackers.

The Syrian civil war and the rise of ISIS were the reason for various defacement campaigns against western websites and social media. Hacks of Twitter and YouTube accounts of US Central Command, the American army for the Middle East and South Asia, were the most striking. The profile showed a picture of a masked militant and texts such as 'Cybercaliphate' and 'I love you ISIS'.³⁵

Jihadist social media were also hit. In mid-2014, Anonymous launched the operation #OpIcElISIS with the aim of countering the ideological statements made by ISIS, for example via attacking Twitter accounts of ISIS sympathisers.³⁶

Malware infections

Hacked websites may cause the spread of large quantities of malware. The results of an investigation³⁷ into the vulnerability of the most visited websites in the world showed that 6 percent of these websites spread malware or spam or were part of a botnet. 21 percent of the websites used software with known vulnerabilities. These were mainly vulnerabilities in widely used components such as PHP, IIS and Apache, but also in CMS software such as Drupal or WordPress. The same investigation showed 99 percent of all malware infections to be caused by website visits.

The extent to which Dutch computers are confronted with malware has remained stable for several years.³⁸ In the third and fourth quarter of 2014, 13.8 percent and 10.1 percent respectively of Dutch Windows computers encountered malware, for example by visiting a website attempting to install malware (worldwide: 20.1 percent and 15.9 percent).³⁹ Most confrontations, however, do not result in infections. For example, if Dutch computer users installed Microsoft's Malicious Software Removal Tool, the malware was discovered and removed in only 3.4% and 1.9% of cases during these periods.

²⁶ https://drive.google.com/file/d/0ByrxbIDXR_yqeUNZYU5WcjFCbXM/view?pli=1

²⁷ <http://www.volkskrant.nl/aanslag-op-charlie-hebdo/franse-sites-gehackt-in-digitale-jihad-oorlog-a3830794/>

²⁸ <http://www.silicon.fr/indisponibilite-oxalide-erreur-humaine-non-attaque-106435.html>

²⁹ Source: own count on the basis of reports at zone-h.org.

³⁰ <https://www.mashable.com/2015/01/13/islamist-hackers-french-sites-anonymous/>

³¹ <http://www.ibtimes.co.uk/anonghost-hackers-deface-un-website-following-al-asqa-mosque-tensions-1474258>

³² <http://www.theprohackers.com/2014/04/opisrael-anonghost-hacked-2000-websites.html>

³³ <http://www.batblue.com/anonghost-hacks-air-france-website/>

³⁴ <http://cyberwarzone.com/breaking-news-subdomain-american-express-website-hacked-anonghost/>

³⁵ <http://techcrunch.com/2015/01/12/cyber-caliphate/>

³⁶ <http://www.hackersnewsbulletin.com/2014/09/anonymous-hackers-launch-cyber-war-isis.html>

³⁷ https://www.menlosecurity.com/resources/Menlo_Security_Vulnerability_Report_Mar_2015.pdf

³⁸ Source: comparison of the most recent Microsoft Security Intelligence Reports (<https://microsoft.com/sir>).

³⁹ Source: <https://microsoft.com/sir>.

Infection by advertisement websites

In the previous reporting period, advertisement servers were abused in the Netherlands and abroad for the spreading of malware. In the Netherlands, popular websites such as nu.nl,⁴⁰ telegraaf.nl, prive.nl⁴¹ and weer.nl fell victim to malvertising.

Advertisement suppliers of Google were hit by several of these attacks. In 2014, Google's advertising service DoubleClick spread malware infections on several occasions. In April 2015, visitors were, for a few hours and without noticing, sent to a website via Engage Lab, a Bulgarian partner, where the Nuclear Exploit Kit sought out vulnerabilities in their system and installed malware.⁴²

In 2014, an attacker placed infected advertisements on websites that were of interest to his target group. He did so using online advertising auctions. It allowed them to penetrate systems in a targeted manner. The campaign seemed to focus on the American defence industry in particular. This attack was called Operation Deathclick⁴³ by the company that discovered the campaign.

IT failure

Accidental failures may cause a reduction in the availability of services. The consequences of any disruptions of this type may be just as large as those of deliberate disruptions.

At the end of March 2015, the North Holland and Flevoland provinces were hit by a massive power failure.⁴⁴ Despite nuisance caused by people being trapped in metros and lifts and cancellations of trains, the number of major IT failures caused by the power failure remained limited. Important computer centres in the affected area used their emergency power systems to make it through the breakdown period.

Digital espionage

Where previous manifestations mainly focused on IT, the goal of espionage is to obtain information.

The number of digital espionage attacks against the Netherlands posing a threat to national security and economic interests has increased significantly over the past year. Research conducted by the AIVD and MIVD showed that, in 2014, Dutch government institutions were often the target of advanced digital espionage attacks. Most of these attacks were carried out using spearphishing e-mails containing attachments infected with malware or links to malware websites.

Moreover, Dutch government agencies and companies, including defence-related companies, have been a victim of so-called watering hole attacks in which malware is installed on targeted websites in order to infect visitors. These attacks show that Dutch government institutions and companies are often the target of digital espionage. Given the global scope and increase of digital espionage, the number of incidents detected is probably only a fraction of the actual number. This makes it likely that the scope of digital espionage in the Netherlands is greater than observed at present.⁴⁵ It is unlikely that a clearer and earlier picture will be obtained in respect of such activities without a broader use of host-based defence, anomaly detection and pattern recognition.

In early 2015, Gemalto, a French company based in the Netherlands, confirmed that it became a victim of digital espionage attacks during the period between 2010 and 2011.⁴⁶ The attackers tried to intercept key data of SIM cards. The attack, which, according to Gemalto, was probably carried out by the British GCHQ and the American NSA, only affected office networks and, according to the company, could not have resulted in a large-scale theft of encryption keys of SIM cards.⁴⁶ Following reports in the media, the AIVD conducted a factual investigation into the alleged Gemalto hack. The national security bodies were informed of the results of this investigation via the appropriate channels.

A number of digital espionage attacks were also detected abroad. In May 2014, a hack on the Belgian Federal Public Service for Foreign Affairs was reported in the media.⁴⁷ According to these reports, Russian hackers tried to obtain secret NATO documents on the crisis in the Ukraine using the Snake virus.

⁴⁰ <http://tweakers.net/nieuws/97041/nu-punt-nl-verspreide-malware-via-geinfecteerd-advertentienetwerk-update-2.html>

⁴¹ <https://www.security.nl/posting/389362/Advertenties+op+Telegraaf,+Priv%C3%A9+en+VI+verspreiden+malware>

⁴² <http://blog.fox-it.com/2015/04/07/liveblog-malvertising-from-google-advertisements-via-possibly-compromised-reseller/>

⁴³ <http://www.invincea.com/2014/10/webinar-targeted-malvertising/>

⁴⁴ <http://www.nrc.nl/nieuws/2015/03/27/dit-zijn-de-gevolgen-van-de-grote-stroomstoring-in-noord-holland/>

⁴⁵ Source: AIVD/MIVD.

⁴⁶ <http://www.gemalto.com/press/Pages/Gemalto-presents-the-findings-of-its-investigations-into-the-alleged-hacking-of-SIM-card-encryption-keys.aspx>

⁴⁷ http://www.tijd.be/nieuws/politiek_economie_belgie/Moskou_hackt_Belgische_staat.9499843-3136.art

Digital warfare⁴⁸

Over the past period, just as in previous years, large investments have been made worldwide in (offensive) digital capabilities and the related equipment for deployment. Nevertheless, there are no examples of this in a standard military sense, with, on the one hand, fatalities, injuries or destruction being attributed to the equipment for deployment and, on the other hand, activities being performed which were aimed at – in the broadest sense – disrupting, changing, misleading or destroying an opponent's equipment in an armed conflict. In this sense, purely digital warfare has not been seen yet. Possible causes for this are unforeseen side effects that may occur during the use of this type of digital equipment and the fact that such technically complex attacks require specialist knowledge and a high-quality technical infrastructure. Building such knowledge and infrastructure takes a lot of time. Moreover, despite the increase in offensive cyber capabilities, actual deployment involves significant legal, political and moral implications.

Nevertheless, a growing number of cyber operations and digital attacks with a political and military purpose have been detected. However, they were part of so-called hybrid warfare. In hybrid warfare, combinations of all possible means (e.g. political, economic and/or military means including cyber capabilities) are used which are tailored to the situation in order to achieve maximum results at minimum cost. These results generally are a purpose set by political leaders. By secretly deploying all or part of the means, it will be possible to deny responsibility for the activities or to place (apparent) responsibility with a third party. This concept is not a new

development, but the addition of cyber operations makes the subject relevant.

Examples of cyber operations (whether or not secret or undercover) which are consistent with hybrid warfare are the more than one hundred DDoS attacks carried out by pro-Russian hackers on Ukrainian pro-European websites. Moreover, NATO became a victim of this type of attacks on several occasions before or during meetings on the crisis in the Ukraine. A day before a meeting between the Ukrainian prime minister and the German federal chancellor, pro-Russian hackers also carried out DDoS attacks on the websites of the federal chancellor and the Bundestag.

Activities related to hybrid warfare are not limited to crisis areas. For instance, several coherent attempts, probably made or sponsored by states, to gather information about industrial control systems (espionage) and to prepare them for sabotage were detected in the western digital domain. In that case, the step from digital espionage to digital or hybrid warfare is a small one. Once access has been gained to such systems and information can be extracted, it is easy to cause physical damage to or with the systems. In case of military conflicts or tensions on representation of interests between states, this knowledge or access may, in due course, be used for military purposes or sabotage. Especially because of attribution problems and the potential impact of cyber operations on society, this is a worrisome (political and military) development.

Belgian media reported that the American CIA pointed out the hack to the Belgian intelligence service.⁴⁹ In October 2014, it was discovered that the White House network had been hacked. Reportedly, this was the non-classified network of the Executive Office of the President.⁵⁰

Economic espionage

Over the past year, the AIVD and MIVD have identified several digital espionage attacks on twenty Dutch companies. These attacks were most likely carried out by foreign intelligence services.⁵¹ These companies are mainly active in the defence, high-tech, horticulture, chemical, energy and space and aviation sectors. As companies are not obliged to report such attacks, the total scope of these digital espionage attacks on Dutch companies

and the resulting economic damage are difficult to determine. There are also known examples of espionage attacks on ICS and of malware that specifically focuses on exploring ICS.⁵² Such malware is also found in Dutch companies.⁵³

ASML, a Dutch manufacturer of microchip machines, stated in a press report⁵⁴ that the company's IT systems had been hacked. For a short period, third parties were able to gain access to a limited part of the IT systems. According to ASML, no unauthorised access to valuable information of the company, its clients or suppliers has been detected. It is unknown who was responsible for the digital attack.

⁴⁸ Source: MIVD.

⁴⁹ http://www.standaard.be/cnt/dmf20140514_01105038

⁵⁰ http://www.washingtonpost.com/world/national-security/hackers-breach-some-white-house-computers/2014/10/28/2ddf2fao-5ef7-11e4-91f7-5d89b5e8c251_story.html

⁵¹ Source: AIVD/MIVD.

⁵² Examples include Black Energy and HAVEX.

⁵³ Source: AIVD/MIVD.

⁵⁴ <http://www.asml.com/asml/show.do?lang=EN&ctx=5869&rid=51584>

Theft of information

Although espionage also includes stealing confidential information, theft of information occurs when attackers steal data with the aim of selling these data for commercial gain, to publish them or to abuse them for activist purposes.

Incidents in the healthcare sector

A new development over the past period was the strong increase in the number of data thefts aimed at patient information. Healthcare insurers and medical institutions in the United States in particular were a popular target. According to Dell SecureWorks, in 2013 patient data sets were sold for 20 dollars per person in underground marketplaces.⁵⁵ At the time, this price was already 10 to 20 times higher than a credit card number with security code.

The thefts of personal data at Community Health Systems⁵⁶ (4.5 million patients), Anthem⁵⁷ (80 million insured persons) and Premera⁵⁸ (11 million insured persons) were, in all cases, linked to Chinese offenders. However, no hard evidence for this has been published. As a result, the intention of the offenders (espionage or theft) was unclear.

Given the sales generated in this sector, also in the Netherlands, such data may become an attractive target. Nevertheless, no large medical data theft has been discovered in the Netherlands.

In 2014, Hold Security, an American security company, got its hands on a dataset containing 4.5 billion stolen user names and passwords. They came from around 400,000 vulnerable websites. After the NCSC had been provided with the set of vulnerable websites and stolen e-mail addresses from the .nl domain, the parties that had been affected were notified.⁵⁹ In April 2014, the German government also received a data set containing 18 million log-in data obtained by cyber criminals. In cooperation with the NCSC, the German BSI built

a website⁶⁰ where users could check if their e-mail address was included in the dataset.

In April 2015, webshop mapp.nl reported that an SQL injection had resulted in the theft of 157,000 e-mail addresses and hashed passwords.⁶¹ The webshop reset all passwords and informed customers of the data theft.

Ponemon Institute, a research centre, described 2014 as the Year of the Mega Breaches⁶² due to the number of data breaches involving large numbers of victims. In the United States in particular, point-of-sale (PoS) systems of large retail chains were hit by data thefts.

At Home Depot, data on 56 million debit cards and credit cards plus 53 million e-mail addresses of customers were stolen. Other large thefts of information on debit cards were committed at Staples⁶³ (1.1 million debit cards) and Michaels Arts & Crafts⁶⁴ (3 million debit cards). In the Netherlands, the collection of data on debit cards is of little use to criminals as Dutch debit cards are equipped with a chip.

In July 2014, the American bank JPMorgan Chase discovered a serious data theft. The theft concerned data on names and home and e-mail addresses of a total of 76 million households and 6 million small businesses.⁶⁵ Account numbers and passwords were not stolen. The hack appeared to have been made possible because the bank forgot to activate two-factor authentication in one test system.⁶⁶ A hack of the online auction site eBay in May 2014 resulted in the theft of data of an unknown number of users.⁶⁷ As a precaution, eBay asked all 145 million users to change their password.

The theft and publication of nude pictures of various celebrities that were stored on iCloud,⁶⁸ also referred to as the *Fappening*, caused a lot of commotion last year. When, moreover, almost 100,000 Snapchat images were leaked from the third-party app SnapSaved, this immediately became known as the *Snappening*.⁶⁹ These incidents attracted worldwide attention to the danger of saving pictures or sharing them via the cloud without paying explicit attention to security.

55 <http://www.secureworks.com/resources/blog/general-hackers-sell-health-insurance-credentials-bank-accounts-sns-and-counterfeit-documents/>

56 <http://www.informationweek.com/attacks-breaches/chinese-hackers-hit-community-health-system/d/d-id/1298099>

57 <http://www.bloomberg.com/news/articles/2015-02-05/signs-of-china-sponsored-hackers-seen-in-anthem-attack>

58 <http://krebsonsecurity.com/2015/03/premera-blue-cross-breach-exposes-financial-medical-records/>

59 <https://www.ncsc.nl/actueel/nieuwsberichten/ncsc-verkrijgt-nederlandse-gegevens-van-hold-security.html>

60 <https://www.ncsc.nl/actueel/nieuwsberichten/nederlandse-accountgegevens-buitgemaakt-in-duitsland.html>

61 https://www.security.nl/posting/425241/Gegevens+157_000+klanten+Mapp_nl+gestolen

62 <http://www.ponemon.org/library/2014-a-year-of-mega-breaches>

63 <https://threatpost.com/staples-confirms-1-2-million-cards-lost-in-breach/110030>

64 <http://krebsonsecurity.com/2014/04/3-million-customer-credit-debit-cards-stolen-in-michaels-aaron-brothers-breaches/>

65 <http://www.theguardian.com/business/2014/oct/02/jp-morgan-76m-households-affected-data-breach>

66 <http://www.esecurityplanet.com/network-security/entry-point-identified-for-jpmorgan-chase-breach.html>

67 <http://www.cnet.com/news/ebay-hacked-requests-all-users-change-passwords/>

68 <http://www.ibtimes.com/jennifer-lawrence-victoria-justice-apparent-nude-photos-leaked-twitter-1674758>

69 <http://www.ibtimes.com/snappening-how-much-trouble-leaked-snapchat-photos-can-get-you-1704287>

Theft of financial means

Information is worth money. That is why criminals try to obtain data sets and sell them for a lot of money. There is a method that works even faster: stealing money by using malware.

Thefts by malware on ATMs were also committed in Western Europe over the past period.⁷⁰ This type of theft had not been detected here before. Criminals first install malware on an ATM; this requires physical access to the machine. After that, they can deplete the machines by entering a certain code.

The criminals who were behind the Carbanak or Anunak campaign managed to deal a bigger blow. Security companies Fox-IT⁷¹ and Kaspersky⁷² reported on this case. The Carbanak gang managed to infect several banks through spearphishing e-mails, after which they conducted a long-term investigation into the working methods of the various banks. Money was then stolen in various ways, for example by transferring money to own accounts and by

manipulating ATMs. It is estimated that the gang stole between 250 million and 1 billion dollars. Dutch banks have indicated that they have not become a victim of Carbanak.

Attacks on clients of Dutch banks have recently been less successful than in previous years. The damage caused by phishing attacks on clients of Dutch banks has decreased from 4.7 million euros in 2013 to 3.9 million euros in 2014.⁷³ This decreasing trend has been seen for several years. The banks also state that the damage caused by malware decreased by 90% during this period.

Moreover, various bitcoin thefts were carried out over the past period. In January 2015, almost 19,000 bitcoins (over 4 million euros) were stolen at Bitstamp, a European bitcoin exchange.⁷⁴ Various smaller thefts of bitcoins⁷⁵ and other crypto currencies⁷⁶ were committed as well. Since the bankruptcy of the large bitcoin exchange Mt. Gox in early 2014, when around 850,000 bitcoins went missing, the bitcoin exchange rate has seen a continuous decline.

70 <https://www.security.nl/posting/405528/Malware+op+20+geldautomaten+in+West-Europa+ontdekt>

71 <https://www.fox-it.com/en/press-releases/anunak/>

72 <https://securelist.com/blog/research/68732/the-great-bank-robbery-the-carbanak-apt/>

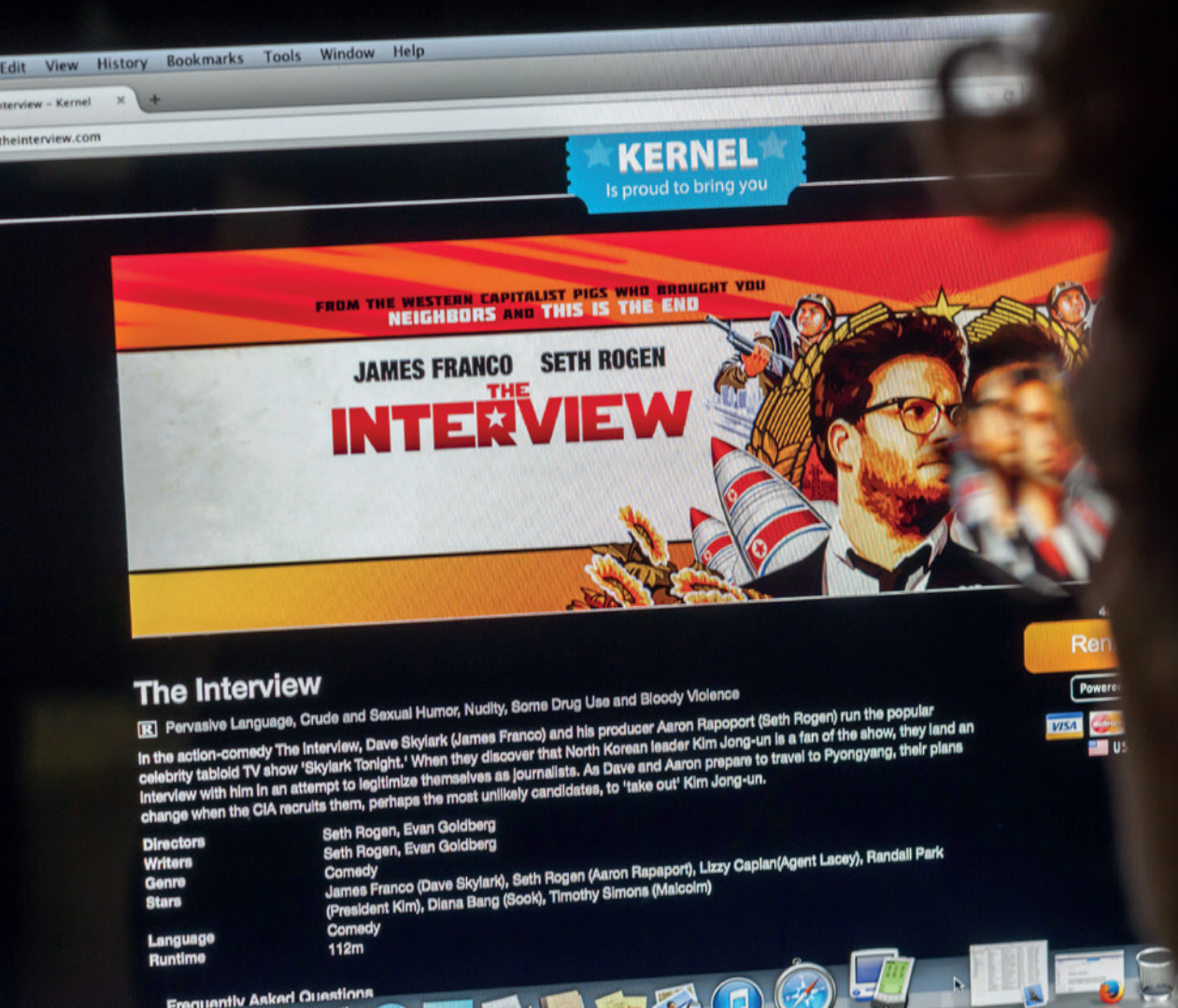
73 <http://www.betalvereniging.nl/wp-uploads/2015/03/150318-Fraude-betalingsverkeer-gehalveerd-20141.pdf>

74 <http://www.zdnet.com/article/bitstamp-bitcoin-exchange-suspended-amid-hack-concerns-heres-what-we-know/>

75 <http://www.coindesk.com/bitcoin-firm-coinapult-restores-services-following-hack/> en <https://www.cryptocoinsnews.com/allcrypt-com-bitcoin-exchange-goes/>

76 <https://www.cryptocoinsnews.com/bitcoin-altcoin-exchange-cryptoine-hacked/>

*Criminals no longer need digital skills
in order to carry out digital attacks.*



2 Threats: actors

As in previous years, the biggest threat comes from professional criminals and state actors. Their numbers are increasing, as are their capabilities. Although the potential of terrorist actors in the digital field is growing, they do not yet pose a serious threat due to their limited technical capabilities.

This chapter deals with the actors who adversely affect the reliability and security of information and information systems, their capabilities and the developments in this area.

Professional criminals

The intention of professional criminals is to earn money. The digital skills of criminals continue to develop. The working method of criminals is innovative and subject to continuous change. Last year, several digital attacks by criminals were notable for their good organisation, accurate implementation and technical sophistication.^{77 78 79} Cyber crime has a high degree of geographical distribution, both of the criminals and victims and of their infrastructure. This geographical distribution makes international cooperation necessary. The threat posed by innovative as well as traditional attacks by criminals is increasing.

This year, it was noticeable that cyber criminals are prepared to invest a lot of time in the preparation of digital attacks, for example with Carbanak, a sophisticated attack against Eastern European banks. Through malware, criminals were able to observe the activities of bank staff digitally and for a long period of time, which eventually allowed the criminals to transfer large sums of money to bank accounts and to manipulate ATMs.⁸⁰

Not only do cyber criminals show more patience in relation to the implementation of their activities and are they well-organised, they also become more creative with regard to cashing in on stolen data. In the United States, attackers used a very specific malware campaign to steal price-sensitive information from the pharmaceutical sector. This information allowed them to predict prices.⁸¹

Another type of attack by criminals that increased strongly in the past year is the use of Point-of-Sale malware.⁸² This PoS malware does not appear to pose a serious threat to the Netherlands, mostly because Dutch debit cards have EMV technology, a chip that makes it difficult to copy information stored on the chip. Moreover, ATMs have a direct protection against copying card data that have been read.

Moreover, criminals in the United States increasingly focus on data thefts in the medical sector.^{83 84 85} The data often concern patient data from healthcare insurers. Attackers probably carry out these hacks in order to obtain social security numbers, birth data and medical information. This not only allows attackers to commit financial fraud, but also insurance fraud.⁸⁶ These attacks have not yet been detected in the Netherlands.

Apart from these developments, criminals are still engaged in less customised services to other parties. This 'cybercrime-as-a-service' continues to develop and to become more professional. These

77 <https://www.fox-it.com/en/press-releases/anunak/>

78 <http://www.kaspersky.com/about/news/virus/2015/Carbanak-cybergang-steals-1-bn-USD-from-100-financial-institutions-worldwide>

79 <http://www2.fireeye.com/rs/fireeye/images/rpt-fin4.pdf>

80 https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf

81 <http://www2.fireeye.com/rs/fireeye/images/rpt-fin4.pdf>

82 Chapter 1 has already discussed this type of attack.

83 <http://abcnews.go.com/Business/fbi-investigating-cyberattack-health-insurance-company-affect-11/story?id=29705722>

84 <http://www.ehackingnews.com/2015/03/data-breach-at-sacred-heart-health.htmlv>

85 <http://www.databreaches.net/childrens-national-health-system-notified-18000-patients-after-employees-fell-for-phishing-scheme/>

86 <http://www.secureworks.com/resources/blog/general-hackers-sell-health-insurance-credentials-bank-accounts-sns-and-counterfeit-documents/>

services have become so extensive that they are even subject to competition in the underground market. This forces these services to become more and more reliable to customers.⁸⁷

Criminals no longer need digital skills in order to carry out digital attacks. It is therefore conceivable that not only the scope, but also the diversity of digital attacks by criminals will increase.⁸⁸

Interaction between actors complicates attribution

The interaction between state actors, criminals and hackers becomes increasingly intensive.⁸⁹ Tools that have so far been used mostly by state actors, are freely available in the underground market for other groups of actors, such as criminals. Moreover, state actors now use tools that were previously used only for other types of attacks. In the past year, for example, specific malware was used for espionage attacks against companies and institutions from the Ukraine, which used to be associated with attacks by criminals.^{90 91}

Hackers and ideological/patriotic hackers may perform activities which seem to be in line with the interests of a state. These activities will then make it difficult to conclude, on the basis of the motive, which type of actor carried out the attack. States may also cooperate with hackers and may hire hackers for their own purposes. It is often difficult to prove these links.

Due to various technical difficulties, attribution of digital attacks has always been difficult. The attacks on Sony Pictures Entertainment and the French television station TV5 Monde as described in Chapter 1, are good examples of this. The interaction between groups of actors, and groups of digital actors in particular, make it more difficult to analyse attacks.

scope and impact and low costs and risks. As a result, the number of actors that may constitute a potential threat to Dutch national security will increase.⁹²

The reporting period saw an increase in the number of countries carrying out digital attacks against or via the infrastructure of Dutch organisations.⁹² Most cases concern digital espionage, with an increase in economic espionage. Moreover, there have been several cases of abuse of Dutch infrastructure for digital sabotage attacks against organisations outside the Netherlands.

The biggest digital espionage threat is posed by foreign intelligence services. Moreover, the scope and diversity of actors involved have increased. For digital attacks, foreign intelligence services often make use of the knowledge, capabilities and resources available to hackers and private organisations, such as IT companies and universities. The software or infrastructure of these organisations is often used for espionage.⁹²

Furthermore, actors with a non-democratic or authoritarian background in the digital domain have a major advantage. Despite international consensus that the international rule of law also applies in cyber space, these actors pay little attention to complying with this rule of law. They are able to use their capabilities – which may be technologically inferior – in a flexible and highly effective manner, as there is no independent supervision and a need for transparency. In such countries, private groups can often perform their activities without interference, as they enjoy a form of protection at various government levels and actions may even be symbiotic. This increase in the number of actors involved complicates a reliable attribution of attacks.

Terrorists

The aim of terrorists is to bring about political and ideological changes by creating fear. Although the potential of terrorist actors in the digital field is growing,⁹³ they do not yet pose a serious threat due to their limited technical capabilities. There are no indications of a specific threat against the Netherlands.⁹⁴

State actors

Dutch national security and the Dutch economy are threatened by state actors. Digital attacks are an attractive alternative to conventional military and espionage equipment due to the large

87 <https://blogs.rsa.com/cybercrime-2015-inside-look-changing-threat-landscape/>

88 <https://www.aivd.nl/@3247/jaarverslag-aivd/>

89 <https://www2.fireeye.com/WEB-2015RPTM-Trends.html>

90 https://www.f-secure.com/documents/996508/1030745/blackenergy_whitepaper.pdf

91 <https://www2.fireeye.com/WEB-2015RPTM-Trends.html>

92 Source: AIVD/MIVD.

93 <https://www.aivd.nl/@3247/jaarverslag-aivd/>

94 <https://www.aivd.nl/@3247/jaarverslag-aivd/>

In the context of digital attacks carried out by terrorists, the biggest threat is currently posed by jihadism.⁹⁵ With the rise of jihadist groups such as ISIS, the digital activities of jihadist groups or jihadist sympathisers receive extensive media attention. Moreover, jihadist groups have repeatedly called for digital warfare or a 'cyber jihad' against the West.^{96 97} Over the past few years, these developments have given rise to the question as to what extent jihadist actors have the capabilities to carry out digital attacks that disrupt society.

So far, digital attacks with jihadist motives which were carried out in the Netherlands have been limited to small-scale attacks requiring little knowledge and manpower. These attacks mainly concern defacements of websites and DDoS attacks.⁹⁸ The motive of these attacks seems to be, as yet, the spread of propaganda.

Capabilities of terrorists

In foreign countries, jihadists are beginning to use low-threshold malware. In Syria, digital attacks were detected which have presumably been carried out by ISIS in order to determine target location data at a local level.⁹⁹

Jihadist groups place information and instructional videos on the internet in order to further spread the digital capabilities of supporters.¹⁰⁰ These instructions are mostly aimed at the digital security awareness of prospective jihadists.^{101 102} Moreover, instructions were found for the use of a Remote Access Tool (RAT).¹⁰³ Although the use of RATs by jihadist groups has not yet been detected in the Netherlands and abroad, their use has been widespread among various political factions in the Middle East.¹⁰⁴ Due to these developments, it is conceivable that the digital capabilities of jihadist groups will further enhance in the future and that they may also perform these activities against Dutch interests.

Jihadist groups also use deceit during their small-scale digital attacks. Jihadists were found to have taken over social media

accounts of the American army. They claimed to have stolen sensitive data from the same server.¹⁰⁵ Personal data of American defence staff were disclosed online on several occasions.^{106 107}

In all cases, however, these 'sensitive data' appeared to be publicly available information likely acquired by jihadist groups by performing targeted searches on the internet.¹⁰⁸ So it would seem that these incidents do not concern data breaches or new digital capabilities of terrorists.

The main reason for this form of deceit is likely to spread propaganda. As it is often not immediately clear whether or not sensitive data have been disclosed, these actions may cause social unrest. However, they do not pose any immediate threat to national security.

Cyber vandals and script kiddies

Activities of cyber vandals and activists are given a lot of media attention, but only posed a limited threat to organisations during this period. The knowledge level of cyber vandals varies and they carry out hacks because it is possible or to demonstrate that they are able to do so. Script kiddies are hackers with limited knowledge who carry out attacks for fun and who are looking for a challenge.

Apart from the limited threat posed by this group, attacks and incidents may provide this group with a catalyst for simple digital activities, such as DDoS attacks and defacements. See also the box 'Digital attacks and conflicts, attacks and incidents'.

In the past year, it was often unclear if digital attacks that were carried out in the Netherlands and abroad had been carried out by jihadists or by vandals. This is often true for DDoS attacks or defacements which include a reference to ISIS. It is often unclear if there are also any jihadist motives behind them.

95 <https://www.nctv.nl/onderwerpen/tb/dtn/>

96 http://www.iss.europa.eu/uploads/media/Brief_2_cyber_jihad.pdf

97 <http://securityaffairs.co/wordpress/36883/cyber-crime/cyber-caliphate-electronic-war.html>

98 <https://www.aivd.nl/@3247/jaarverslag-aivd/en CSBN-4>

99 <https://citizenlab.org/2014/12/malware-attack-targeting-syrian-isis-critics/>

100 <https://www.youtube.com/channel/UCTDqtFlzEZG1NrkgzjZxbg>

101 <http://grugq.tumblr.com/post/109088631293/isis-compilation-of-intelligence-and-security>

102 <http://www.dailymail.co.uk/news/article-3029500/How-Snowden-helped-three-terror-groups-Al-Qaeda-linked-extremists-said-changed-way-communicate-leaks-traitor.html>

103 <http://blog.sensecy.com/2015/02/02/al-qaeda-electronic-jihad/>

104 <http://www.bbc.com/news/technology-28418951>

105 <http://www.washingtonpost.com/blogs/the-switch/wp/2015/01/12/the-centcom-hack-that-wasnt/>

106 <http://www.militarytimes.com/story/military/pentagon/2015/03/23/pentagon-notifying-troops-named-by-alleged-islamic-state-hackers/70332846/>

107 <http://www.washingtonpost.com/blogs/the-switch/wp/2015/01/12/the-centcom-hack-that-wasnt/>

108 Refer to note 110 and <http://www.militarytimes.com/story/military/pentagon/2015/03/23/pentagon-notifying-troops-named-by-alleged-islamic-state-hackers/70332846/>

Cyber vandals or script kiddies use the reference to ISIS as a deception or for the shocking effect and the media attention this reference creates.¹⁰⁹

Last year, we saw cyber vandals and script kiddies refer to ISIS in DDoS attacks on online gaming platforms¹¹⁰ and the defacement of the website of Malaysian Airlines.¹¹¹

This type of attacks may cause social unrest in the future if popular websites are attacked, widely used services become unavailable or if socially relevant web pages are attacked.

Hacktivists

Hacktivists want to achieve ideological objectives or come closer to these objectives by carrying out digital attacks. This group of actors also includes hackers with ideological motives or patriotic hackers. Attacks carried out by this group of actors can often be placed in geopolitical context. Last year, hacktivists posed a relatively minor threat to the Netherlands.

They usually perform simple digital activities, such as DDoS attacks and defacements. Sometimes, these groups claim to have stolen confidential data from opponents.¹¹²

The risk of digital attacks by hacktivists is increasing during national and international conflicts, attacks and incidents. See also the box 'Digital attacks and conflicts, attacks and incidents'. Moreover, the capabilities of this group may be increasing as tools used to carry out digital attacks become more accessible.

Internal actors

Internal actors are individuals who are or have been working within an organisation (whether temporarily or not), such as (former) employees, temporary workers and suppliers.

Last year showed that if the reliability of an information or other system is affected, this is not always caused by financial, political or personal motives. Inattention and human errors may also play a role.

In various incidents that occurred this year, staff members placed sensitive information on private servers and this information could be viewed and downloaded via the internet. For instance, a staff member of an insurance company placed claim data from 27,000 insured persons on a private server in order to test software.¹¹³ Another example is a police system administrator who placed sensitive information about investigations on a private website. This information could then be found on the internet.¹¹⁴

The availability of information or other systems may also be affected by human errors. For example, an error during maintenance work resulted in the failure of internet hub AMS-IX in May 2015.¹¹⁵

As a result, various websites and other services were temporarily unavailable or only available to a limited extent. As the AMS-IX is one of the biggest internet hubs in the world, the failure also had an impact abroad. The failure did not last long: according to AMS-IX, it lasted for no more than ten minutes.¹¹⁵

Cyber researchers

Cyber researchers look for vulnerabilities in IT environments for the purpose of exposing low levels of security. They often publish their findings and increase cyber security awareness through the media. Any publicity on these vulnerabilities may (temporarily) make institutions and companies extra vulnerable, as malicious parties may then benefit from the research findings. In some cases, cyber researchers are suspected of having committed criminal offences themselves.

It often happens that researchers or journalists who want to demonstrate vulnerabilities come into contact with the law. This happened last year, for example when members of the House of Representatives had become the target of a phishing attack by a television programme that wanted to demonstrate a security vulnerability. The phishing e-mail asked recipients to fill in all kinds of personal data on a phishing website. The attack was discovered in time and was reported to the police. The police are still investigating the case.¹¹⁶

Since the publication of the Guidelines for arriving at a practice for responsible disclosure¹¹⁷ in 2013, cyber researchers, together with

109 <http://www.theguardian.com/world/2015/jan/26/malaysia-airlines-website-hacked-by-lizard-squad>

110 <http://krebsonsecurity.com/2014/12/cowards-attack-sony-playstation-microsoft-xbox-networks/>

111 <http://www.thestar.com.my/News/Nation/2015/01/26/MAS-website-hacked-ISIS/>

112 <http://www.bbc.com/news/world-europe-30453069>

113 <http://www.cooperatievgz.nl/newsroom/verdere-aanscherping-procedures-vertrouwelijke-informatie>

114 <http://www.volkskrant.nl/binnenland/geoelinge-informatie-op-straat-door-veiligheidslek-politie-a3793726/>

115 <http://tweakers.net/nieuws/103067/internetknooppunt-ams-ix-kampt-met-uitval-update-2.html>

116 <https://www.security.nl/posting/416784/Mogelijk+boete+voor+phishingaanval+op+Kamerleden>

117 <https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsible-disclosure.html>

the IT security community, have been able to report any vulnerabilities in a confidential and responsible manner by following a procedure that provides safeguards. The purpose of the guidelines is to facilitate reporters and to quickly solve any vulnerabilities.¹¹⁸

Responsible disclosure is used more often and by an increasing number of organisations. Chapter 5 discusses the state of affairs of responsible disclosure in the Netherlands.

Private organisations

Private organisations may breach the confidentiality of information or other systems for financial gain. They may also commit corporate espionage in order to improve their competitive position. It is not expected that the threat level of digital corporate espionage will differ

much from that of physical corporate espionage. No new trends or phenomena of threats have been observed in the field of digital corporate espionage.

Conclusion and looking ahead

The largest digital threat is still posed by criminals and state actors. Criminals are well-organised and become more creative with cashing in on stolen data. They are also prepared to spend a lot of time in the preparation of attacks. The threat posed by both innovative and traditional attacks by criminals will further increase.

For state actors, digital attacks are still an attractive alternative to conventional military and espionage equipment, due to the large scope and impact and the low costs and risks. This will cause a further increase in the number of actors posing a potential threat to national security.

Digital attacks and conflicts, attacks and incidents

Various actors often use national and international conflicts, attacks and incidents as a reason to carry out digital attacks. In the past year, for example, many digital attacks were detected which can be placed in a geopolitical context, such as the malware attacks that can be linked to the conflict in the Ukraine. It is often very difficult to link the attacks to parties. Both state actors and activist hackers with patriotic motives have the intentions and tools to carry out these attacks.¹¹⁹

Attacks, disasters and incidents may also create situations in which parties want to obtain information by performing digital activities. This situation was seen last year during a targeted digital attack against Malaysian government officials and staff members of Malaysian Airlines who investigated the disappearance of flight MH370. It is suspected that the attackers were searching for documents related to the investigation into MH370 and then stole these data.¹²⁰ It is also reported that the telephone of the Australian Minister of Foreign Affairs was compromised during international contacts on flight MH17.¹²¹

Although it is always difficult to establish the origin and motives of these attacks with certainty, it is conceivable that parties may have an interest in intercepting information and positions on these events. Criminals often use attacks, disasters and incidents as a means to make money. Both the Charlie Hebdo attacks and the disaster with flight MH17 were used by criminals to generate income through click fraud and advertisements, or to spread malware.¹²² They did so by creating false profiles of victims of the disaster, for example.¹²³ Criminals also tried to compromise systems by spreading malware in photographs or video players that were used to play videos of the crash.¹²⁴

Attacks and incidents provide a catalyst for attacks with ideological motives. This usually concerns simple digital activities, such as DDoS attacks and defacements. In early 2015, the attack on the Charlie Hebdo editors in Paris marked the beginning of various digital attacks in France. Most of these attacks were carried out by pro-jihadist parties who wanted to make an ideological statement.¹²⁵ In response to these attacks, the group of hackers called 'Anonymous' focused on deactivating social media accounts and websites of pro-jihadist parties.^{126 127}

118 <http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/12/19/tk-voortgang-responsible-disclosure.html>

119 <http://www.crowdstrike.com/2014-global-threat-report/>

120 <http://www.thestar.com.my/News/Nation/2014/08/20/Hacker-targets-info-on-MH370-probe-Computers-of-officials-infected-with-malware/>

121 <http://www.heraldsun.com.au/news/foreign-minister-julie-bishops-phone-was-hacked-at-the-height-of-the-mh17-crisis/story-fniofiyv-1227026241325>

122 <https://www.bluecoat.com/security-blog/2015-01-14/miscreants-say-je-suis-charlie-too>

123 <http://nos.nl/op3/artikel/677528-grof-geld-verdienen-met-mh17kliks.html>

124 <https://www.security.nl/posting/397457/Zogenaamde+raketvideo+MH17+verspreidt+ongewenste+software>

125 <http://www.newsweek.com/19000-french-websites-and-counting-hacked-charlie-hebdo-attack-299675>

126 <http://www.nu.nl/internet/3969091/anonymous-beloofd-enorme-reactie-aanslag-in-parijs.html>

127 <http://www.independent.co.uk/life-style/gadgets-and-tech/opcharliehebdo-anonymous-take-down-french-extremist-website-after-threatening-re-tribution-for-charlie-hebdo-attacks-9972013.html>

Table 2 **Actors and their intentions**

Actor	Intentions
Professional criminals	Financial gain (directly or indirectly)
State actors	Improving geopolitical (or internal) position of power
Terrorists	Bringing about changes in society, seriously frightening the population or influencing political decision-making
Cyber vandals and script kiddies	Demonstrating vulnerabilities, hacking because it is possible, for fun, looking for a challenge
Hacktivists	Ideological motives
Internal actors	Revenge, financial gain, ideological motives (possibly 'driven')
Cyber researchers	Demonstrating weaknesses, own profiling
Private organisations	Obtaining valuable information

As a result of this increase in the number of actors (both state actors and criminals), it will also become more difficult in the future to attribute digital attacks to parties.

Jihadist groups are starting to use low-threshold malware, but most attacks are still small-scale and simple. There are no indications of a specific threat against the Netherlands. There is often a lack of clarity as to whether defacements have been carried out by jihadist actors or by vandals. However, the increasing availability of advanced malware on the internet make it conceivable that the digital capabilities of jihadist groups will further increase in the future.

Finally, conflicts, attacks and incidents give various actors a reason to carry out digital attacks. State actors, criminals and actors with ideological motives use these situations to achieve their goals.

.....

Because of the success of spearphishing, this form of social engineering is the primary attack vector for digital espionage.



3 Threats: tools

The tools available to actors have become more advanced. More ready-made tools are available for actors with limited knowledge. Ransomware continues to develop, is becoming more professional and focuses on more different systems. In other areas, too, malicious parties continue to look for innovation to ensure a continued success and effectiveness of attacks. For instance, attackers carrying out DDoS attacks continue to look for new amplification methods, malware writers try to bypass detection in various ways and recognising spearphishing attacks has become more difficult.

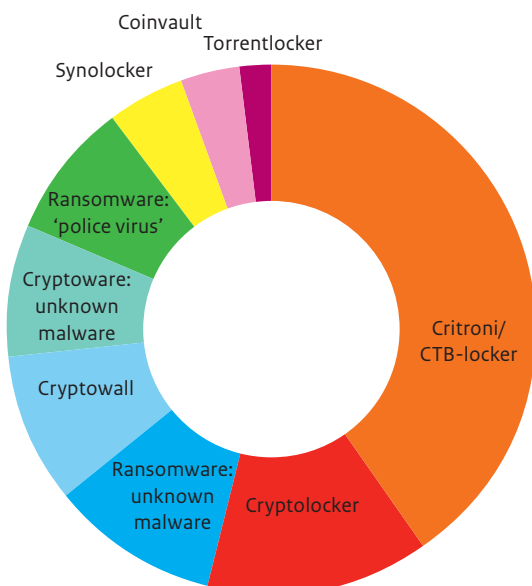
When carrying out digital attacks, actors make use of tools to abuse or enhance vulnerabilities. This could involve both technical tools as well as methods of attack. This chapter discusses these tools.

Malware

Ransomware is becoming more and more professional and is a growing problem

The amount of ransomware (and cryptoware, see the box on the following page) is growing further. The Team High Tech Crime (THTC) of the police sees that the rise of cryptoware in the Netherlands, which was already predicted in the previous CSAN, has become reality during the period covered by this CSAN. Various cryptoware campaigns, such as Critroni/CTB-Locker, Cryptolocker and Cryptowall, caused Dutch victims during this period. This is evident from reports to the Dutch police. The overview in figure 1 is based on 87 reports which the police received during the reporting period and which were found in the police systems using search terms. A ransom was paid by approximately 10 percent of the 75 reporters who are known to have paid or not paid a ransom. This percentage is relatively high compared to other countries. The fact that the number of reports is low compared to the number of infections is shown by the Coinvault case (box in Chapter 1). Approximately 1.5 percent of the victims paid a ransom. It could be that victims who paid a ransom are more motivated to file a report than victims who did not pay a ransom.

Figure 1 Reports of ransomware in the Netherlands ¹²⁸



¹²⁸ Source: police.

Ransomware versus cryptoware

Ransomware is malware that blocks access to a system. Victims have to transfer money to criminals in order to regain access to the system. An example is the 'police virus',¹²⁹ which surfaced some time ago, sending messages to users that they supposedly committed criminal offences.

Cryptoware is a form of ransomware. With cryptoware, criminals go one step further by also encrypting files in the system of a user. These files can only be decrypted using a secret key, which the criminals possess. Victims are only given this key by paying. This is, however, no guarantee for obtaining the key and the original files. The police therefore strongly advise against payment.¹³⁰

New variants of this type of malware appear frequently and the proceeds generated by criminals are high. For instance, an analysis of bitcoin payments conducted by Fox-IT showed that the makers of the TorrentLocker ransomware probably earned over 250,000 euros with their criminal activities, which money came from at least 653 victims. So the proceeds probably amount to several hundreds of euros per person per payment.¹³¹

The financial remuneration stimulates criminals to continuously improve their malware and their approach in order to increase its success and the income it generates. In the past, the developers of ransomware sometimes made technical errors. One error, for example, allowed users to regain access to encrypted files by using a key that was left in the system¹³² or via shadow copies of Windows.¹³³ This is no longer possible in newer versions of ransomware and victims have to rely on back-ups or have to pay an amount to criminals, which usually varies between 100 and 700 euros.¹³⁴

The criminals behind ransomware use various tools to try to reduce the traceability of individuals and the technical infrastructure behind this infrastructure. They increasingly rely on anonymous networks such as Tor and I2P¹³⁵ for network communications and of bitcoin or other crypto currencies in order to collect the amount requested. For instance, Critroni – ransomware which cyber criminals offer for sale online for an amount of approximately 1500 dollars – uses Tor to communicate with the criminals' servers. If a victim has not installed any Tor software on his system, the

malware automatically connects to an online Tor browser in order to make the connection. This allows the criminals to avoid detection.

Ransomware is used more broadly

Criminals want to attack new target groups with their ransomware, thereby increasing their impact. This is shown by the attacks of more operating systems (including mobile platforms) and the attacks against business users, in addition to the group of consumers that is already targeted.

In addition to the encryption of system files, attackers also lock files on, for example, SD cards, USB sticks and network sources, even if these network sources are not linked to the user's system.¹³⁶

Ransomweb, a special form of cryptoware, uses a vulnerability to install itself on web servers. After that, it secretly encrypts information in the database of this website for a longer period of time (for example six months) and decrypts it again using a secret key. Criminals store this key on an external server that is controlled by them.¹³⁷ After a certain period, attackers delete this external key and the information in the database is no longer accessible. Only then will an owner discover that parts of the database – and the back-ups of these parts – can no longer be read. Here, too, criminals of course promise the owner of the website to give the key after he has paid the amount demanded.

The way in which cyber criminals infect their victims with ransomware varies. In many cases, victims reply to e-mails sent in the name of known companies. These e-mail try to convince users to open an infected file or to visit a rogue website. Moreover, criminals are known to sometimes contact victims by telephone on behalf of Microsoft and spread ransomware via malicious files in news groups.

The problem of ransomware will probably grow in the coming period, as the locking of systems or data has been successful so far and can be used in all digital systems. The approach to cryptoware continues to be a point for attention. The secret key, which is required in order to restore files and regain access, can usually only be obtained by paying criminals. In some cases, however, private organisations retrieved keys, which allowed victims to decrypt their files without making any payment. For instance, Fox-IT and Kaspersky Lab provided victims with the secret keys. Fox-IT did so

¹²⁹ <https://www.politie.nl/themas/ransomware.html>

¹³⁰ <https://www.politie.nl/nieuws/2014/maart/10/11-politie-waarschuwt-voor-cryptolock.html>

¹³¹ <http://blog.fox-it.com/2014/10/21/update-on-the-torrentlocker-ransomware/>

¹³² <http://www.itworld.com/article/2697593/security/mistake-in-ransomware-program-leaves-decryption-key-accessible.html>

¹³³ <https://technet.microsoft.com/en-ie/magazine/2006.01.rapidrecovery%28en-us%29.aspx>

¹³⁴ Depending on the bitcoin exchange rate.

¹³⁵ <http://blog.trendmicro.com/trendlabs-security-intelligence/android-ransomware-uses-tor/>

¹³⁶ <http://www.bleepingcomputer.com/forums/t/569157/cryptofortress-a-torrentlocker-clone-that-also-encrypts-unmapped-network-shares/>

¹³⁷ https://www.htbridge.com/blog/ransomweb_emerging_website_threat.html

by cracking the algorithm of the Cryptolocker¹³⁸ keys and Kaspersky Lab by providing access to keys that were found on the server of a criminal.¹³⁹ Prevention by means of back-ups nevertheless continues to be the main measure to limit potential damage caused by ransomware.

The risk of malware on mobile platforms is still limited

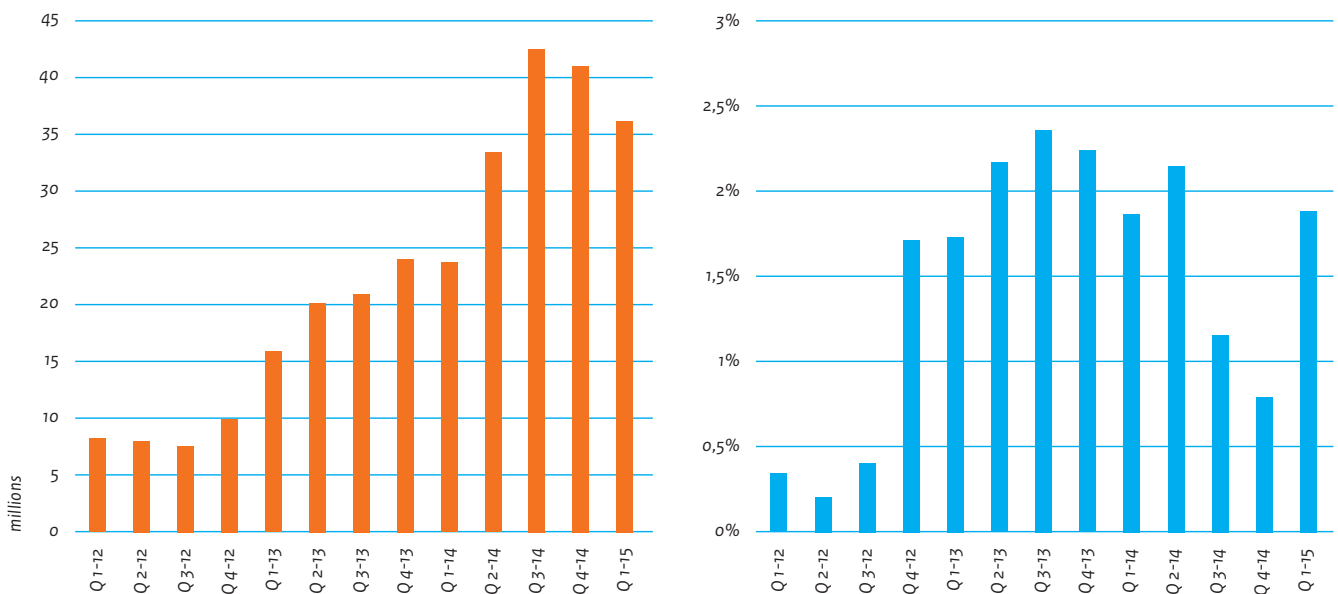
Although malware for mobile platforms exists, the threat posed by this malware is still limited. Any abuse usually focuses on Android (94 to 98 percent)^{140 141} and less on iOS (no more than 6 percent).¹⁴² The following comments are important here:

- 81.5 percent of all new smartphones sold in 2014 were Android phones.¹⁴⁴ It is therefore logical that the main focus of mobile malware writers is on this mobile platform.
- Most malware is installed on user devices via rogue apps. Android users who are only connected to the official Google Play Store run a very small risk of downloading an infected app. Only

1 in 1,000 apps are reported to have malicious intentions.¹⁴⁵ This percentage is often considerably higher for the app stores of other providers. Google figures show that less than 1 percent of Android users have installed a potentially harmful app on their system when using several stores. This is 0.15 percent for users that are only connected to the Google Play Store.¹⁴⁶

- The location of users – and the app stores which they use – seems to be an important factor. For instance, Android users in China reportedly have a much higher chance of downloading a rogue app than users in other countries. For in China, intensive use is made of third-party stores instead of the official Google Play Store.^{147 148} These stores often contain repackaged apps from the official store. Criminals sometimes add malicious codes to these apps. In some cases, criminals try to place these repackaged apps in official stores as well.¹⁴⁹

Figure 2 Number of unique malware samples and share of Android malware per quarter¹⁴³



¹³⁸ <https://www.decryptcryptolocker.com/>

¹³⁹ <https://noransom.kaspersky.com/>

¹⁴⁰ http://www.symantec.com/security_response/publications/threatreport.jsp

¹⁴¹ <http://media.kaspersky.com/pdf/Kaspersky-Lab-KSN-Report-mobile-cyberthreats-web.pdf>

¹⁴² <https://know.elq.symantec.com/LP=1543>

¹⁴³ Source: AV-test Institute.

¹⁴⁴ <http://www.idc.com/getdoc.jsp?containerId=prUS25450615>

¹⁴⁵ <https://www.pulsesecure.net/lp/mobile-threat-report-2014/>

¹⁴⁶ https://source.android.com/devices/tech/security/reports/Google_Android_Security_2014_Report_Final.pdf

¹⁴⁷ https://www.f-secure.com/documents/996508/1030743/Threat_Report_H2_2013.pdf

¹⁴⁸ An important reason for the use of these alternative stores is that in China only free apps from the official Google Play Store can be installed; see <https://support.google.com/googleplay/answer/143779>.

¹⁴⁹ <http://www.trendmicro.nl/cloud-content/us/pdfs/security-intelligence/white-papers/wp-fake-apps.pdf>

Most mobile malware focuses on Android. This does not mean that users of other mobile platforms, such as Apple iOS, are not infected by malware. In many cases, however, a user need to have cracked (jailbroken) his device so that it also allows unauthorised, and therefore untrusted, apps, in order for an attack on iOS to be successful. Known examples of iOS malware discovered in this area in the past year are the Xsfer mRAT,¹⁵⁰ an RAT which used to be found on Android systems only, and Xagent,¹⁵¹ which is used to collect user data. At the end of 2014, however, the first malware for iOS was found (WireLurker).¹⁵² WireLurker does not require a jailbroken system. This malware scans and infects mobile Apple devices as soon as they are connected to the USB portal of an infected Apple Mac OS X system.

Ransomware and mobile platforms

Ransomware no longer focuses on Windows only. It has also been detected on mobile platforms. Although the simple blocking of Android-based devices is not a new development (e.g. ScarePackage¹⁵³), the first cryptoware (Simplocker¹⁵⁴) surfaced last year. Just as with traditional Windows cryptoware, this cryptoware encrypts system files. Users of Apple iOS also encountered a form of ransomware, only files were not encrypted. During this Oleg Pliss attack, the attackers displayed a message on iOS devices stating that the device had been blocked. The attackers again demanded a sum of money in order for the device to be unblocked. They probably abused the Apple IDs of victims, but it is still unclear how they retrieved the log-in data for this purpose.¹⁵⁵

Tools

Ready-made tools are popular tools

The many public reports on advanced attacks show that attackers gratefully make use of tools that have not necessarily been developed for malicious purposes, but sometimes also for the screening of systems or the performance of penetration tests. It appears that attackers do not want to reinvent the wheel and therefore opt for these standard tools. Examples are SaaS-based

services, such as booter services, which allow attackers to carry out DDoS attacks via a website.

Another example is MimiKatz, a tool that is mainly used to retrieve passwords, Kerberos tickets and hashes from the memory of a Windows system. Actors responsible for the Cleaver¹⁵⁶, Hurricane Panda¹⁵⁷ and Anunak¹⁵⁸/Carbanak¹⁵⁹ attacks use this tool to retrieve log-in data of the Windows network, thereby gaining easy access to almost all systems within the network.

In some cases, the attackers use ready-made exploits of the popular Metasploit framework.¹⁶⁰ Metasploit allows attackers to abuse known vulnerabilities and to exploit these vulnerabilities in various ways. For this purpose, they do not require any in-depth knowledge on the vulnerability or further abuse. Although the tool is intended as a tool for penetration testers, malicious parties can also use the tool to carry out digital attacks.

Ready-made exploits, exploit kits and malware are also popular

The equipment available to attackers not only includes tools, but also exploits, exploit kits and malware. It is striking that various (types of) actors use the same malware and the same exploit kits, such as the PlugX RAT and the Angler exploit kit.¹⁶¹

Public exploits mostly focus on Windows and PHP applications

Just as in previous periods, the number of public exploits further decreased again in this period (see figure 3, left). A possible explanation is that it has become more difficult to write exploits for modern software. Defence mechanisms such as sandboxing and address space layout randomization (ASLR) are used in an increasing number of products. It also appears that older exploits can still be used by attackers, as not all software is up to date. An analysis of 276 public reports on APTs shows that most of the abused vulnerabilities in targeted attacks have existed for several years.¹⁶²

Subdivided into platforms, most exploits still focus on PHP applications and applications on Windows platforms. A large part

¹⁵⁰ http://media.scmagazine.com/documents/98/xsfer_mrta_-_akamai_advisory_24310.pdf

¹⁵¹ <http://blog.trendmicro.com/trendlabs-security-intelligence/pawn-storm-update-ios-espionage-app-found/>

¹⁵² https://www.paloaltonetworks.com/content/dam/paloaltonetworks-com/en_US/assets/pdf/reports/Unit_42/unit42-wirelurker.pdf

¹⁵³ <https://www.lookout.com/resources/reports/mobile-threat-report>

¹⁵⁴ <http://www.welivesecurity.com/2014/06/04/simplocker/>

¹⁵⁵ <http://www.zdnet.com/article/icloud-not-compromised-in-apple-id-attack-apple/>

¹⁵⁶ http://www.cylance.com/assets/Cleaver/Cylance_Operation_Cleaver_Report.pdf

¹⁵⁷ <http://go.crowdstrike.com/rs/crowdstrike/images/GlobalThreatIntelReport.pdf>

¹⁵⁸ https://www.fox-it.com/en/files/2014/12/Anunak_APT-against-financial-institutions2.pdf

¹⁵⁹ https://securelist.com/files/2015/02/Carbanak_APT_eng.pdf

¹⁶⁰ See for instance <https://securelist.com/files/2014/07/EB-YetiJuly2014-Public.pdf>

¹⁶¹ <http://www.crowdstrike.com/2014-global-threat-report/>

¹⁶² Analysis on the basis of APTnotes, a public list of APT reports: <https://github.com/kbandla/APTnotes> (geraadpleegd op 13 juli 2015).

of the exploits for PHP applications focuses on (plug-ins for) Wordpress and Joomla, which are popular PHP-based content management systems (see figure 3, right). This share has slightly increased over the past few years. In the current reporting period, the joint share of Wordpress and Joomla exploits was slightly over 26 percent of the total number of PHP-based exploits. A possible explanation for the large share of these exploits is that WordPress and Joomla are the two most popular (open source) content management systems.¹⁶³

Exploit kits more often focus on Adobe Flash

Various actors use exploit kits to exploit vulnerabilities. The exploits included in these exploit kits provide a picture of the software they abuse. Figure 4 shows the development of built-in exploits for products on the basis of the content of sixty different exploit kits. Compared to the previous CSAN, Adobe Flash in particular has become a more popular target, while Adobe's PDF products have become less popular.

RATs are abused for digital payment fraud in SMEs

The police have found that, in the Netherlands, RATs are used more often for a new form of digital payment fraud. It is relatively easy

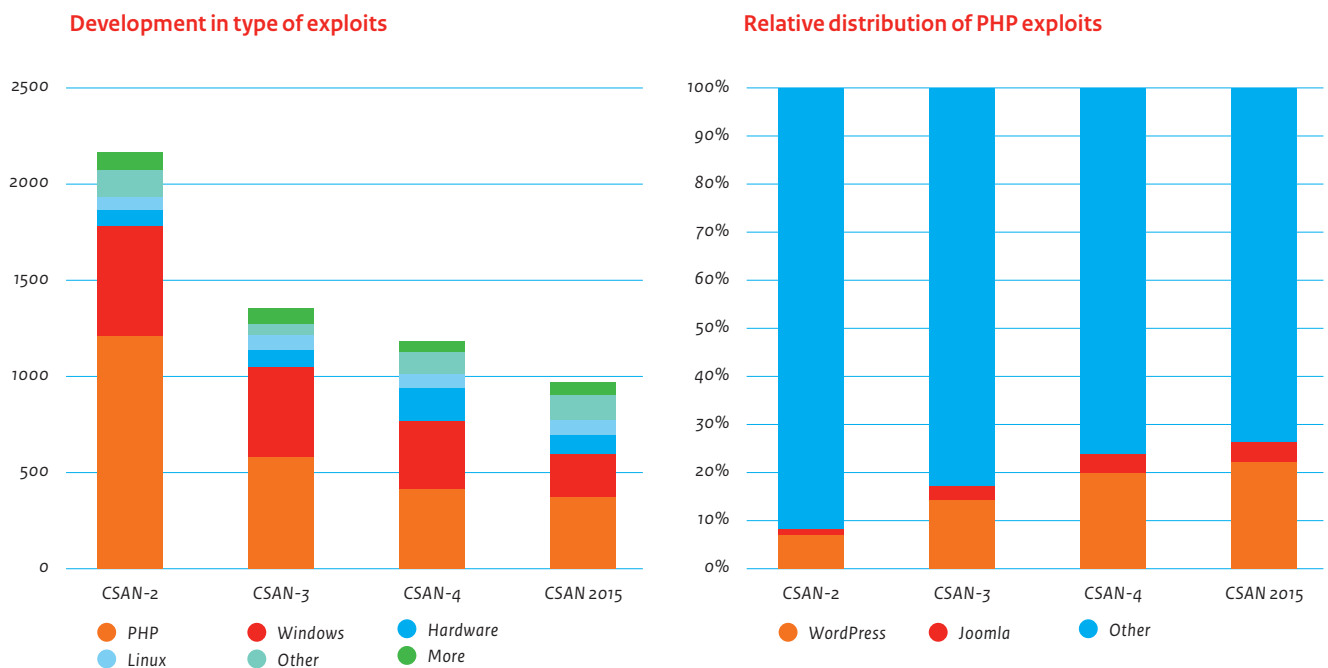
to acquire and use RATs. As a result, committing digital fraud, for example, has become accessible to various offender groups.

The use of RATs for payment fraud is a new development and seems to focus on SMEs for now. Contamination is caused by business (spear)phishing e-mails. Criminals use RATs to gain access to various payment environments of a company, for example the internet banking environment or accounting records. They then try to divert money to money mules, after which the money is laundered.

The scope of this new form of digital fraud and the damage it has caused are currently unknown. Its implications may, however, be serious:

- The impact of this type of fraud may be extensive in terms of economic and reputational damage. Moreover, the integrity of business payments is at issue.
- It concerns a relatively accessible form of cyber crime, which may be committed by a broad group of fraudsters. The malware used is inexpensive, readily available and can be used with limited digital knowledge.

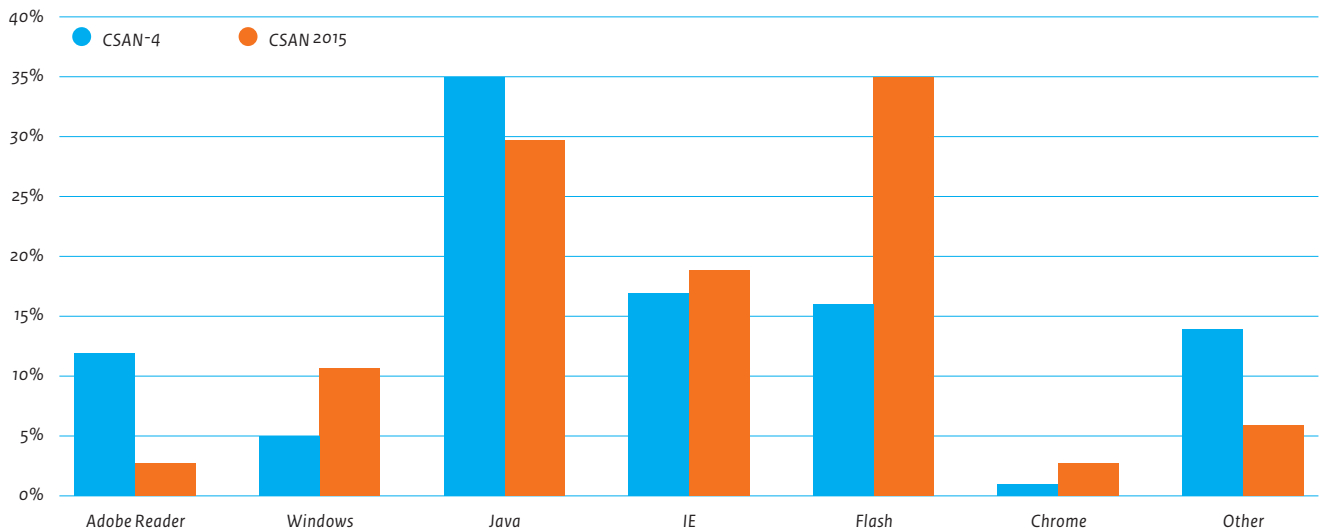
Figure 3 Number of published exploits per platform^{164 165}



¹⁶³ <http://www.opensourcecms.com/general/cms-marketshare.php>

¹⁶⁴ Source: <http://exploit-db.com/>.

¹⁶⁵ Explanation of the labels in the left figure: exploits in the 'Other' category focus on another platform (e.g. Android or ARM), while exploits in the 'Multiple' category focus on multiple platforms simultaneously (e.g. Windows and Linux).

Figure 4 Products as a target in exploit kits¹⁶⁶

Denial-of-Service attacks

DDoS attacks continue, but cause limited disruptions

DDoS attacks are still taking place, but the disruptions they cause in the Netherlands are limited. The anti-DDoS measures taken by many organisations in the Netherlands appear to be successful. Although these measures limit the impact of DDoS attacks, they require a continuous investment in often expensive solutions. Only the symptoms are combated, the attacks themselves continue to take place.

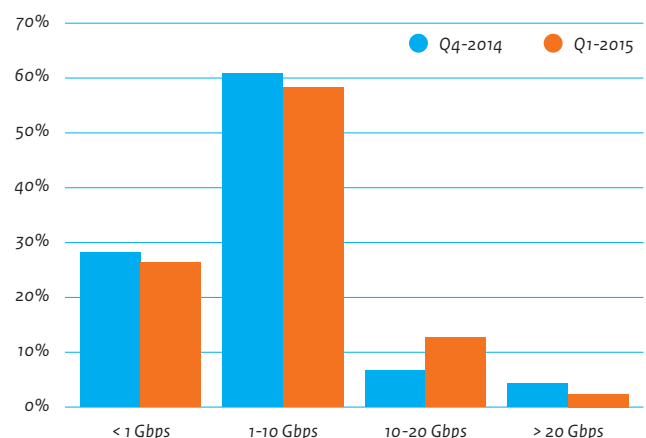
Reports¹⁶⁷ on DDoS attacks show that the maximum volume of attacks is further increasing to around 400 Gbps. Although still high, the average bandwidth of a DDoS attack appears to be much lower, with volumes between 8 and 12 Gbps. These volumes are more in line with the attacks which are detected by the target groups of the NCSC and which are experienced by a Dutch group of providers who have jointly implemented an anti-DDoS solution. The figures provided by this latter group show that almost 85 percent of the attacks had a volume of less than 10 Gbps in the first quarter of 2015 (see figure 5). This is slightly lower compared to the last quarter of 2014, when almost 90 percent of the attacks did not exceed 10 Gbps.

Another important observation is that the duration of an average DDoS attack decreases. Most attacks stop after 30 minutes to one hour. This is confirmed by the figures from the above-mentioned organised group of Dutch providers. 59 percent of attacks stop within 15 minutes and over 87 percent stop within one hour (see

figure 6). Sometimes, attacks only last for five minutes. This could indicate a free testing of booter services which can easily be used to carry out a DDoS attack (see the box 'Use of booter services'). Sometimes, the experience is that although the attacks are shorter, they are more intensive.

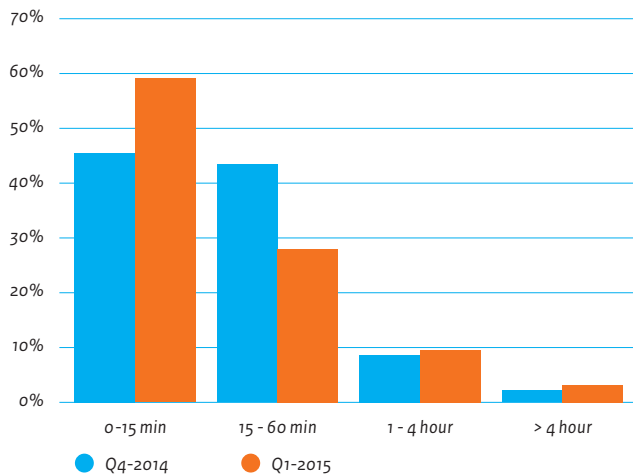
Attackers continue to search for new forms of amplification

In order for a DDoS attack to be as effective as possible, attackers continue to search for new ways to increase the amount of data they generate. Amplification is the method used by attackers for

Figure 5 Volume of DDoS attacks¹⁶⁸

¹⁶⁶ Source: <http://contagiodump.blogspot.com/>, geraadpleegd mei 2015; https://docs.google.com/spreadsheets/ccc?key=oAjvsQV3jSLa1dEgEVGhjeUhvQTNReko3czxhTmphLUE&usp=drive_web#gid=0.

¹⁶⁷ DDoS reports from Akamai, Arbor Networks, Black Lotus, BT, Corero, Link11, Kaspersky, Neustar, NSFOCUS, Radware, Symantec and Verisign have been read for this purpose.

Figure 6 Duration of DDoS attacks¹⁶⁸

Use of booter services

In the experience of the police, actors often use booter or stresser services to carry out DDoS attacks. Such services allow actors to carry out DDoS attacks which require no subject-matter knowledge (DDoS-as-a-service). A booter service combines various known DDoS attack vectors. Users can often test the services for free for a few minutes, after which they have to pay a small amount, for example 2 dollars per hour.¹⁶⁹ They can then use the service to carry out DDoS attacks on random targets.

this purpose: sending a small query and expecting a large response. In extreme cases, the response can be almost 360 times as high as the query, resulting in a very high amplification.¹⁷⁰ As amplification attacks use UDP, attackers can provide any IP address the server should send the reply to. Of course, attackers select the IP address they want to overload with traffic. Limited filtering by some network operators allows attackers to state a random IP address ('spoofing').

The NTP protocol in particular used to be a popular tool for carrying out DDoS attacks. Due to the release of a patch and a change in configurations by NTP operators, this form of amplification became less successful and attackers looked for new

forms of amplification and other DDoS techniques. As a result, more attacks have become visible over the past period which abuse other UDP-based protocols such as SSDP/UpnP¹⁷¹, SNMP¹⁷² and multicast DNS¹⁷³. Researchers also demonstrated that TCP-based protocols, apart from the traditional UDP-based protocols, may cause a high degree of amplification.¹⁷⁴

Obfuscation

For actors, it is important to stay low when carrying out digital attacks, to leave as few traces as possible and to be difficult to trace. This makes the attribution of their acts more difficult. Any activity performed by them for this purpose is called obfuscation.

Abuse of bona fide services for (encrypted) communication

Tracing suspicious traffic within a network is more difficult due to bona fide domain names, websites and services for communication by malware. Detection focuses on IP addresses and domain names known for their involvement in digital attacks (rogue IP addresses and domain names). That is why no warning is received when bona fide IP addresses and domains are used. If bona fide websites – or other services – also support TLS encryption, the information a system exchanges with such website within the network is also unclear, as detection tools have no insight into traffic at network level. So detection is only possible at locations where the information is decrypted again (at a user's work station, for example). Although this is no new development, it appears that this approach is still used by attackers.

Table 3 shows a number of recent examples of abuse of bona fide services for communication by malware. The table distinguishes between the use of services for the configuration and control of infected systems (information to the infected system) and the exfiltration of data (information from the infected system). What is striking is that apart from bona fide services, attackers sometimes also use steganography to hide the communication.

Malware writers bypass detection by not using obfuscation

Malware writers probably obfuscate their malware as much as possible in order to make it more difficult for specialists to analyse it.

¹⁶⁸ Source: organised Dutch group of providers.

¹⁶⁹ <https://www.verisigninc.com/assets/report-ddos-trends-Q42014.pdf>

¹⁷⁰ <https://www.us-cert.gov/ncas/alerts/TA14-017A>

¹⁷¹ <https://isc.sans.edu/forums/diary/1900UDP+SSDP+Scanning+and+DDOS/18599>

¹⁷² http://www.prolexic.com/kcresources/white-paper/white-paper-snmp-ntp-charge-reflection-attacks-drdoS/An_Analysis_of_DrDoS_SNMP-NTP-CHARGEN_Reflection_Attacks_White_Paper_A4_042913.pdf

¹⁷³ https://github.com/chadillac/mdns_recon

¹⁷⁴ <https://www.usenix.org/system/files/conference/woot14/woot14-kuhrer.pdf>

Table 3 Overview of abuse of bona fide services as communication channel

Goal	Abused service	Particulars
Configuring and controlling infected systems	Dropbox ^{175 176}	Changing C&C settings in targeted attacks and hosting parts of an exploit.
	Pinterest ¹⁷⁷	In order to forward users to rogue websites, information on these websites was coded and included in 'pins'.
	Reddit ¹⁷⁸	List of C&C servers included in a comment in a Reddit post.
	Vkontakte ¹⁷⁹	Information on the C&C server stored as a message on the "wall" of users of this social network.
	Google Docs ¹⁸⁰	Information on the C&C server included in a BMP file on Google Docs using steganography.
	Microsoft Technet ¹⁸¹	IP addresses of C&C servers included in comments on a Technet Forum thread.
Exfiltration of data	Gmail ¹⁸²	The attackers store data in draft messages in Gmail.
	Video services ¹⁸³	Uploading video files to, for example, YouTube containing steganographically hidden data.

It seems that sometimes, attackers choose not to do this, as they did with the foxy¹⁸⁴ and Babar malware. This makes it easier for researchers to dissect the malware, because the code can be cracked more easily, for example. The detection of malware within a network is, however, more difficult. For the use of obfuscation and encryption techniques by a program is a sign for virus scanners and other detection tools within a network to distrust a program. Attackers therefore usually do not use this in targeted attacks.¹⁸⁵ Preventing recognition is apparently more important than preventing recognition of the intentions and working method of the malware.

Attack vectors

Attack vectors are methods that attackers can use to attack their victim(s). An attack vector is the means used by an attacker to try to take control of a user's system. This paragraph discusses a number of individual attack vectors that have occurred over the past period. Attackers usually do not use one specific attack vector, but combine different vectors in order to achieve their goal.

Phishing, or spearphishing in particular, is the most frequently used tool for targeted attacks

In the past period, criminals conducted dozens of different phishing campaigns in the Netherlands alone. In many cases, the e-mails seemed to come from reliable parties, such as bol.com, post.nl,¹⁸⁶ KPN, Intrum Justitia and all major banks¹⁸⁷. Government organisations such as DigiD, the Tax and Customs Administration and the Central Fine Collection Agency were also abused as sender. The incident reports to the NCSC suggest that the emphasis is on the business sector. 37 percent of the incidents reported by private organisations were related to phishing, compared to 16 percent for government authorities.¹⁸⁸

Attackers were particularly successful when using spearphishing. In that case, one person or a limited group of persons receives a phishing e-mail. Through this e-mail, attackers try to obtain a staff member's log-in data for webmail, for example. They can then use these log-in data to carry out further attacks on other persons within the organisation. In other cases, the attackers use infected attachments or links to exploit kits to infect the system of their victim. Although the attackers do not fish for sensitive information

¹⁷⁵ <http://blog.trendmicro.com/trendlabs-security-intelligence/plugx-rat-with-time-bomb-abuses-dropbox-for-command-and-control-settings/>

¹⁷⁶ <http://blogs.cisco.com/security/a-string-of-paerls/3>

¹⁷⁷ <http://www.pcrisk.com/internet-threat-news/8568-trojan-leverages-pinterest-to-communicate-with-c-and-c-servers>

¹⁷⁸ <http://news.drweb.com/show/?i=5977&c=5&lng=en&p=0>

¹⁷⁹ <http://community.websense.com/blogs/securitylabs/archive/2015/01/30/new-foxy-malware-employs-cunning-stealth-amp-trickery.aspx>

¹⁸⁰ <http://blog.airbuscybersecurity.com/post/2014/12/Vinself>

¹⁸¹ <https://www2.fireeye.com/WEB-2015RPTAPT17.html>

¹⁸² <http://www.wired.com/2014/10/hackers-using-gmail-drafts-update-malware-steal-data/>

¹⁸³ <http://www.tripwire.com/state-of-security/incident-detection/hackers-exfiltrating-data-with-video-steganography-via-cloud-video-services/>

¹⁸⁴ <http://community.websense.com/blogs/securitylabs/archive/2015/01/29/new-foxy-malware-employs-cunning-stealth-amp-trickery.aspx>

¹⁸⁵ See the report on Babar malware, <https://drive.google.com/file/d/oBgMrr-en8FXqdzJqLWhDblhseTA/view?pli=1>.

¹⁸⁶ <https://www.security.nl/posting/405715/PostNL+waarschuwt+klanten+voor+besmette+e-mails>

¹⁸⁷ <https://www.fraudehulpdesk.nl/sub-vragen/phishingmails/>

¹⁸⁸ See Appendix 1: NCSC statistics.

directly via these attachments and links, this type of attack also constitutes spearphishing. Because of the success of spearphishing, this form of social engineering is the primary attack vector for digital espionage.

Apart from spearphishing, actors still use standard phishing as a tool. Attackers mostly use spearphishing to infect the systems of their victims for sensitive information. The purpose of standard phishing is much more to seek financial gain without choosing a select group of victims. What is striking is that the Netherlands is a popular target for phishers. Research conducted by RSA shows that a total of 3¹⁸⁹ to 6 percent¹⁹⁰ of the world's phishing e-mails focuses on Dutch users. The popularity of the Netherlands may have to do with the relatively good economic situation and the strong euro.¹⁹¹ However, the damage caused by phishing aimed at Dutch banks decreased from 4.7 million euros in 2013 to 3.9 million euros in 2014.¹⁹²

Watering hole attacks are a popular addition to spearphishing

If a spearphish is unsuccessful, attackers often choose a second popular tool for targeted attacks: a watering hole. In case of a watering hole attack, the attacker spreads his exploits and malware via a website frequently visited by many of his victims by abusing a vulnerability in this website or a CMS on which the website is based.¹⁹³ After that, the attacker usually tries to infect the systems of visitors via an exploit aimed at these systems. The use of these drive-by exploits via such websites is not a new development, but still poses a real threat. A special attack vector used in the past year was the installation of infected software on a website of a supplier of industrial routers. Customers then automatically infected their systems with the Havex RAT when installing this software.¹⁹⁴

Rogue advertisements continue to pose a danger to internet users

The use of rogue advertisements by cyber criminals (malvertising) still poses a danger to many internet users. Advertisements have been incorporated in countless websites, some of which have a high number of visitors. Attacks with rogue advertisements are therefore a form of watering hole attacks. One rogue advertisement may have a high impact in a short period of time, especially if this advertisement is shown via websites such as YouTube¹⁹⁵ or nu.nl.¹⁹⁶ If a user opens a website containing a rogue advertisement, this often results in all kinds of vulnerabilities on

the user's system being exploited fully automatically. Rogue advertisements often use exploit kits, containing high-quality exploits, which increase the chances of success for criminals. Nowadays, cyber criminals also abuse advertisement networks to attack a specific user group. They use real-time bidding (RTB) advertising networks for this purpose. Advertisements are then selected on a dynamic basis, depending, among other things, on the characteristics of the user visiting the website. An RTB network provides bona fide advertisers with the opportunity to offer their advertisement only to users that meet a certain profile (e.g. only persons with specific interests and coming from a specific country).

If an RTB network is used, malvertising will not only allow for the carrying out of random drive-by attacks, but also more targeted attacks such as in case of watering holes. Invincea discovered, for example, that specific American defence companies were attacked via rogue advertisements.¹⁹⁷ This indicates that, in the future, malvertising will not only form part of the range of tools used by the average cyber criminal, but may also be used more often in APTs.

Popular Javascript libraries offer a lot of potential for attackers

The inclusion of external Javascript and other libraries in a website has, over the past period, resulted in a number of incidents (see the box 'Javascript libraries as a tool for digital attacks'). Many websites use external Javascript libraries to easily add functionalities to a website. Examples are the popular Javascript libraries of jQuery and Google Analytics.

Website developers often directly refer to a Javascript library instead of copying this library to their own website. From a security point of view, the latter has a strong preference, because the owner of the website keeps control of what it offers to visitors. If such a library is popular, it becomes a very interesting tool for attackers. If an attacker manages to manipulate a Javascript library, this attacker may then attack all websites containing a dynamic reference to this library. The Javascript file does not always have to be adjusted immediately on the server of the maker himself. The adjustment of scripts via man-in-the-middle (MitM) attacks or the hacking of DNS records may also be effective.

189 <http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-0614.pdf>

190 <http://www.emc.com/collateral/fraud-report/rsa-online-fraud-report-102014.pdf>

191 <http://www.nu.nl/internet/3389377/nederlanders-populair-doelwit-van-phishing.html>

192 <http://www.betalvereniging.nl/wp-uploads/2015/03/150318-Fraude-betalingsverkeer-gehalveerd-20141.pdf>

193 See, for example, the method used by the Waterbug group: http://www.symantec.com/content/en/us/enterprise/media/security_response/whitepapers/waterbug-attack-group.pdf.

194 <https://www.f-secure.com/weblog/archives/00002718.html>

195 <http://blogs.cisco.com/security/talos/kyle-and-stan>

196 <http://tweakers.net/nieuws/97041/nu-punt-nl-verspreide-malware-via-geinfecteerd-advertentienetwerk-update-2.html>

197 <http://www.invincea.com/wp-content/uploads/2014/10/Micro-Targeted-Malvertising-WP-10-27-14-1.pdf>

Javascript libraries as a tool for digital attacks

Attackers from the Syrian Electronic Army (SEA) served a modified version of a Javascript file of Gigya,¹⁹⁸ a service that website owners can use to add social medial functionalities to their website. They had the domain on which this file was offered refer to their own server via a DNS-hack. As a result of the modification, users of various websites saw the message that reads “You’ve been hacked by the Syrian Electronic Army (SEA)”.

In the case of Gigya, the damage was limited to a message being displayed. This was not the case in early 2015, when an analysis script of the Chinese website Baidu referred to GitHub in some cases. As the analysis script was used by countless websites, the GitHub¹⁹⁹ website became overloaded and was unavailable or hardly available for a number of days.

During an attack on Afghan government websites, a frequently used Javascript of these websites was modified and offered via a distribution network.²⁰⁰ According to ThreatConnect researchers, this was abused in order to infect visitors via watering hole attacks.

The impact of a rogue Javascript can be compared with the impact of malvertising. In both cases, a large group of users is offered a single piece of rogue code in a short period of time.

Macros are a popular attack vector (again)

Recent malware families such as Dridex,²⁰¹ Vawtrak²⁰² and Cryptodefense²⁰³ are examples of malware that are installed on systems of end users through rogue macros. The abuse of Office macros by malware is not a new phenomenon. In 1995, the Concept virus was the first virus that abused these macros and, in 1999, the infamous Melissa virus used macros to spread itself further.²⁰⁴ Despite the fact that the first abuse of macros dates back twenty years, it still appears to be attractive.

In the past, macros were used to spread viruses within a network. Nowadays, malicious parties mostly use macros to download and install additional malware on a system. Another important difference with the early days of macro malware is that Office products normally no longer run macros automatically.

The attacks with macros often make use of social engineering to convince users to enable macros.²⁰⁵

(Wireless) routers appear to be interesting tools for attackers

Attackers are interested in routers of private individuals and small businesses in order to carry out digital attacks, as shown in the examples in the box ‘Possible uses of compromised routers’. An important reason for this could be that these routers can be attacked in various ways. Non-infected systems within a network may also be accessed via these routers and successfully infected routers offer various possibilities to malicious parties. There are only few users who install the required updates on these routers, which allows for vulnerabilities to be abused for a long period of time. In early 2015, it became known that infected routers were used as part of the LizardStresser service in order to carry out DDoS attacks.²⁰⁶

Conclusion and looking ahead

Given the rapid emergence of ransomware, a further growth of this type of malware is expected in the future. Ransomware mostly focuses on traditional PCs and also on smartphones now. Due to the ever growing connectivity of systems, however, it is conceivable that ransomware will, in the future, also focus on other devices that are connected to the internet. Imagine that, in the future, it is possible to disable a television or car by infecting it with ransomware. Chances are that a victim will pay the amount demanded so that he can watch TV or start the car again. It is also conceivable that ransomware will be used to frustrate the operational management of an organisation.

¹⁹⁸ <https://nakedsecurity.sophos.com/2014/11/28/syrian-electronic-army-returns-with-thanksgiving-press-hack/>

¹⁹⁹ <http://arstechnica.com/security/2015/03/github-battles-largest-ddos-in-sites-history-targeted-at-anti-censorship-tools/>

²⁰⁰ <http://www.threatconnect.com/news/operation-poisoned-helmand/>

²⁰¹ <http://blogs.technet.com/b/mmpc/archive/2015/01/02/before-you-enable-those-macros.aspx>

²⁰² <http://blog.trendmicro.com/trendlabs-security-intelligence/banking-malware-vawtrak-now-uses-malicious-macros-abuses-windows-powershell/>

²⁰³ <http://www.symantec.com/connect/blogs/ransomware-return-macro>

²⁰⁴ <http://edition.cnn.com/TECH/computing/9903/29/melissa.idg/>

²⁰⁵ <http://stopmalvertising.com/malware-reports/macro-viruses-a-blast-from-the-past.html>

²⁰⁶ <http://krebsonsecurity.com/2015/01/lizard-stresser-runs-on-hacked-home-routers/>

Possible uses of compromised routers

A compromised router is an interesting tool for many malicious parties. Some examples from last year:

- The adjustment of DNS settings on routers allows attackers to redirect users in the home network to rogue web pages or to provide them with rogue updates without the system in the network itself having been infected.²⁰⁷
- Routers are a convenient tool for carrying out DDoS attacks, for example if the router is part of a botnet or if the router has opened a service that can be abused for amplification attacks, such as DNS.²⁰⁸
- A worm can spread through home routers, as shown by the Moon worm.²⁰⁹
- Normally, a router protects internal systems, but if the router has been compromised, attackers can penetrate this protection. They will then have access to, for example, external hard drives that are connected to the router via USB.²¹⁰
- Malware on a router can manipulate traffic without being detected. In case of internet voting, for example, a person may, without noticing it, vote for another candidate²¹¹ or malware is injected into incoming traffic.

It can, however, be explained why the development of a trojan for mobile platforms is so expensive compared to traditional systems. In traditional systems, many people use the same browsers for all the services they consult. On mobile platforms, however, people use separate apps with different designs, protocols and techniques. In order to attack these apps, an attacker will, in many cases, have to write a targeted, and therefore expensive, trojan for a specific app. So as long as writing malware for traditional PCs remains more profitable, the amount of malware for mobile platforms will not suddenly increase.

Finally, techniques and methods of attack that have existed for some time will continue to cause problems in the coming period. For instance, spearphishing will continue to be used by various actors to break into the systems of their victims, malvertising will continue to be used to infect large groups of users in a short period of time with, for example, ransomware, it will become increasingly difficult to detect and trace back digital attacks and criminals will, in all these cases, keep refining their approach.

Actors already use DDoS attacks to frustrate services. It is not always clear why an actor carries out this type of attack. Chances are that criminals will use DDoS attacks more often for financial gain, just as with ransomware. When carrying out a DDoS attack, a criminal locks part of the infrastructure of an organisation and as a ransom is demanded to unlock it, the model for DDoS attacks may become similar to the model for ransomware. An example of such manifestation which is already visible is, is the DD4BC group, which threatens to carry out a DDoS attack if the organisation refuses to pay bitcoins to the attacker.²¹²

The question remains whether malware on mobile platforms will actually cause serious problems. This threat exists at present, but is still limited. It seems that the architecture of mobile platforms is not yet attractive for criminals in order to carry out large-scale attacks. It could be that it is simply still too expensive to make a trojan for mobile platforms and that traditional trojans still generate sufficient money. This may be an explanation for the fact that less fraud with banking apps is detected.²¹³

207 http://www.cert.pl/news/8019/langswitch_lang/en;https://securelist.com/blog/incidents/66358/web-based-attack-targeting-home-routers-the-brazilian-way/;https://www.proofpoint.com/us/threat-insight/post/Phish-Pharm

208 <http://nominum.com/news-post/24m-home-routers-expose-ddos/>

209 <https://isc.sans.edu/diary/Linksys+Worm+%22TheMoon%22+Summary%3A+What+we+know+so+far/17633>

210 <http://www.pcworld.com/article/2086280/default-settings-leave-external-hard-drives-connected-to-asus-routers-wide-open.html>

211 <http://galois.com/wp-content/uploads/2014/11/technical-hack-a-pdf.pdf>

212 <https://blogs.akamai.com/2015/04/dd4bc-operation-profile-medium-risk.html>

213 <https://www.security.nl/posting/431645/ING%3A+mobiel+bankieren+apps+niet+interessant+voor+crimineel>

.....
*There is no cloud, just other people's
computers.*



4 Resilience: vulnerabilities

In the past year, the image of vulnerabilities was determined by publicity campaigns such as Heartbleed, having a name, logo and website. As a result, the general public became more familiar with vulnerabilities in software. Attention was also paid to users as a source of vulnerabilities due to phishing attacks and to security problems of cloud services. Vulnerabilities in software are still the Achilles' heel of cyber security.

A vulnerability is a property of IT, an organisation or a user that can be abused by actors to achieve their goals or which can lead to a disruption through a natural or technical event. This chapter deals with the developments in the field of vulnerabilities.

Organisational developments

Vulnerabilities with publicity campaigns

In the past reporting period, technical vulnerabilities attracted a lot more publicity. Heartbleed, one of the most well-known vulnerabilities of 2014, marked the beginning of this.²¹⁴ The vulnerability in OpenSSL allowed attackers to read out the internal memory of systems from a distance. At the time Heartbleed was made public, the persons who discovered it had created a full website, including a slick logo. The campaign underlined that security of open source solutions such as OpenSSL depends on financial support, among other things.

Other vulnerabilities were also made public through similar campaigns. Shellshock,²¹⁵ a vulnerability in the Bash shell, was made public in September 2014. Shellshock allowed attackers to execute commands on infected systems from a distance.

²¹⁴ <http://heartbleed.com/>

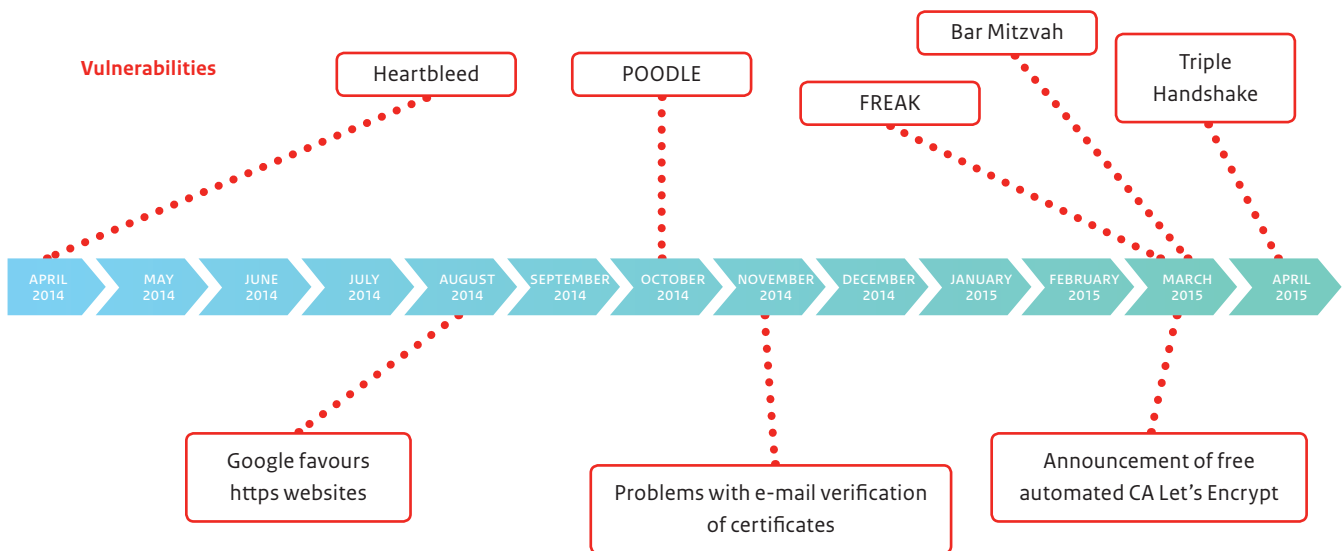
²¹⁵ <https://securityblog.redhat.com/2014/09/24/bash-specially-crafted-environment-variables-code-injection-attack/>

²¹⁶ Published with the permission of the creator, Ken Westin.

Figure 7 Overview of the vulnerabilities that attracted a lot of attention²¹⁶



Figure 8 Developments surrounding TLS in the past year



As the Bash shell is an important part of Linux is, which is used by many other programs, the impact of this vulnerability was high.

POODLE was made public in October 2014.²¹⁷ This vulnerability allowed attackers to break into secure connections that used SSLv3. This vulnerability was announced beforehand without any details in order to prepare for updates, but this time, only a written article was published and no website or logo were created. The vulnerability clearly showed that SSLv3 really could no longer be considered as safe and had to be phased out. Linux vulnerability GHOST was also made public in detail in January 2015. This vulnerability was shared with most Linux distributions in advance, so that its impact remained limited.

The next cryptographic vulnerability, FREAK,²¹⁸ was announced in March 2015. This vulnerability allowed attackers to lower the security level of secure connections. As a result, weak key material was used for these connections, which could then be hacked easily. The announcement was supported with a website, this time without a logo, and again attracted a lot of publicity. The FREAK vulnerability showed that weakening cryptography under the pressure of export controls²¹⁹ can have considerable consequences.

Various sectors have reported that these publicity campaigns involve a risk. Due to the great deal of attention that is paid to individual vulnerabilities, the issues of the day may divert attention from structural solutions. In that case, management will not always make decisions based on the correct information. Organisations will form the picture that security officers are insufficient prepared.

In the past year, researchers were hoping that a number of other vulnerabilities also received the same amount of publicity, but they did not. An example is the Triple Handshake,²²⁰ a vulnerability in the TLS protocol that allowed attackers to listen in on secure connections in some cases. This (complex) vulnerability was solved relatively quickly by the various implementations.

Another example was the Bar Mitzvah attack²²¹ that was made public in March 2015. This attack made use of an old vulnerability in RC4. Since as early as 2013, this cryptographic method has been known to be very weak.^{222 223} If systems are designed not to make use of RC4, they are not vulnerable to this attack.

²¹⁷ <https://www.openssl.org/~bodo/ssl-poodle.pdf>

²¹⁸ <https://freakattack.com/>

²¹⁹ http://en.wikipedia.org/wiki/Crypto_Wars

²²⁰ <https://www.secure-resumption.com/>

²²¹ http://www.imperva.com/docs/HII_Attacking_SSL_when_using_RC4.pdf

²²² <http://www.isg.rhul.ac.uk/tls/>

²²³ <https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen/NCSC-2013-0208+1.00+Gebruik+RC4+in+TLS+ontra-den.html>

Cloud infrastructure as an extension of the corporate network

Due to the increasing use of cloud services users are faced with a number of challenges. They have to take security measures themselves. Moreover, the security of the infrastructure of the cloud itself may be a problem. At the front, it is not always clear that providers of certain services make use (behind the screens) of cloud services, such as the Amazon cloud as a platform for mobile apps. Recent research²²⁴ shows that the average company uses more than 500 cloud apps.

As cloud services are used more often, it is not only necessary to properly secure the corporate network, but also the access to cloud services and the storage of data. Moreover, many of these 'other people's computers' are not located in the Netherlands. This increases the risk of espionage²²⁵ or violation of privacy legislation.²²⁶

Remaining up to date

Vulnerabilities in software are solved by suppliers by releasing updates. If software is not up to date, the vulnerabilities will remain.²²⁷ This is because users are insufficiently familiar with the necessity of updates, or because updates cause conflicts with other programs. Research²²⁸ shows that almost 80 percent of the abused vulnerabilities of the most common exploit kits are more than one year old. The fact that old vulnerabilities are still relevant is also shown by figures from the Dutch Consumers' Association:²²⁹ 39 percent of the computers investigated contained outdated versions of Java, Adobe Flash or Adobe Reader. The content management systems of web pages also contain many vulnerabilities.²³⁰

In the past year, a lot of attention was paid to the end of life of Windows XP. After 14 April 2014, no more updates would be released for Windows XP. According to statcounter.com,²³¹ the number of Dutch Windows XP users was halved during the reporting period. However, 3.1 percent of the Dutch still use Windows XP. The predicted 'XPocalypse' (also referred to in the previous CSAN) did, however, not happen.

Applications and operating systems often still inform users of updates, whether or not via the software itself. This is not always the case with other devices. Even if users are aware of the fact that updates need to be installed, actually installing these updates is not always easy. This is the case, for example, with home routers, devices in the Internet of Things²³² and ICS. The security of these billions of devices is a matter of great concern for researchers and security officers.²³³

User as a vulnerability?

In the past year, several technical developments showed that it is risky to rely on user awareness as a basis for solving vulnerabilities. E-mails with phishing attempts can hardly be distinguished from genuine e-mails. The security of accounts for web services also appeared to be insufficient, resulting in large amounts of sensitive information becoming public knowledge.

Phishing

Phishing is a well-known subject that was discussed in previous editions of the CSAN. This year, too, this form of social engineering was a popular vulnerability to be exploited. The quality of phishing texts has increased. Users can hardly be blamed for buying them. Recent research²³⁴ conducted by Google shows that as high as 45 percent of users walk into the trap of a well-executed phishing e-mail.

A domain name holder can make phishing from his domain more difficult by using the standards DomainKeys Identified Mail (DKIM), Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting, and Conformance (DMARC). Legitimate e-mail from his domain can then be recognised, which makes phishing more difficult. The use of these standards is, however, lagging behind: within the government, DKIM is enabled on 10.5 percent of the domain names, SPF on 7.7 percent and DMARC on 4.4 percent.²³⁵ This use was higher for the .nl domains for e-mail tested at internet.nl. Here, DKIM was enabled on 42.1 percent of the domains, SPF on 55.6 percent and DMARC on 15.3 percent.²³⁶

224 <https://blog.cloudsecurityalliance.org/2015/04/23/compromised-accounts-and-cloud-activity/>

225 See also the 2014 annual report of the AIVD.

226 https://cbpweb.nl/sites/default/files/downloads/med/med_20120910-zienswijze-toepassing-wbp-surfmarket-cloud-computing.pdf

227 <https://www.security.nl/posting/424028/Ongepatchte+Microsoft+Office+zwakke+plek+Windowsgebruikers>

228 <http://contagiodump.blogspot.nl/2010/06/overview-of-exploit-packs-update.html>

229 <http://www.consumentenbond.nl/actueel/nieuws/2015/tweederde-windows-pc-s-heeft-ernstige-beveiligingsproblemen/>

230 See Chapter 3 for details.

231 <http://gs.statcounter.com/#desktop-os-NL-monthly-201404-201504>

232 See also the section "Internet of Things" in the CSAN-4.

233 See for instance <http://www.forbes.com/sites/chrisclearfield/2013/09/18/why-the-ftc-cant-regulate-the-internet-of-things/>

234 http://services.google.com/fh/files/blogs/google_hijacking_study_2014.pdf

235 Measured by internet.nl on 9430 government domain names, July 2015.

236 Results of scans by visitors of internet.nl on 863 e-mail domains, period April-July 2015.

The increasing overlap between business and private use of equipment makes it more difficult for organisations to prevent phishing using e-mail filtering. For phishing e-mails are also received on private accounts. As a result of Bring Your Own Device (BYOD), phishing poses an indirect threat to the corporate network. Several critical infrastructure sectors have indicated that they are struggling with these problems.

Log-in data for the cloud are a weak link

More and more data are stored in the cloud. That is why cloud access security becomes increasingly important. In 2014, the “Fappening” drew attention to the vulnerability of traditional log-in methods. The incident received a lot of media attention,²³⁷ as many compromising photos of celebrities were published.

At first, a technical vulnerability at Apple seemed to have caused the incident, as many photos came from Apple iCloud. Later, this appeared to be more nuanced; the attackers probably collected information in a targeted manner and abused weak password recovery mechanisms in order to gain access to the photos.

This incident made regular users more aware of the risks of storing data in the cloud. In turn, this increased the willingness of the makers of these programs to take action. The password recovery mechanisms of many cloud services have become more secured over the past year. This was often done by introducing two-factor authentication or by improving control before passwords can be reset.

Technical developments

Vulnerabilities also developed in a technical area. In addition to attacks on firmware with a high impact, a new type of vulnerability of mobile telephone networks was made public.

Vulnerabilities in firmware

Firmware is software that is used in devices such as hard drives and USB sticks, but also in washing machines, cars and other devices. Vulnerabilities in firmware can have major consequences, but it is unknown how many vulnerabilities firmware contains. During the reporting period, a number of vulnerabilities in various types of firmware were made public. These discoveries confirmed that attacks become increasingly difficult to detect. After infection, it is nearly impossible to detect the attack on the device itself.

In August and October 2014, presentations were given on BadUSB, a vulnerability in USB firmware. A computer may become infected by plugging a USB device in the computer. The new technique of

BadUSB can cause an infection without a user or anti-virus software detecting this.

The firmware of hard drives can also be abused. This was published in a report on the Equation Group. The abuse of vulnerabilities in this firmware requires substantial knowledge and has a serious impact. The Equation Group abused these vulnerabilities only sporadically, probably only in order to attack important targets.²³⁸ This shows its great value to attackers.

A computer also contains firmware that is used to start up the computer. A vulnerability was found in this firmware as well. In March 2015, it appeared that UEFI firmware was vulnerable. An attacker that abused this vulnerability was able to install malware on the system. Firmware bypasses security mechanisms of an operating system, because firmware is used in the system at a low level. The infection may persist even after the hard drive has been erased in full.

Mobile telephone network

Vulnerabilities were also found in mobile telephone networks.²³⁹ Providers use the SS7 protocol to pass on calls to each other. It appeared that SS7 took too little account of security. Attackers could intercept calls and text messages. As it concerns a defect in the protocol (and not a software error), it is difficult to fully repair this vulnerability.

Conclusion and looking ahead

The development of the cloud clearly continues. As a result, both users and companies are faced with a challenge. For users, it is not always clear that data are stored in the cloud. Access security for cloud services has been a point for attention. Many services have switched to two-factor authentication. For companies, the cloud is an extension of their own facilities. This means that access to and storage of data in cloud services should be properly assessed. If a cloud is poorly secured, the risk of espionage or a violation of privacy legislation will increase.

Over the past few years, various campaigns have been conducted in order to make users aware of digital threats and possible protection against these threats. Abuse of vulnerabilities becomes more advanced and more difficult to detect. Some phishing e-mails are so carefully written that users can hardly be blamed for buying them.

Attention should also be paid to the security of underlying infrastructure. Vulnerabilities in firmware of devices cause security risks at a low level, which are very difficult to detect.

²³⁷ http://en.wikipedia.org/wiki/2014_celebrity_photo_hack

²³⁸ https://securelist.com/files/2015/02/Equation_group_questions_and_answers.pdf

²³⁹ <http://www.washingtonpost.com/blogs/the-switch/wp/2014/12/18/german-researchers-discover-a-flaw-that-could-let-anyone-listen-to-your-cell-calls-and-read-your-texts/>

Developments in security on the transport layer

The use of https offers advantages for all types of web services. It prevents any unwanted monitoring of user browsing behaviour. It also offers protection against watering hole attacks, as the authenticity of the content can be guaranteed better. Finally, https is more attractive for web services as Google places https websites higher in the search results.²⁴⁰ In April 2015, Google even added a feature to its Chrome browser, warning users of websites without https.

The use of encryption is becoming increasingly accessible. In November 2014, it was announced that in mid-2015, a new free certificate authority, Let's Encrypt, will open its doors. Let's Encrypt automates the process of applying for and issuing certificates. Nowadays, most web services also offer their services in https, or even automatically switch to a secure connection.

22.1 percent of the world's most popular websites use https.²⁴¹ 19.4 percent of the government's websites use https. 29.4 percent of these websites use a safe configuration based on the NCSC's IT security guidelines for TLS. This is 5.8 of the total.

The increase in the use of https also causes other risks to decrease. The risks of open wireless networks have been pointed out for years. If all website traffic uses https in the right way, it will be much more difficult to attack users of open wireless networks.

²⁴⁰ <http://googlewebmastercentral.blogspot.nl/2014/08/https-as-ranking-signal.html>

²⁴¹ Measured by internet.nl on 9430 government domain names, July 2015.

.....

Sharing threat information will allow organisations to gain a more complete picture of (potential) threats with less effort.



5 Resilience: measures

Competence is increased as a result of a conscious implementation of technical and non-technical measures. In the financial sector, the measures taken were effective: they resulted in, for example, certain attacks being carried out less frequently or not at all, or no longer causing any damage. There are, however, also threats that are more difficult to combat. Measures are subject to constant change due to new vulnerabilities.

This chapter discusses measures that increase the resistance and resilience of individuals, organisations and society and limit human and technical vulnerabilities. Measures may be preventive or reactive in nature and are aimed at human beings or at systems (technology).

Human beings

Home users, employees, employers and entrepreneurs may affect resilience both positively and negatively. The extent to which one is aware of the interests, vulnerabilities and threats present and the way in which one deals with the associated risks play a crucial role here. In addition to conscious and competent users, there should be sufficient professionals available in order to remedy the continuous stream of vulnerabilities. They can offer solutions that we can use to better protect ourselves from increasingly advanced threats.

Conscious and competent users act more safely

In February 2015, the European Commission published the Eurobarometer 2014, a public opinion survey on cyber security in the 28 EU Member States.²⁴² Dutch respondents indicated that they are well informed of the risks of cyber crime (67 percent versus an EU average of 47 percent). The concerns raised by Dutch respondents on internet use do not differ much from those raised by respondents from other Member States. However, they more often change the way they use the internet. For instance, more

Dutch respondents have installed anti-virus software (82 percent versus an EU average of 61 percent) and Dutch respondents more often do not open e-mails from people they do not know (71 percent versus an EU average of 49 percent). Moreover, Dutch respondents are less likely to give personal information on websites (65 percent versus an EU average of 38 percent) and more often use different passwords for different websites (58 percent versus an EU average of 31 percent).²⁴³

In the past period, cyber security in general and specific topics of cyber security were brought to the attention of Dutch nationals in various ways. This was often done during national and international campaigns, such as the European Cyber Security Month,²⁴⁴ Alert Online,²⁴⁵ 'Hang op, klik weg, bel uw bank'²⁴⁶ ('Hang up, click close, call your bank') and Safer Internet Day.²⁴⁷

Organisations have difficulty recruiting sufficient cyber security professionals

'The' cyber security professional does not exist. Cyber security is a complex subject, to be approached by various disciplines

²⁴² http://ec.europa.eu/public_opinion/archives/ebs/ebs_q23_en.pdf

²⁴³ http://ec.europa.eu/public_opinion/archives/ebs/ebs_q23_fact_nl_nl.pdf

²⁴⁴ <http://cybersecuritymonth.eu/>

²⁴⁵ <https://www.alertonline.nl/>

²⁴⁶ <https://www.veiligbankieren.nl/>

²⁴⁷ <https://www.saferinternetday.nl/>

'Hang op, klik weg, bel uw bank' campaign

While, in 2014, the total damage caused by internet banking fraud more than halved compared to 2013 (from 9.6 million euros in 2013 to 4.7 million euros in 2014), the damage caused by phishing 'merely' decreased from 4.7 million euros to 3.9 million euros.²⁴⁸ This was a reason for banks to continue to draw attention to this subject, for example during the 'Hang op, klik weg, bel uw bank' ('hang up, click close, call your bank') campaign. In a number of national radio and television commercials and on the related website, it was explained how users can arm themselves against phishing, social engineering and other forms of internet banking fraud.²⁴⁹

(computer and behavioural sciences and the law, for example).²⁵⁰ Some positions specifically focus on cyber security, but for other positions, cyber security is only part of the job. Moreover, the orientation level of the positions may vary: strategic, tactical and/or operational.

Several universities offer Master's degree programmes in cyber security

In 2015, three university Master's degree programmes in cyber security were launched. The Cyber Security Academy, an initiative of the Leiden University, the Delft University of Technology and the Hague University of Applied Sciences, started offering the executive Master's degree programme in Cyber Security in January 2015. In September 2015, the Delft University of Technology and the University of Twente started the 3TU Cyber Security Master's degree programme. The TRU/e Master's degree programme in Cyber Security at the Radboud University and the Eindhoven University of Technology also started in September 2015. The 3TU and TRU/e programmes are the follow-up to the Kerckhoffs Institute, having offered a specialised Master's degree programme in cyber security since 2006. The Master's degree programme in System and Network Engineering of the University of Amsterdam, which has been offered since 2003, is another well-known preparatory programme for cyber security professionals.

The gap between the supply of and demand for cyber security professionals receives a lot of worldwide attention.

A survey conducted among more than three thousand business and IT professionals worldwide showed that 86 percent of them believe that there is a shortage of competent cyber security professionals.²⁵¹

Cisco's 2014 annual security report speaks of a shortage of over one million professionals worldwide.²⁵² Various countries, including the United States²⁵³ and the Netherlands, have conducted a labour study into cyber security professionals.

The study into the supply of and demand for cyber security professionals in the Netherlands was conducted by PLATO and Ockham IPS,²⁵⁴ on the instructions of the Research and Documentation Centre (Wetenschappelijk Onderzoeks- en Documentatiecentrum, WODC). The study shows that the demand for professionals will increase in the next five years, but that, in terms of numbers, the supply will be sufficient to meet the demand. However, supply and demand do not properly match at present. Although sufficient students participate in relevant degree programmes, too few students move on to specific cyber security positions and the alignment of education and employment is insufficient.

Technology

Although human beings are often considered to be the weakest link in the cyber security chain, technology is also indispensable for guaranteeing cyber security. This paragraph discusses the most important developments in this area over the past period.

Two-factor authentication becomes popular

The most common way to gain access to an account is by means of a user name and password. This technology has been used for decades. Users often choose simple passwords that are easy to remember. This allows malicious parties to gain access to accounts more easily. More and more websites support two-factor authentication.²⁵⁵ This technology prevents attackers from gaining access to accounts through phishing or by guessing passwords. An example of two-factor authentication is the DigiD-authentication level 'DigiD Midden': citizens receive a text message containing a verification code after having logged in with their user name and password. The use of 'DigiD Midden' increased in 2014 by 32.7 percent compared to 2013. At present, 80 percent of DigiD users can make use of 'DigiD Midden'.²⁵⁶

248 <http://www.betaalvereniging.nl/wp-uploads/2015/03/150318-Fraude-betalingsverkeer-gehalveerd-20141.pdf>

249 https://www.veiligbankieren.nl/nl/nieuws/nieuwe-campagne-veilig-bankieren_hang-op_klik-weg_bel-uw-bank_.html

250 <https://www.salve.edu/sites/default/files/filesfield/documents/Professionalizing-Cybersecurity.pdf>

251 http://www.isaca.org/cyber/Documents/2015-Global-Cybersecurity-Status-Report-Data-Sheet_mkt_Eng_0115.pdf

252 http://www.cisco.com/web/offer/gist_ty2_asset/Cisco_2014_ASR.pdf

253 http://www.rand.org/content/dam/rand/pubs/research_reports/RR400/RR430/RAND_RR430.pdf en <https://www.salve.edu/sites/default/files/filesfield/documents/Professionalizing-Cybersecurity.pdf>

254 <http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2015/05/02/tk-bijlage-eindrapport-arbeidsmarkt-cybersecurity-professionals.html>

255 An overview is available at <https://twofactorauth.org/>.

256 <https://zoek.officielebekendmakingen.nl/kst-31200-III-3-b1.pdf>

Recruitment in cyber security: many vacancies, few people

The labour market for cyber security professionals has, for some time now, been characterised by a large difference between the supply of and demand for (technical) cyber security professionals. The number of vacancies is increasing. Organisations often experience difficulties in filling job vacancies. This applies to technical cyber security positions in particular.

The government has also recruited new staff members in this area over the past period.

- Team High Tech Crime (THTC) organised another Cyber Crime Challenge and the planned capacity increase to 119 FTEs was realised at the end of 2014.²⁵⁷ The regional units also started recruiting an additional 100 digital experts.
- The team that is engaged in high tech crime at the National Public Prosecutors' Office was expanded from four to seven FTEs.²⁵⁸
- The Ministry of Defence set up the Defence Cyber Expertise Centre and the Defence Cyber Command. The Defence Cyber Expertise Centre is responsible for the development, retention and dissemination of knowledge about cyber security within the Ministry of Defence.²⁵⁹ It is expanded to 18 FTEs. The Defence Cyber Command is responsible for the integration of cyber security into military operations and the development²⁶⁰ of offensive cyber capabilities. Sixty new staff members were recruited for the Defence Cyber Command.²⁶¹
- The Joint Sigint Cyber Unit of the AIVD and MIVD started in June 2014. The joint unit carries out activities to assist the AIVD and MIVD in the exercise of (special) powers in the area of signals intelligence (Sigint) and Cyber. Signals intelligence is intelligence that is gathered from (tele)communications. Cyber is used as a collective name for different activities that are related to computer networks and data flows.²⁶²
- Since 1 January 2015, the NCSC has started the National Cyber Security Operations Center (NCSOC), which acts as a reporting centre 24 hours a day and 7 days a week, detects new threats and vulnerabilities and provides its network with information.²⁶³ This start also involved a staff expansion.

Cryptography plays a key role in technical security

Cryptographic protocols can be used to encrypt information. This is usually applied when the information is sent or stored over a network. Several vulnerabilities in cryptographic applications (including Heartbleed, POODLE and FREAK) have led to updates having to be installed on devices and keys and certificates having to be replaced.

Transport Layer Security (TLS) is a protocol for setting up and using a cryptographically secure connection between two computer systems, e.g. a client and a server. TLS is used for various purposes, including web traffic (https), e-mail traffic (IMAP and SMTP over STARTTLS) and certain types of virtual private networks (VPN). There are various configuration options for TLS and not all options are safe. 13.7 percent of the websites with .nl domain names tested at www.internet.nl used a safe TLS configuration based on the NCSC's IT security guidelines for TLS.²⁶⁴

DNS Security Extensions (DNSSEC) is a form of cryptographic security for the DNS protocol.²⁶⁵ Since 15 May 2012, it has been possible to use DNSSEC for all .nl domain names. DNS has always been vulnerable to malicious parties. This increases the chance of internet users visiting a rogue website, while the domain name used is correct. When DNSSEC is used, it is checked whether the reply given is authentic and comes from the correct source. So users can verify if they are visiting the correct website. This increases the reliability of DNS. Over the past period, the use of DNSSEC has increased by 12 percent: over 43 percent of the .nl zone is now protected.²⁶⁶ This percentage is lower for the government: 7.8 percent of the government's domain names are protected with DNSSEC.²⁶⁷ Half of all DNSSEC-secured domain names worldwide end on .nl. So the Netherlands is far ahead in absolute numbers.

Detection capacity is essential for the discovery of advanced attacks

Earlier DDoS attacks have resulted in more detecting and mitigating measures. The measures taken in the financial sector against DDoS attacks appear to be effective. DDoS attacks no longer cause any major problems in the financial sector. More advanced attacks such as Advanced Persistent Threats (APTs) are a different story. These attacks, aimed at organisations in various sectors, often bypass existing security measures and are very difficult to detect. It often

²⁵⁷ The Hague Unit Annual Report 2014, via <http://www.regioburgemeesters.nl/regio/6-den-haag/>.

²⁵⁸ <http://www.tweedekamer.nl/kamerstukken/detail?id=2015Do4792>

²⁵⁹ <http://www.vovklic.nl/intercom/2014/3/33.pdf>

²⁶⁰ <http://www.defensie.nl/actueel/nieuws/2014/09/25/minister-geeft-startschot-voor-defensie-cyber-commando>

²⁶¹ <https://tweakers.net/nieuws/98679/minister-van-defensie-opent-cyber-commando-krijgsonderdeel.html>

²⁶² <https://www.aivd.nl/publicaties/@3115/joint-sigint-cyber/>

²⁶³ <https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/24-uurs-hulp.html>

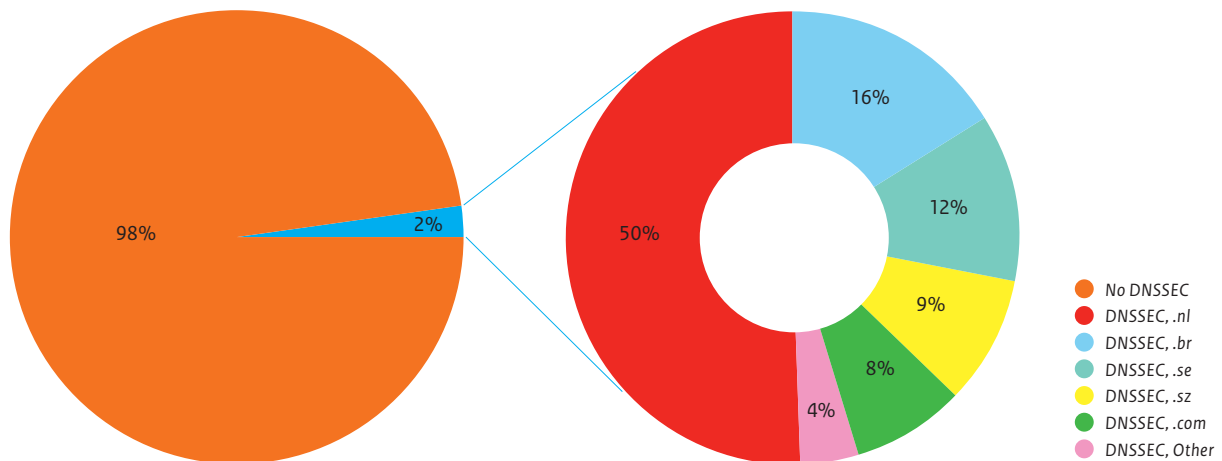
²⁶⁴ Results of scans by visitors of [internet.nl](http://www.internet.nl) on 3067 domain names, period April-July 2015.

²⁶⁵ <http://dnssec.nl/wat-is-dnssec/overzicht.html>

²⁶⁶ <https://stats.sidnlabs.nl/>

²⁶⁷ Measured by [internet.nl](http://www.internet.nl) on 9430 government domain names, July 2015.

Figure 9 Use of DNSSEC on domain names worldwide and under specific top level domains.



Left: global ratio of DNSSEC/no DNSSEC. Right: structure of domain names that use DNSSEC.²⁶⁸

Restricting cryptography

As cryptography can complicate investigations, some government bodies argue for restricting the use of cryptography. This wish was already expressed long ago: in the 1990s, for example, the United States restricted the export of strong cryptography.²⁶⁹ In January 2015, there was a new discussion on this topic, also in the Netherlands, when David Cameron, the prime minister of the United Kingdom, said during a press conference that, due to new counterterrorist measures, he wants to ban communications services that use end-to-end encryption (such as WhatsApp). According to Cameron, secret services should always be able to access the content of such communication.²⁷⁰ Those opposing such restrictions mostly point out the importance of cryptography for digital security, privacy and economic activities. They also have doubts about the feasibility and effectiveness of such ban.²⁷¹

takes months or years before the attacks are discovered, which may result in serious and extensive damage for the organisations affected. It is also difficult to prevent attacks permanently. On several occasions, the AIVD observed that, after detection and removal of the initial malware, attackers quickly managed to penetrate the same target network in another way.²⁷² Although an increasing number of organisations have special software to protect them against APTs, it appears that the prevention of such attacks is

mostly unexplored territory for many organisations. The many reports on APTs that were published²⁷³ in the previous period may, however, help to gain more insight into the effect of APTs and thereby to determine measures.

Security of open source software comes at a price

The Heartbleed vulnerability²⁷⁴ showed that open source software is not automatically safer, even if it is used frequently. The OpenSSL library contained a bug that was only discovered after several years. The publicity surrounding this bug resulted in large internet companies joining forces in April 2014 in the Core Infrastructure Initiative. The initiative invests in the open source basic infrastructure of the internet and makes funds available in order to support open source software projects, such as OpenSSL. OpenSSH and NTP are now also supported. This initiative improves the basic security of the internet. However, it currently only covers a small part of the open source projects responsible for the infrastructure of the internet. Fewer funds are available for other projects.

²⁶⁸ Analysis on the basis of data from <http://rick.eng.br/dnssecstat/> and <https://www.verisigninc.com/assets/domain-name-report-march2015.pdf>.

²⁶⁹ See for example: <http://www.heise.de/tp/artikel/2/2898/1.html>.

²⁷⁰ <http://www.theguardian.com/commentisfree/2015/jan/13/cameron-ban-encryption-digital-britain-online-shopping-banking-messaging-terror>

²⁷¹ See for example: <http://dspace.mit.edu/handle/1721.1/97690>.

²⁷² <https://www.aivd.nl/@3247/jaarverslag-aivd/>

²⁷³ See for instance APTnotes, a public list of APT reports: <https://github.com/kbandla/APTnotes>.

²⁷⁴ See Chapter 4 Resilience: vulnerabilities.

Responsible disclosure

The number of organisations in the Netherlands pursuing a responsible disclosure (RD) policy is still growing.²⁷⁵ Within and outside the critical infrastructure sectors, many individual and collaborating parties have been working on preparing their own RD policy. Moreover, websites have been launched and discussion sessions organised in order to promote RD. In 2014, 120 useful reports were received by the responsible disclosure reporting centres of telecommunications companies, compared to 77 reports in 2013. In the past period, the NCSC handled over 150 RD reports. See also the paragraph on Responsible Disclosure in Appendix 1.

Ethical hackers sometimes have concerns about RD, as they believe that prosecution should not be possible. The increasing number of reports nevertheless indicates a growing trust between the wider IT community, the government and the business sector.²⁷⁶ In the past period, the Public Prosecution Service did not prosecute reporters who acted in accordance with the RD policy of the relevant organisations.²⁷⁷

Cooperation

The Netherlands has many cooperative arrangements with the aim of strengthening digital resilience. This paragraph explains some of these initiatives.

Malware fraud is reduced successfully

Despite the continued strong growth of internet banking, the damage caused by malware to Dutch banks decreased by 90 percent to less than 500,000 euros.²⁷⁸ Interbank detection systems (such as the Cybercrime Monitoring & Investigation Services) can increasingly and automatically detect and prevent malware fraud. Dutch banks are probably successful because they do not compete on security.²⁷⁹ According to the Dutch Payments Association and the Dutch Banking Association, good cooperation is the key to keeping payment transactions safe.²⁸⁰

Fight against botnets: takedown and sharing data

In June 2014, the FBI, Europol, various commercial security and other companies and researchers of the VU University Amsterdam

Skimming is virtually non-existent

The skimming of debit cards was significantly reduced in 2014. The damage caused by skimming decreased by 82 percent to less than 1.3 million euros in 2014.²⁸⁰ Skimming is no longer attractive to fraudsters since the introduction of the EMV payment chip on all debit cards, the geoblocking of PIN payments outside Europe and the implementation of additional anti-skimming measures at unmanned point-of-sale terminals and ATMs. The last time a person was skimmed in the Netherlands at a manned point-of-sale terminal was in 2012. The last time a person was skimmed at a Dutch ATM was in late 2013.²⁸⁰

took down the notorious GameOver Zeus botnet.²⁸¹ This Operation Tovar was given a lot of publicity and resulted in the arrest of various persons. One month later, the UK National Crime Agency and Europol reported on the takedown of the Shylock botnet.²⁸² Although botnet takedowns attract a lot of media attention, they are quickly followed by reports questioning their success. Soon after the GameOver Zeus botnet was taken down, an amended form of the botnet became active. Moreover, there are various botnets (some of whom are derived from Zeus) that fill the vacuum left by GameOver Zeus. Although taking down individual botnets continues to be necessary, it remains to be seen whether this approach helps to solve the overall botnet problem.

The Abuse Information Exchange Association is an initiative of KPN, SIDN, Solcon, Tele2, UPC, XS4ALL, Zeelandnet and Ziggo. The association represents more than 90 percent of the market of Dutch internet providers and aims to improve the provision of information about botnets and other forms of internet abuse in the Netherlands. They compile and correlate data on infections from different sources to one central point. As a result, botnet infections can be countered more quickly and more effectively, improving the safety and stability of the internet. This system, AbuseHUB, was officially launched in June 2014.²⁸³

Sharing threat information will help to deploy capacity efficiently

The need for solutions in the area of monitoring is increasing. A continuous monitoring of the systems and applications in the

²⁷⁵ Letter to Parliament on the progress of responsible disclosure, <http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/12/19/tk-voortgang-responsible-disclosure.html>.

²⁷⁶ <https://www.ncsc.nl/actueel/nieuwsberichten/responsible-disclosure-steeds-breder-toegepast.html>

²⁷⁷ <http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2014/12/19/tk-voortgang-responsible-disclosure.html>

²⁷⁸ <http://www.betalvereniging.nl/wp-uploads/2015/03/150318-Fraude-betalingsverkeer-gehalveerd-20141.pdf>

²⁷⁹ <http://fd.nl/economie-politiek/1102338/aanpak-cybercrime-bij-banken-wordt-exportproduct>

²⁸⁰ <http://www.betalvereniging.nl/nieuws/fraude-met-internetbankieren-gehalveerd>

²⁸¹ <https://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted>

²⁸² <https://kcdp.ncsc.nl/Global%20action%20targeting%20Shylock%20malware.pdf>

²⁸³ <https://www.abuseinformationexchange.nl/>

'Nederland Schoon' project

The Netherlands is not only a direct target, but also a large transit port for digital attacks.²⁸⁴ The Netherlands is known worldwide for being an important hosting country of digital data, among other things due to its stable networks, high bandwidths and relatively low costs. The presence of one of the largest internet hubs in the world and a professional and adult hosting sector also contribute to this reputation. These circumstances attract activities from all over the world. Most of these are bona fide activities, but unfortunately sometimes also less bona fide activities. As a result the Netherlands relatively frequently forms a base for various forms of cyber crime, such as the spreading of malware, the dispatch of phishing and spam messages and the storage of stolen data.

In order to take responsibility nationally and internationally as a hosting country, the police, the Netherlands Authority for Consumers & Markets, the Public Prosecution Service and the Delft University of Technology launched the 'Nederland Schoon' (Clean Netherlands) project in 2014. The purpose of this project is to fight cyber crime from those infrastructures in close cooperation with the sector itself. In the coming period, 'Nederland Schoon' will conduct various campaigns.

In cooperation with the Delft University of Technology, information was gathered about the hosting providers that are used by cyber criminals. Many hosting companies are making good progress in preventing cyber crime. Some hosting providers play a facilitating role in cyber crime. Hosting companies may be unaware of their facilitating role. That is why the project forms a basis for engaging into talks with hosting providers who, according to the measurement conducted by the Delft University of Technology, obtained higher scores than other companies in their sector.

network allows for an early detection of threats and a quick response in case of an actual event, thereby limiting the damage. Monitoring is, however, labour-intensive and cost-intensive. It is not feasible for every organisation to deploy staff 24 hours a day and 7 days a week for this purpose.²⁸⁵ Sharing threat information will allow organisations to gain a more complete picture of (potential) threats

with less effort and to respond to such threats. The STIX²⁸⁶ and TAXII²⁸⁷ standards, for example, are available for this purpose.

An example of cooperation for the sharing of threat information is the National Detection Network (NDN). The NDN is a Dutch public-private network aimed at a better and faster detection of digital threats and risks. By sharing threat information, parties can take appropriate measures in good time as part of their own responsibility, to limit or to prevent possible damage.²⁸⁸

Exercises help in preparing for a response

Various national and international exercises were held in the past period. On 28 April 2014, more than 200 organisations and 400 cyber security professionals from all over Europe, including the Netherlands, participated in ENISA's Cyber Europe exercise.²⁸⁹ CyberDawn, aimed at cooperation between telecommunications companies, critical infrastructure sectors and the government in case of large digital attacks,²⁹⁰ took place in October 2014. By participating in such exercises, staff members and organisations learn what they should and can do in case of any (impending) incidents.

Regulation

The Data Breaches (Duty to Report) Bill was adopted unanimously by the Dutch House of Representatives on 10 February 2015.²⁹¹

The purpose of the proposed duty to report data breaches is to prevent any security breaches and, should any breaches occur, limit the consequences for those involved as much as possible.²⁹²

In case of a breach which can reasonably be assumed to result in a considerable risk of loss or unlawful processing of personal data, the controller (both in the private and public sector) must report this to the supervisor, the Dutch Data Protection Authority and the data subject. The failure to report a data breach may be subject to an administrative penalty.

In the past period, attention was paid in various ways to the use of norms, standards, guidelines and good practices used by organisations to increase resilience. Research conducted by ISACA shows that many organisations have an extensive cyber security policy in place, using norms and standards, but that these policies do not always provide adequate cover due to the rapidly evolving threat landscape.²⁹³ Managers have a key role to play, because they

284 <https://www.aivd.nl/@3247/jaarverslag-aivd/>

285 Capgemini, Report titled 'Trends in Veiligheid 2014', <http://www.trendsineveiligheid.nl/publicaties2014>.

286 <https://stix.mitre.org/>

287 <https://taxii.mitre.org/>

288 <https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/het-nationaal-detectie-netwerk.html>

289 <https://www.enisa.europa.eu/media/press-releases/biggest-eu-cyber-security-exercise-to-date-cyber-europe-2014-taking-place-today>

290 <http://www.nederlandict.nl/index.shtml?id=13663&ch=ICT>

291 http://www.eerstekamer.nl/wetsvoorstel/33662_meldplicht_datalekken_en

292 http://www.eerstekamer.nl/behandeling/20130617/memorie_van_toelichting_4/document3/f=/vjc76lpxgryk.pdf

293 <https://isaca.nl/dmdocuments/ISACA-survey2014.pdf>

Abolition of the obligation to retain telecommunications data

Apart from the new acts that are being prepared, an act was also rendered inoperative in the Netherlands in the past period: the Telecommunications Data (Retention Obligation) Act. This Act was introduced in 2009 and was based on the EU Data Retention Directive. The purpose of this Act was to ensure that telecommunications data that could be important for the investigation and prosecution of criminal offences were retained for a specified period of time and were thus available for the purpose of investigating serious crimes.²⁹⁴

On 8 April 2014, the European Court of Justice declared this directive invalid with retroactive effect. The court considered that the directive violated the privacy and right to protection of personal data of EU citizens too much. Shortly after the judgment, several interest groups demanded in preliminary relief proceedings that the Dutch Telecommunications Data (Retention Obligation) Act be abolished as well. In the judgment in preliminary relief proceedings on 11 March 2015, the court decided in favour of the interest groups.²⁹⁵

The Public Prosecution Service and the police used the historical traffic data on mobile and fixed-line telephony and internet use for the investigation and prosecution of traditional forms of crime (such as murder, violent house robberies, rape and human trafficking) as well as for cyber-related crime (such as hacking systems, carrying out DDoS attacks, downloading child pornography or online grooming of children). The AIVD and MIVD also used stored telecommunications data for their investigations. A report by the police and the Public Prosecution Service underlines the importance of the retention obligation for the investigation and prosecution of cyber-related crime; in such cases, user and traffic data are often the only evidence available to the investigative services.²⁹⁶ Moreover, the Netherlands is an important internet hub for a lot of international internet traffic. According to the Public Prosecution Service, a limitation or abolition of the retention obligation will make it difficult to meet international obligations to comply with foreign requests for information about IP addresses.

The Ministry of Security and Justice is working on a bill to replace the abolished Act.

continuously have to determine the frameworks for the formulation, implementation, monitoring and enforcement of the

cyber security policy at a strategic level. The Cyber Security Council has drawn up a guide for managers in order to support them in this.²⁹⁷

The Internet Standards Platform, a partnership between parties from the internet community and the Dutch government, aims to stimulate the use of modern internet standards (such as IPv6, DNSSEC, TLS, DKIM, SPF and DMARC), making the internet more reliable for everyone.²⁹⁸ In April 2015, the platform launched the website internet.nl.²⁹⁹ On this website, visitors can easily check if their internet connection, their e-mail and the websites they visit use modern, safe internet standards.

Conclusion and looking ahead

The government and the business sector make large investments in the protection of interests and strengthening of the digital resilience of individuals, organisations and society. The resilience initiatives described in this chapter are not the only ones that are taken in the Netherlands. Attention is paid to the human factor (with the necessity of conscious and competent users on the one hand and of professionals on the other hand), to technological means and to cooperation with others for the purpose of better addressing any challenges.

There are few figures and statistics available on the measures taken by organisations. Understandably, organisations are cautious when it comes to sharing information about their measures, because actors may benefit from this information. It is therefore difficult to provide an overall picture of the measures taken. This makes it difficult to give an estimation of the current resilience level.

Investing in measures and cooperation absolutely pays off, but is not yet effective in all cases. It appears that, for certain threats, such as botnets and APTs, the right measures are yet to be found. Organisations must be aware of the fact that their cyber security policies do not always provide adequate cover due to the rapidly evolving threat landscape. It is therefore important that they regularly review their policies and measures. As attacks become more advanced and are increasingly difficult to detect, awareness continues to be important. Monitoring, detection and response are also essential, not in the least because actors are continuously looking for ways to bypass existing security measures.

²⁹⁴ WODC (2013) The Telecommunications Data (Retention Obligation) Act, consulted via: <https://www.wodc.nl/onderzoeksdatabase/evaluatie-wet-be-waarplicht-telecommunicatiegegevens.aspx>.

²⁹⁵ <https://www.rechtspraak.nl/Actualiteiten/Nieuws/Pages/Wet-bewaarplicht-telecommunicatiegegevens-buiten-werking-gesteld.aspx>

²⁹⁶ Public Prosecution Service and Police (2014) The obligation to retain telecommunications data and investigations - The importance of historical telecommunications data for the investigative services, consulted via: <http://www.rijksoverheid.nl/documenten-en-publicaties/rapporten/2015/04/01/tk-bijlage-de-bewaarplicht-telecomgegevens-en-de-opsporing.html>.

²⁹⁷ http://www.nederlandict.nl/Files/ICT/Handreiking_cyber_security_voor_de_bestuurder.pdf

²⁹⁸ <https://www.internet.nl/about/>

²⁹⁹ <https://www.forumstandaardisatie.nl/actueel/item/titel/lancering-internetnl-tijdens-cyber-week-2015/>

The interests protected by the critical infrastructure sectors remain large and show little change.



6 Interests

In a changing world, the consequences of cyber security breaches change as well. Reports on incidents cause users to be less inclined to embrace new and existing services. At the same time, IT systems in new appliances, such as in cars or medical equipment, also appear to be vulnerable for methods of attack that apply to traditional IT systems. The increased use of IT often goes hand in hand with the disappearance of analogue alternatives. As a result, IT systems become increasingly important. Within these shifts, the interests of the critical infrastructure remain large, but show little change.

Cyber security breaches harm individual, organisational and public interests. Changes in society may result in these breaches having more serious or less serious consequences. This chapter describes relevant developments in these interests.

Less trust in digital services curbs economic activities

Many people noticeably have less faith in digital services due to reports on the reliability of IT systems. Reports on data breaches, IT failures and Snowden's revelations cause people to become more cautious when using these systems.

In the past year, for instance, one quarter of the Dutch population indicated that they make less use of internet banking, make fewer online purchases and use fewer apps on their telephone.³⁰⁰ When people make less use of digital services, this may curb economic growth. Other services, such as social media, were also used less. The impact of less trust on the use of social media was, however, smaller. The most important reasons for such caution were inadequate privacy safeguards, inadequate security and insufficient availability of services.

Concerns about privacy are an important motivation for users to better protect themselves. Mobile messaging service providers responded to this by offering end-to-end encryption. The use of this encryption ensures that service providers cannot read the contents of the messages. A well-known example is the end-to-end encryption in the Android version of the WhatsApp messaging service.³⁰¹

New areas of application result in vulnerabilities and debate

IT is used in new ways, as a result of which security breaches may have new consequences. If, for example, a refrigerator has software and is connected to a network, a malware infection may have consequences for food safety. An attacker could increase the temperature of the refrigerator from a distance, causing the food to go bad. Such risks may also arise if the software used contains bugs, a licence expires or a network service is no longer available. Security often has no priority in the development of this type of new applications.

³⁰⁰ <http://publications.tno.nl/publication/34611864/kSscvS/TNO-2014-R11119.pdf>

³⁰¹ See also: <http://www.nrcq.nl/2014/11/18/whatsapp-gaat-versleuteling-aanbieden-in-een-volgende-update>.

Digitised mobility requires separated networks

More IT is installed in cars, aircraft and other means of conveyance. This requires attention for the security of this IT. For a security problem in an entertainment system on board should not affect the operation of the vehicle. A lack of security may then even have fatal consequences.

Developments in the security of this 'digitised mobility' primarily focus on separating networks. For cars as well as aircraft, attention was paid to the risks associated with linking internal IT systems with different security levels.

In aviation, passengers are more and more often allowed to use their own devices during flights. Several carriers already offer wireless internet facilities to their passengers. Of course, these networks must remain separate from the aircraft control system. A researcher who twittered on an alleged link between these systems was banned from his flight by United Airlines.³⁰² The American Government Accountability Office considered such an attack to be very unlikely.³⁰³ This will, however, strongly depend on the measures taken.

New cars contain all kinds of IT systems, varying from an internal entertainment system to possibilities for the manufacturer to open the car from a distance. These systems often hardly have anything to do with the car's control. If, however, these systems are not separated from the car control systems, attackers may use a vulnerability in such an IT system to influence the car's control, causing an accident, for example. As early as in 2011, researchers managed to exploit such vulnerabilities and influence a car's control from a distance.³⁰⁴

The development of autonomous cars will undoubtedly raise more security issues in the future. In an autonomous car, it is an IT system that drives the car. This is expected to be an important subject of discussion in the coming years.

Medical devices are also computers now, giving rise to comparable threats

Due to IT systems in the medical sector, everyday vulnerabilities may have consequences for patients' health. More and more medical devices can be administered from a distance, for instance via WIFI or bluetooth. If an attacker manages to take over this administration, he may harm the patients involved. If it concerns a device maintaining vital bodily functions, this may have fatal consequences.

Research conducted by Deloitte into the security of medical equipment in Dutch hospitals showed that a majority of the interviewed institutions had experiences with malware infections in their medical equipment.³⁰⁵ This is an indication of the complexity and vulnerability of such devices. As they have become fully-equipped computers, they are confronted with the same risks as traditional systems.

Analogue alternatives disappear

If IT systems for the support of social processes are not available, it is, in a growing number of cases, no longer possible to rely on analogue alternatives. The availability of these IT systems thus becomes more important: failure is no option. At the same time, the underlying technology is more complex than with analogue systems. Moreover, these systems can be attacked more easily if they can be accessed via the internet.

In case of a failure of an IT system supporting a social process, society will have to rely on analogue alternatives. If no analogue alternatives are available, such failure will have serious consequences. In case of a failure of internet banking services, the consequences will be more serious if customers cannot go to a bank office.

At the same time, IT systems are more complex than their analogue alternatives. This makes them more susceptible to failure. Their infrastructure is geographically spread, often even worldwide. Many organisations do not know which IT systems are crucial to them. Moreover, the complexity of hardware and software makes it impossible to predict the behaviour of a system in all cases.

Example: the government wants digital contact with citizens

The government wants citizens and businesses to arrange more and more affairs digitally. This is set out in the 2017 Digital Government Vision Plan.³⁰⁶

Government authorities want to provide certain services in digital form only. In recent years, a number of municipalities decided to publish official announcements in digital form only.³⁰⁷ The Tax and Customs Administration makes it mandatory for businesses to file a digital return for certain taxes.³⁰⁸ In July 2014, the municipality of Tilburg announced that social assistance benefits can, from that date onwards, only be applied for digitally.³⁰⁹ Research conducted in Amsterdam showed, however, that citizens do not want their contact with the government to be digital in all cases.³¹⁰

³⁰² <https://nakedsecurity.sophos.com/2015/04/20/security-researcher-barred-from-united-airlines-flight-after-hack-tweet/>

³⁰³ <http://www.gao.gov/products/GAO-15-370>

³⁰⁴ <http://www.nytimes.com/2011/03/10/business/10hack.html>

³⁰⁵ <http://www2.deloitte.com/nl/nl/pages/over-deloitte/articles/cyber-security-medische-apparatuur-beeld.html>

³⁰⁶ See also: <http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2013/05/23/visiebrief-digitale-overheid-2017.html>.

³⁰⁷ Bijvoorbeeld: <http://www.nrc.nl/handelsblad/van/2015/januari/02/gemeente-bekendmakingen-alleen-nog-maar-digitaal-1446984>.

³⁰⁸ http://www.belastingdienst.nl/wps/wcm/connect/bldcontentnl/belastingdienst/zakelijk/aangifte_betalen_en_toezicht/aangifte_doen/

³⁰⁹ <http://www.tilburg.nl/actueel/nieuws/item/nieuwe-werkwijze-aanvraag-uitkering/>

³¹⁰ <https://www.utwente.nl/nieuwsevents/!2015/1/346014/digitaal-vaardige-burgers-willen-niet-altijd-digitaal>

Example: the payment system offers increasingly fewer analogue alternatives

In the past few years, the payment system has shifted from cash and paper-based transactions to digital systems. There are only few offline banking options available for consumers, for which they often have to incur additional costs.³¹¹

Cash payments become increasingly less common. Many vending machines, but also some shops, no longer allow cash payments. If the system for card payments is unavailable, it is still possible to pay in these shops using a single direct debit mandate.³¹² This is, however, not possible for vending machines.

Although banking using analogue means is only possible to a limited extent, banks and other providers increasingly offer digital alternatives. Most banks offer, for example, their own app in addition to internet banking. If one channel cannot be accessed, the other channel is sometimes still available.³¹³ The availability of the payment system also benefits from the popularity of alternative payment services such as PayPal.

Interests of critical infrastructure are large but stable

The interests protected by the critical infrastructure³¹⁴ sectors remain large and show little change. This is evident from meetings with representatives of organisations in those sectors, as well as other partners of the NCSC. Although the security of information and systems creates new challenges each time, the underlying reasons for security have hardly changed. Three examples from these sectoral analyses are briefly discussed below.

The energy sector is responsible for a reliable and undisturbed power supply. Some developments change the nature of the threat and measures to be taken. An example is the introduction of smart meters. Ultimately, however, this development, too, serves the same purpose.

The Dutch goods transport sector serves the economic interests of the Netherlands as a key party in the distribution of goods. Disruptions may harm these interests, as goods will then have to be transported via other countries. Long-term disruptions also affect society at a deeper level: food supply largely depends on this sector.

IP technology is used in disaster and crisis communication

Crisis communication systems are digitised as well, which increases manageability and functionality. At the same time, the availability of the technology used is a concern in terms of conversion.

The Emergency Communication Facility [Noodcommunicatie-voorziening, NCV] uses IP technology for communication between affiliated parties.³¹⁵ The NCV is the network for communication between critical infrastructure organisations in case of a crisis. The NCV provides for communication via fixed-line and mobile telephony and data connections. In 2010, the NCV succeeded its predecessor, the National Emergency Network [National Noodnet].³¹⁶ The design of the NCV is such that it will still be available if regular telephone communications are no longer possible during a disaster.

The telecommunications sector plays a facilitating role for other critical infrastructure sectors. Electronic communications networks are used, for example, for the automated management of process control systems. In order to communicate with citizens, systems such as the 112 emergency service and NL-Alert depend on a proper functioning of electronic communications networks.

Conclusion and looking ahead

The reliability of software becomes more important as IT systems are used in more devices. Mobility and medical equipment are examples of this. The impact of a breach may be much more serious for these applications, as the systems have a direct influence on people's physical environment. Such breaches are certainly not imaginary, as priority is not always given to digital security. This situation is not expected to change without external stimuli, such as an incident or regulation.

The party responsible for a social process also monitors the availability of the underlying IT systems, thereby considering the possible impact of an IT failure on society.

The interests of the critical infrastructure will remain the same in the coming years. The experience gained by the organisations in these sectors increasingly enables them to guarantee these interests.

³¹¹ <http://www.consumentenbond.nl/betaalrekening/Extra/bankieren-zonder-internet/>

³¹² http://www.betalvereniging.nl/wp-uploads/2014/05/Betaalwijzer_mei_2014.pdf

³¹³ For example: <https://tweakers.net/nieuws/102469/internetbankieren-ing-kampt-met-storing.html>.

³¹⁴ A reassessment of the vital infrastructure in the Netherlands was performed during the reporting period of the CSAN. The most current list can be found at: <http://www.nctv.nl/actueel/nieuws/kabinet-versterkt-crisisbeheersing.aspx?cp=126&cs=60005>

³¹⁵ <http://www.telecompaper.com/nieuws/kpn-levert-ipnetwerk-voor-noodcommunicatie-overheden--703707>

³¹⁶ See also: <http://www.rijksoverheid.nl/nieuws/2009/11/18/nieuw-noodcommunicatienetwerk-voor-bestuurlijk-nederland-en-vitale-organisaties-bij-ramp-of-crisis.html>.

Appendices

Appendix 1 NCSC statistics

This appendix offers a summary of the responsible disclosures, security advisories and incidents that have been handled by the NCSC.

The NCSC facilitates the making of responsible disclosure reports for both its own infrastructure and that of the Central Government and several private parties. It issues security advisories for its participants and deals with cyber security incidents. Relevant statistics for the current reporting period have been calculated and are presented below. By comparing these statistics with earlier reporting periods, it is possible to identify trends and other developments.

Responsible disclosure

In 2013, the NCSC published a guideline for disclosure responsible³¹⁷ as well as a responsible disclosure policy³¹⁸ for its own website. In 2015, the NCSC and its partners published a best practice guide³¹⁹ to share experiences in this area, helping other organisations with implementing or improving their own responsible disclosure policy. With these publications, the NCSC contributed to a responsible reporting and handling of vulnerabilities in information systems and software and other products. It is partly due to these publications that the NCSC became more visible and was contacted by more reporters, resulting in a considerably higher number of reports during this period. Moreover, some reporters (20 percent of the total) made several reports during this period, which suggests that their experiences were positive and the interaction with the NCSC was useful.

During the reporting period, the NCSC received over 150 reports. These concerned reports for its own systems as well as for other government systems and systems of private parties. In some cases, double reports were filed, for example if two or more researchers reported the same vulnerability. As a result, the total number of reports is not representative of the total number of vulnerabilities.

In 20 percent of all reports, further research showed that there was no vulnerability. These cases were classified as false positives.

Figure 10 shows the different types of reports, including the above-mentioned false positives. Slightly less than half (49 percent) of all reports concerned a vulnerability in a website, a web application or infrastructure for web applications. Examples of such reports are Cross-Site Scripting (XSS) or SQL injection. About one sixth (17 percent) of all reports had to do with an error in the configuration of a software product, such as a web server. Examples of such reports are the support of an outdated TLS version or the lack of certain http headers. Only 5 percent of all reports had to do with vulnerabilities in software (excluding web servers or applications). An example of this is a vulnerability in a smartphone application. Finally, 9 percent of all reports concerned other vulnerabilities not belonging to one of the above-mentioned types. Examples of such reports are a vulnerability in a hardware product of a private party or the possibility to retrieve sensitive data by using a commercial service.

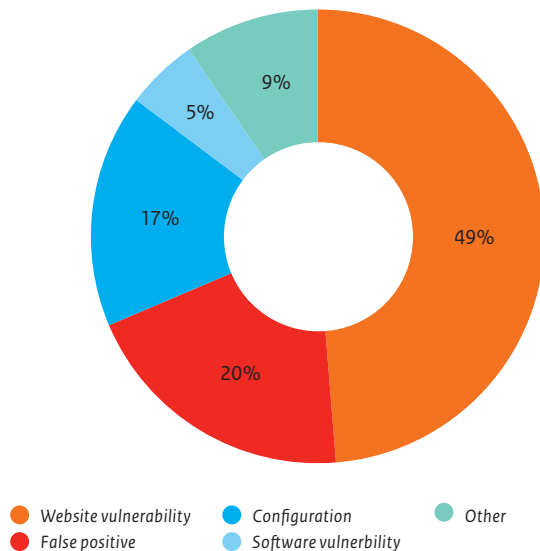
Compared with the previous reporting period, around 50 percent more reports were made in the current reporting period. The total number of reports on website vulnerabilities was around as high in the current reporting period as during the previous reporting period. Their share in the total decreased, however, by 25 percentage points. In the previous period, this was 76 percent of 95 reports, compared to 51 percent of 156 reports during this period. This probably has to do with a substantial increase in false positives and other reports.

³¹⁷ <https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsible-disclosure.html>

³¹⁸ <https://www.ncsc.nl/security>

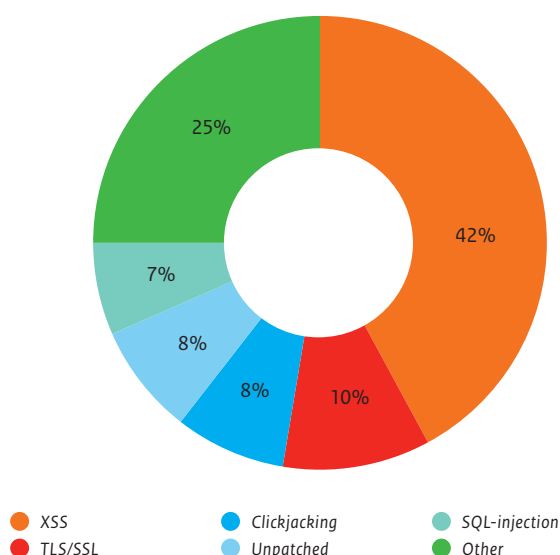
³¹⁹ <https://www.ncsc.nl/actueel/nieuwsberichten/ncsc-presenteert-best-practice-guide-responsible-disclosure-in-aanloop-naar-de-global-conference-on-cyberspace.html>

Figure 10 Types of responsible disclosure reports



Since the great majority of the reports under the scope of responsible disclosure relate to vulnerabilities in websites, this type of vulnerability is analysed in more detail in figure 11. This figure shows that many vulnerabilities (42 percent) have to do with XSS. In the previous period, XSS covered around 50 percent of all website vulnerabilities. The decrease probably has to do with a substantial increase in the number of other website vulnerabilities. Examples of such vulnerabilities are vulnerable authentication mechanisms or sensitive information that can be found via public search engines. 'Other' reports include, for example, intranet pages that can be accessed via the internet and vulnerable authentication mechanisms.

Figure 11 Reported website vulnerabilities



Security advisories

The NCSC publishes security advisories in connection with software vulnerabilities or perceived threats. A security advisory describes the problem, the systems that may be affected and what needs to be done in order to prevent an organisation from becoming a victim. Figure 12 shows the number of advisories that the NCSC published per quarter between the second quarter of 2003 and the first quarter of 2015. Here, a distinction is made between new advisories (with version number 1.00) and updates of existing advisories.

The NCSC security advisories are classified based on two elements. Firstly, based on the chance that the vulnerability will be abused. Secondly, based on the damage that occurs when the vulnerability is abused. So the classification comprises two criteria: chance and damage. A level is estimated for both criteria on the basis of several different aspects: High (H), Medium (M) or Low (L). If there is a high chance, for example, that a particular vulnerability will be abused, but the expected damage caused by the abuse is low, the corresponding security advisory will be classified as H/L. Figure 13 shows the ratios between these levels of all advisories published during the reporting period.

Damage caused by vulnerabilities in software

Every security advisory comes with a description of the possible damage that malicious parties could cause if the advisory is not followed. In order to gain an overview of this damage, advisories are categorised on the basis of a standard list of damage descriptions. For the reporting period, the percentage of advisories per damage description is shown in table 4. This clearly shows that most security advisories (51 percent) had to do with Denial-of-Service (DoS), followed by remote code execution with user rights

Table 4 Percentage of security advisories per damage description

Damage description	%
Denial-of-Service (DoS)	51%
Remote code execution (User rights)	29%
Access to sensitive data	26%
Bypassing security measures	19%
Increased user rights	14%
Access to system data	9%
Cross-Site Scripting (XSS)	6%
Manipulation of data	5%
Bypassing authentication	4%
Remote code execution (Administrator/root rights)	4%
Spoofing	2%
Cross-Site Request Forgery (XSRF)	1%
SQL injection	1%

Figure 12 Number of advisories per quarter (2003Q2 - 2015Q1)

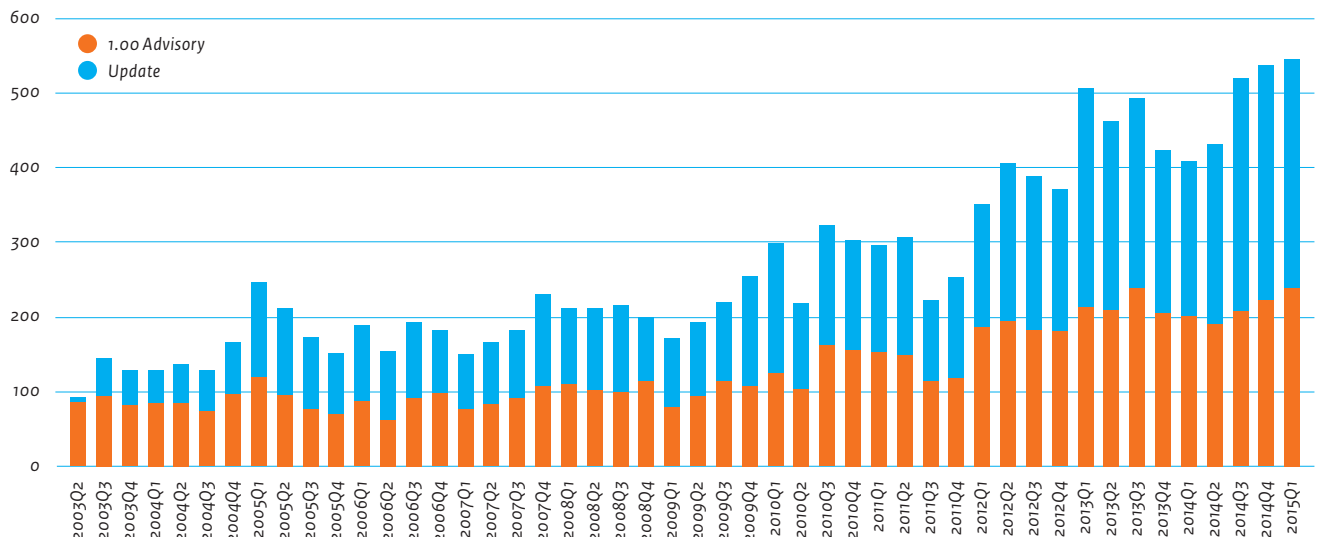
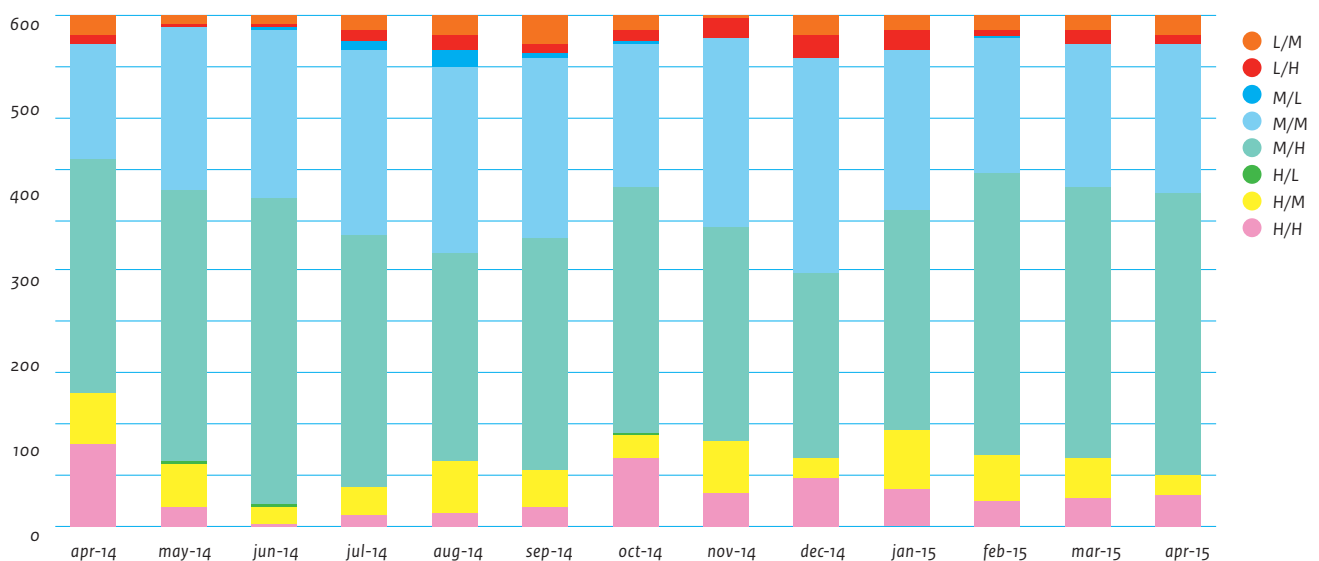


Figure 13 Classification of advisories during the reporting period



(29 percent), access to sensitive data (26 percent) and bypassing security measures (19 percent). An advisory often comes with several damage descriptions.

The NCSC assists governmental departments and organisations in critical infrastructure sectors in handling incidents in the area of IT security. In this role, the NCSC receives reports of incidents and vulnerabilities and also identifies incidents and vulnerabilities itself, for example on the basis of various different detection mechanisms. In addition, the NCSC acts, at the request of national and international parties, as an intermediary towards Dutch internet service providers in order to provide assistance in responding to IT security incidents, the source of which lies in the

Netherlands (for example from a fraudulent web server or from infected PCs in the Netherlands).

Number of incidents handled

The number of incident reports handled by the NCSC during the reporting period is calculated and presented differently than in previous versions of the CSAN. The reason for this is as follows. In the last quarter of 2013, the NCSC automated some of its incident reports, which resulted in a strong increase (around 400 percent) in the number of incidents handled, while the current threat showed little change. In the previous CSAN, these automated controls were added to all other incidents. In this CSAN, they are shown separately.

Figure 14 Incidents handled (excluding automated controls)

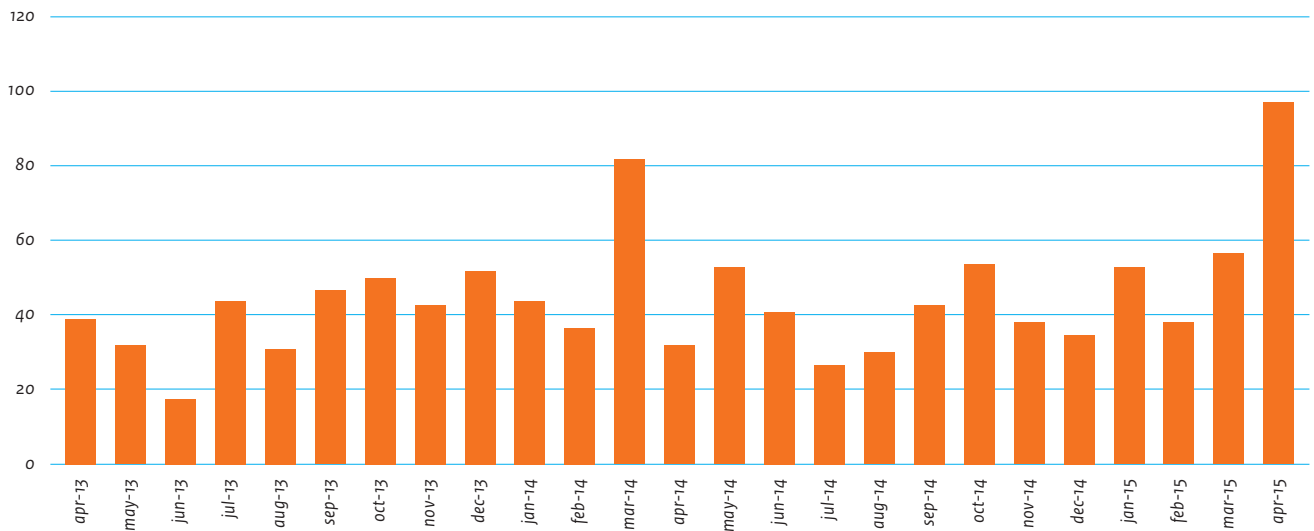


Figure 15 Automated controls

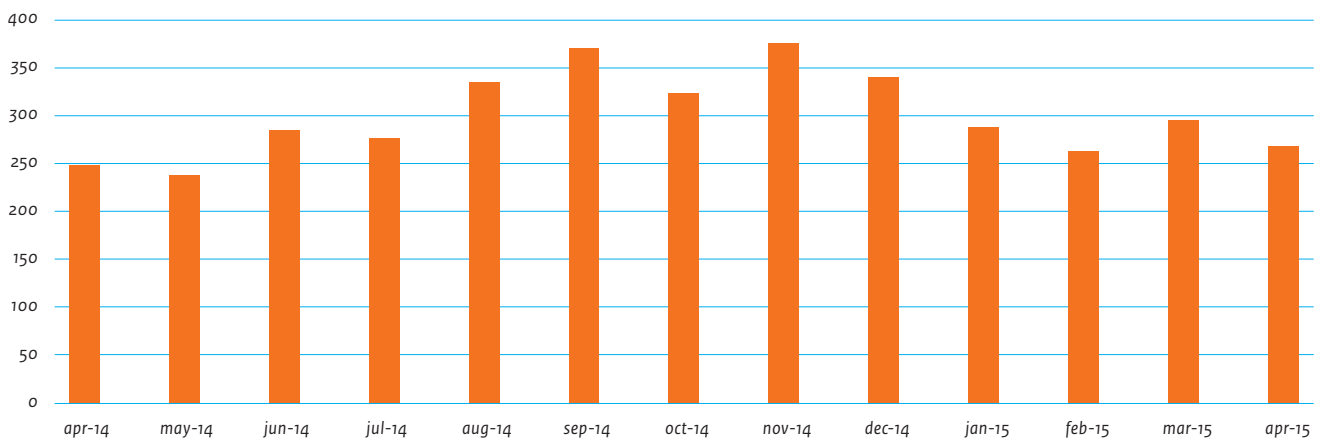


Figure 14 shows the number of incidents handled per month for the period between April 2013 and April 2015. Apart from a few deviations in March 2014 and April 2015, the number of incidents remained relatively stable. The absolute numbers also show this. In the previous reporting period, a total of 519 incidents were reported. In this reporting period, 598 incidents were reported (excluding automated controls). The difference can be partly explained by the fact that the current period is slightly longer than the previous period: 13 months instead of 12.

Figure 15 shows the results of automated controls for the reporting period. This shows that, on average, there are 300 incident reports per month on the basis of this automation. A report may concern several infected systems within an organisation.

Figure 16 shows the incidents handled (excluding automated controls) broken down into tools. In this context, a tool is the type of attack that resulted in the incident. The concept of 'tool' usually does not apply, for example in case of a responsible disclosure report on outdated software. The remaining incidents mainly concern phishing, ransomware and cryptoware and information leakage. If the tool used is phishing, the incident often concerns a notice-and-takedown (NTD) request. The totals of this breakdown may differ from the above-mentioned totals, as for some incidents, several tools were used and have therefore been counted more than once.

Figure 17 shows a breakdown of the incidents handled per type. This shows that responsible disclosure reports represent a substantial share (26 percent). The second most common incidents are NTD reports. Most NTD requests are requests from Dutch

Cyber security incidents registered with the NCSC

The NCSC defines an incident as ‘an IT-related security incident that has been reported or discovered and in which there was an immediate threat or damage to IT systems or electronic information, relating to one or more specific organisations, to which the NCSC responded with action for these organisations’. This definition does not cover fully automated reports. This definition implies that an incident may not always have resulted in damage yet, but can be a danger without damage already having been caused. Incidents can be broken down into three types:

- **Attack:** an (attempted) attack has actually taken place, possibly resulting in a breach of security. An attack could involve hacks, malware infections or DDoS attacks.
- **Threat:** there is a malicious intention on the part of an actor to carry out an attack, but this attack has not been carried out yet.
- **Vulnerability:** an IT environment is vulnerable as a result of a software, hardware or system configuration error, for example. A vulnerability may not be the subject of a threat or attack (yet), but it does make abuse possible.

financial institutions to help with tackling phishing attacks. These attacks are aimed at these institutions and are usually carried out from abroad.

Division of incidents between government and critical infrastructure sectors

The NCSC supports both the central government and the critical infrastructure sectors in security incidents. The NCSC also acts as a contact point for international requests for assistance with regard to information security.

Figure 18 shows the structure of the number of incidents handled, broken down into type of organisation concerned. The division between private and public organisations did not vary much during the reporting period. A total of 50 percent of the incidents concerned a public organisation. 40 percent concerned a private organisation. The remaining 10 percent concerned an international request for assistance. The number of international requests for assistance varied more during the reporting period, from 3 percent in April 2014 to 16 percent in April 2015.

Figure 19, figure 20 and figure 21 show the structure of the incidents involving different types of organisations. The type of incidents involving government organisations and private parties does not vary considerably. However, it is clear that private parties relatively frequently ask for support in phishing incidents. This includes, for example, requests for support in blocking a phishing website for a bank. Governments are more often involved in incidents concerning information leakage and injection attacks. This concerns, for example, RD reports of vulnerabilities in websites of government organisations.

Figure 16 Incidents handled by tool

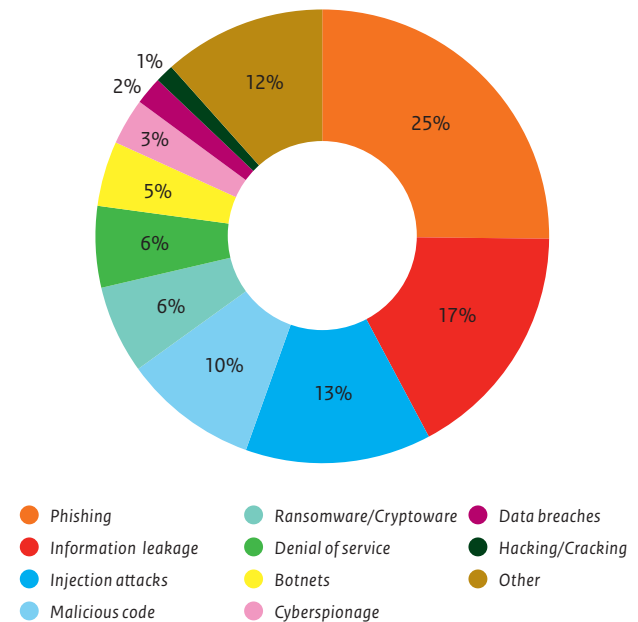
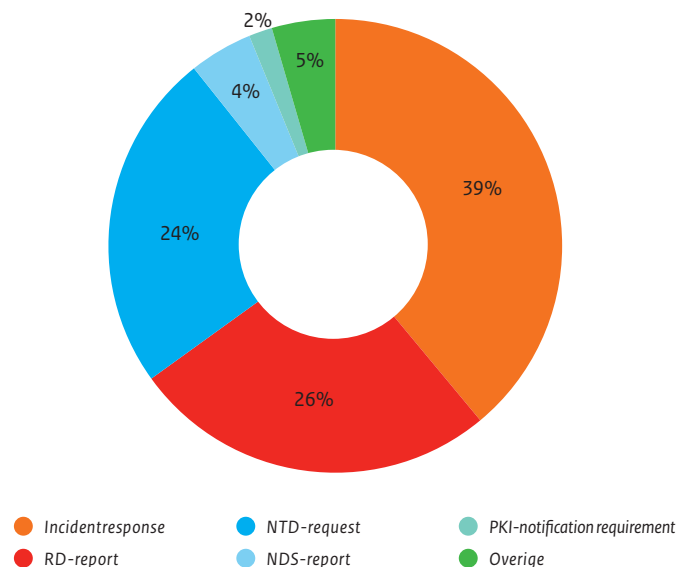


Figure 17 Incidents handled by type



The international requests for assistance have, however, a clearly different structure. Half of the requests involve phishing, often concerning requests to block phishing websites.

Figure 18 Incidents handled per month per type of organisation

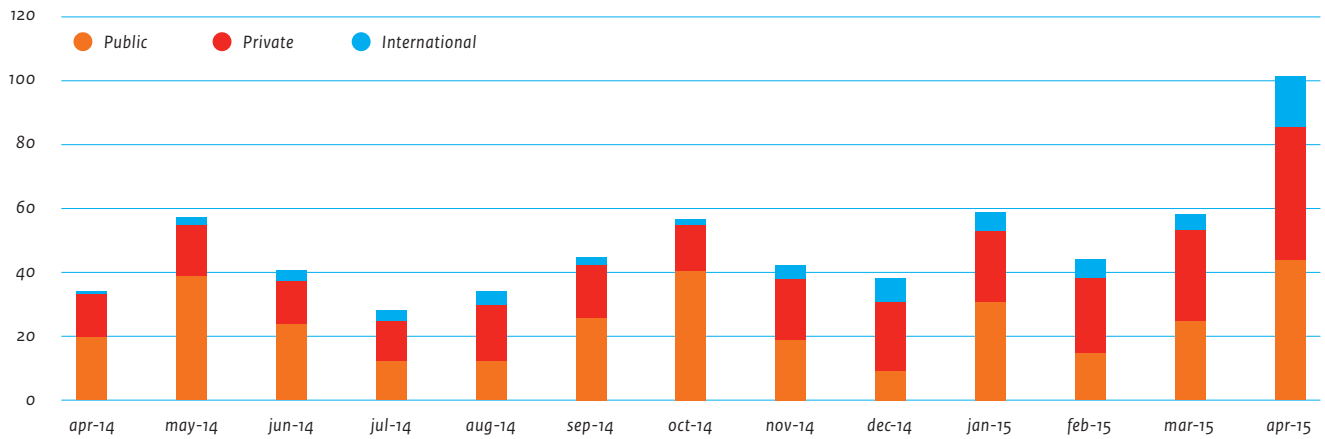


Figure 19 Type of incidents involving a government party

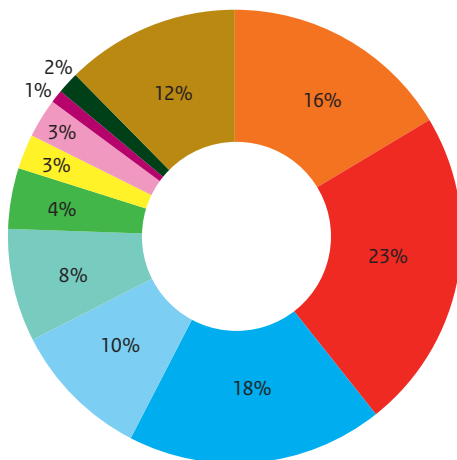


Figure 20 Type of incidents involving a private party

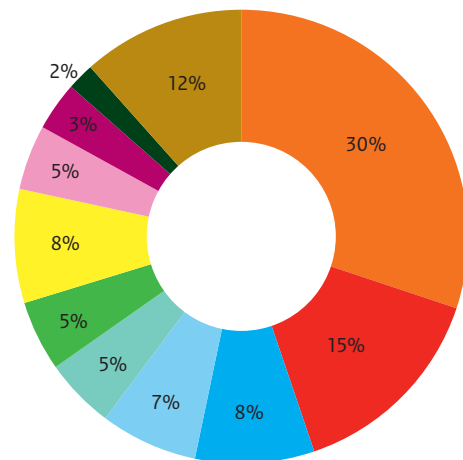
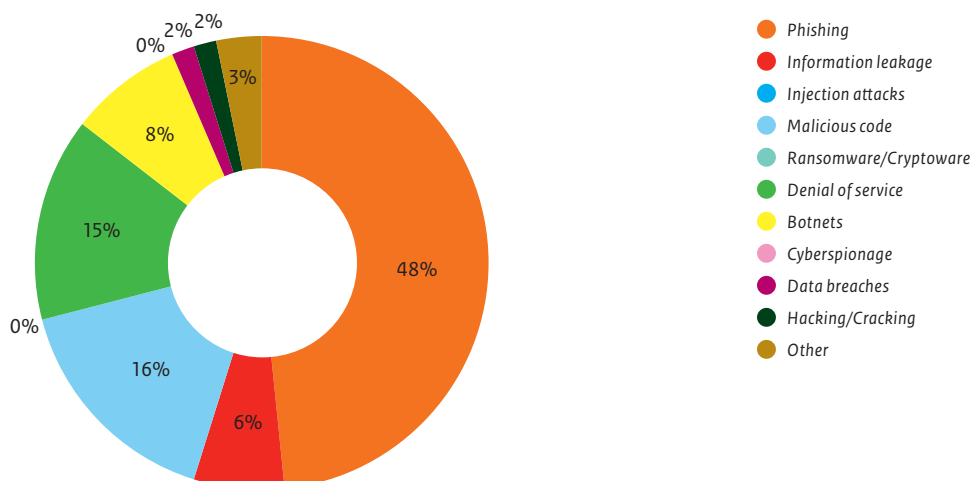


Figure 21 Type of incidents for which the NCSC received an international request for assistance



Appendix 2 Sectoral Assessment

During the preparation of the Cyber Security Assessment Netherlands, meetings were held with representatives of the Dutch critical infrastructure sectors and partner organisations of the

NCSC. These meetings have helped to conduct the analyses included in this CSAN and to substantiate insights. This appendix represents the picture outlined by these representatives during the meetings.

Sector	Manifestations	Threats: actors	Threats: tools
Drinking water supply	No large incidents happened.	The sector does not experience any major threat of certain categories of actors.	Malware and phishing in office IT; malware in process automation.
Energy	No large incidents happened.	The threats specific to this sector are posed by state actors, hacktivists and internal actors. Moreover, the important interests could also be an interesting target for extortion by criminals.	Advanced tools are more accessible to hacktivists. DDoS-as-a-service using booter services is an example of this. Moreover, many (spear) phishing attacks take place.
Financial sector	<p>The number of incidents with identity fraud continues to be high. Offenders do not only focus on persons but also on companies.</p> <p>There have been DDoS attacks during the reporting period, but these attacks were not larger than in 2013.</p>	Criminals still pose the biggest threat to the interests which the sector represents.	<p>Criminals are becoming more professional. What is striking is the quality of phishing e-mails and (in some cases) the focus of phishing. Some attacks only seem to be carried out after months' of 'harvesting' information.</p> <p>The nature of DDoS attacks in the rest of the world is becoming increasingly varied. This trend was not yet visible in Dutch financial institutions during the reporting period.</p>
Managed Service Providers	The power failure in Diemen led to communication failures in both data and voice networks (especially GSM). As a result, the services of service providers throughout the province of North Holland and parts of Flevoland were disrupted. This illustrates the sector's dependence on energy supply.	The biggest threats for this sector are posed by state actors and criminals. The general picture is that the capabilities of terrorists are increasing, which could make them a more relevant threat.	End users of customer organisations are often confronted with cryptoware attacks. Extensive phishing and other social engineering have been detected. The sector is also worried about government authorities concealing zero-day vulnerabilities.

Resilience: vulnerabilities	Resilience: measures	Interests
Many innovative services (not being primary processes, for example reports of failures) use cloud services.	Raising staff awareness; more sector-internal cooperation and cooperation with the NCSC; increased zoning and monitoring in networks for security of SCADA systems.	Drinking water supply is essential for public health and for the functioning of society. Any failure will result in social disruption.
Drastic separation of networks makes the actual energy supply less vulnerable. The surrounding systems which facilitate trade are, however, connected to the internet. Sometimes a monoculture exists as some IT suppliers supply to (almost) all energy companies. Remote access to equipment has advantages for availability, but also creates a basis for attacks.	Incident response is given more attention within the sector. The Netherlands has relatively few statutory requirements for the security of power plants.	Apart from the primary interest of supply, the introduction of smart meters also involves privacy interests.
Banks remain somewhat vulnerable to phishing attacks. Only (very) large and long-term DDoS attacks will cause damage. Mitigation will then be difficult.	Major investments are made in fraud management (such as detection and forensic investigation). The sector has taken effective anti-DDoS measures improving the availability of the payment system. Banks are investigating additional measures should 'all other measures fail', in case of very large attacks. Financial institutions regularly share information about DDoS incidents that have occurred. Financial institutions often check their DDoS mitigation measures.	The monitoring of potential fraud cases is a continuous process for financial institutions. Financial institutions continue to focus on improving the monitoring process. Moreover, the further roll-out of "what you see is what you sign" solutions for signing and authentication purposes has a preventive effect. The availability of financial transactions services is crucial. That is why a lot of attention is paid to
Protection of privacy and the use of encryption make effective monitoring of network traffic more difficult. Attacks are then more difficult to detect.	Cooperation in cyber security is going well. The Netherlands is a unique country when it comes to this. Moreover, more cyber security professionals are trained. A blind trust in the value of security certification is considered to be a risk.	The sector constitutes an important link in many chains. This way, any problems can pose a risk to many social processes in the Netherlands. Examples are healthcare and the payment system.

Sector	Manifestations	Threats: actors	Threats: tools
Nuclear	The manifestations observed are generic (phishing, malware) and do not seem to be aimed at the sector.	State actors and internal actors (displeased staff members) are the most important threats to the sector. Criminals pose a threat to office automation.	Office automation is faced with cryptoware. Moreover, many (spear) phishing and other malware attacks are detected. Specific ICS malware has not yet been detected in the sector.
Central government	The sector is often confronted with cryptoware infections and more serious and more frequent DDoS attacks. Most cryptoware is received via private e-mails sent to staff members. Spearphishing focuses on key positions within the government, for example procurement officers.	The biggest threat for the sector is posed by state actors and criminals. Internal actors are also an obstacle to cyber security. They may be motivated by financial gain, but may also have ideological motives.	'Regular' criminals have easier access to powerful attack tools. Targeted attacks often take place, with information being gathered about a staff member's conduct. This information is used for a swift attack with non-digital consequences.
Telecom	Organisations are often faced with cryptoware infections, mainly through private e-mails sent to staff members. Moreover, spearphishing attacks are carried out against persons in security and management positions.	Sector-specific threats are mainly posed by state actors. Generic attacks by criminals (for example using cryptoware) are detected as well. If users overload the network, this may also constitute a threat to availability.	Attackers often use cryptoware, more than reported by the media. DDoS attacks remain a concern. Moreover, there is still a lot of spam.
Transport (port, airport, rail)	Incidents do take place, but linking the event (for example stolen containers) to a digital attack continues to be difficult. Spearphishing attacks are sometimes highly targeted and advanced. Moreover, several cryptoware infections were detected.	Criminals pose the biggest threat to the sector. By manipulating information, they can smuggle goods or know where to steal valuable goods, for example.	According to the sector, attackers increasingly focus on process control systems. Attackers also carry out cryptoware attacks and (spear) phishing attacks.
Insurers	Targeted attacks against insurers have been detected. Sometimes, insurers are extorted by attackers threatening to publish allegedly stolen client data. Phishing, cryptoware and DDoS attacks continue to take place.	The main threat to the sector is posed by criminals.	Actors use cryptoware, DDoS attack tools, malware and phishing.
Healthcare	There is a clear increase in the number of cryptoware- incidents. Sometimes, even systems not linked to the internet are infected with infected USB sticks. There are also several incidents of 'internal' hacking by patients.	The biggest threat to the sector is posed by state actors (espionage of research data) and internal staff members gaining unauthorised access to data. Criminals seem to have limited interest in medical data.	Cryptoware attacks are popular but do not seem to be sector-specific. A lot of phishing takes place. It often concerns very specific attacks, for example against a person or department.

Resilience: vulnerabilities	Resilience: measures	Interests
There are no relevant developments.	The measures taken by the sector are checked by the government against the DBT Cyber Security. IAEA has taken international initiatives to further improve cyber security in the sector. The sector works more closely with the NCSC. Moreover, the cyber component of the Counterterrorism Alert System has been implemented.	IT mostly plays a supporting role within the sector, for example when arranging access security. The importance of nuclear safety is a well-known fact.
According to the sector, the wide dissemination of personal and other data within the government does not always entail a corresponding transfer of responsibilities for the security of such data.	There is a decrease in the use of BYOD in favour of IT managed by the organisation.	The government serves a broad range of interests that depend on IT. Examples include citizens whose primary income depends on it (the Employee Insurance Agency, Social Insurance Bank), the effective actions taken by the police and judicial authorities or the control and management of surface water.
Sometimes a monoculture exists as some IT suppliers supply to (almost) all telecommunications companies. Organisations also find it difficult to 'keep up' with the security of new technologies (such as 4G, 5G and IPv6).	Data minimisation is considered to be a way to represent a less attractive target for attacks. Moreover, initiatives such as AbuseHUB (exchange of information on infections) and MANRS (agreements on internet routing) are of great value to network stability.	The reliability of telephony networks is directly relevant for society. There are also other systems that strongly rely on these networks, such as process control systems (ICS).
The transport sector is characterised by its dependency on a few coordination points. Moreover, processes often become more dependent on IT due to laws and regulations in the sector. If any systems are breached, the impact of such breach will be more substantial.	Awareness is growing, also at the administrative level. The government is also more interested in adequately securing infrastructures.	Short disruptions may have economic consequences as transports then take place via other countries. Long-term disruptions may lead to problems in food supply.
Actors specifically focus on digital fraud. Due to the shift to online services which has been initiated, internet vulnerabilities and the abuse of these vulnerabilities represent an increasing risk to insurers, authorised representatives and intermediaries.	The sector is continuously working on increasing and maintaining the maturity level of security measures, taking account of a continuously evolving risk landscape. This is supervised by De Nederlandsche Bank (DNB).	<p>The sector is digitally responsible for large money flows and financial transactions and processes many sensitive data belonging to citizens.</p> <p>If an insurer suffers financial damage, this will have indirect consequences for the premium insured persons have to pay.</p> <p>Individual incidents may have an impact on the reputation of the sector as a whole..</p>
The 'own initiative' of medical specialists (setting up their own databases) or pharmaceutical companies (providing their own apps) makes security difficult. It is believed that data classification is used insufficiently or improperly.	The establishment of the ISAC for the healthcare sector gives rise to important cooperation in the security of data. The duty to report data breaches and attention of management and supervisory boards ensure that the subject is placed on the management agenda.	The sector is responsible for the quality of patient care. The quality and confidentiality of patient data are important preconditions here.

Appendix 3 Terms and Abbreviations

0day	See Zero-day vulnerability.
2G/3G/4G	Different generations of mobile communication. In the Netherlands these generations stand for GSM (2G), UMTS (3G) and LTE (4G).
AIVD	General Intelligence and Security Service
APT	An Advanced Persistent Threat (APT) is a motivated (and sometimes advanced) targeted attack on a nation, organisation, person or group of persons.
Authentication	Authentication means finding out whether the proof of identity of a user, computer or application complies with the authenticity characteristics agreed in advance.
Bitcoin	A currency, see crypto currency.
Booter service	Online service carrying out DDoS attacks against payment for actors without technical knowledge.
Bot/Botnet	A bot is an infected computer that can be operated remotely with malicious intent. A botnet is a collection of such infected computers that can be operated centrally. Botnets form the infrastructure of many types of internet crime.
BSI	The Bundesamt für Sicherheit in der Informationstechnik (BSI) is the German public service for connection and information security.
BYOD	Bring Your Own Device (BYOD) is a regulation in organisations whereby personnel are permitted to use their own consumer devices for carrying out tasks for the organisation.
C&C	A Command & Control (C&C) server is a central system in a botnet from which the botnet is operated.
Certificate	A certificate is a file that serves as a digital identification of a person or system. It also includes PKI keys used to encrypt data during transmission. A familiar application of certificates is an https secure website.
Certificate authority	A certificate authority (CA) in a PKI system is an organisation that is trusted to generate, issue and withdraw certificates.
Cloud/Cloud services	A model for system architecture based on the internet (the 'cloud'), whereby use is mainly made of Software as a Service (SaaS).
CMS (Content Management System)	A content management system is a software application that allows users without a lot of technical knowledge to place documents and data on a website.
Confidentiality	A quality characteristic of data in the context of information security. Confidentiality can be defined as a situation in which data may only be accessed by someone with the authorisation to do so. This is determined by the owner of the data.
Crypto currency	An umbrella term for digital currencies whereby cryptographic calculations are used as authenticity feature and for transactions. The bitcoin is the most common crypto currency.
Cryptoware	Type of ransomware that encrypts files on a computer or in a network. The key is only issued against payment.

Cyber criminal	Actors who commit cyber crime professionally, the main aim of which is monetary gain. The CSAN differentiates the following groups of cyber criminals: <ul style="list-style-type: none"> • in a strict sense, those who carry out attacks themselves (or threaten to do so) for monetary gain; • criminal cyber service providers, those who offer services and tools through which or with which others can carry out cyber attacks; • cyber dealers or service providers for stolen information; • criminals who use cyber attacks for traditional crime.
Cyber researcher	An actor who goes in search of vulnerabilities and/or breaks into IT environments in order to expose weaknesses in the security.
Cyber security	The state of being free of danger or damage caused by a disruption or failure of IT or through the abuse of IT. The danger or damage caused by abuse, disruption or failure may comprise a limitation of the availability and reliability of the IT, violation of the confidentiality of information stored in IT environments or damage to the integrity of that information.
Data breach	The intentional or unintentional disclosure of confidential data.
(D)DoS	(Distributed) Denial of Service is the name of a type of attack whereby a particular service (for example a website) is made inaccessible to the customary users of that service. A DoS on a website is often carried out by subjecting the website to a great deal of network traffic, which subsequently makes the website inaccessible.
DigiD	The digital identity of citizens used to identify and authenticate themselves on government websites. It allows government institutions to ascertain whether they are actually dealing with the individual in question.
DKIM	DomainKeys Identified Mail is a protocol that allows for the sending mail server to place digital signatures in legitimate e-mails. 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 state what needs to be done with non-authentic e-mails from his domain. The authenticity of e-mails 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 (DNS) links internet domain names to IP addresses and vice versa. For example, the website 'www.ncsc.nl' represents IP address '62.100.52.109'.
DNSSEC	DNS Security Extensions (DNSSEC) is a set of extensions to DNS involving the addition of an authentication and integrity check to the existing system.
EMV	Europay Mastercard Visa (EMV) is a standard for debit card systems using chip cards and chip card pay terminals. The chip card replaces cards with an easy-to-copy magnetic strip.
Encryption	Encoding information to make it unreadable for unauthorised persons.
End of life	In the software industry, the end of life of a product is the moment at which a product is no longer considered current software by the supplier. Software suppliers generally stop releasing updates for end-of-life software and end their software support services.
ENISA	European Network and Information Security Agency
Exploit	Software, data or a series of commands that exploit a hardware or software vulnerability for the purpose of creating undesired functions end/or behaviour.
Exploit kit	A tool used by an actor to set up an attack by choosing from ready-made exploits, in combination with desired effects and method of infection.
GCHQ	Government Communications Headquarters (British intelligence service)

Hacker/Hacking	The most conventional definition for a hacker (and the one used in this document) is someone who attempts to break into computer 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: individuals or groups who launch activist digital attacks motivated by a certain ideology.
Hashing	Hashing is a cryptographic processing used for the irreversible mangling of data. Hashing is used to store passwords in such a way that they are more difficult to abuse after a data breach.
ICS	Industrial Control Systems (ICS), also called Supervisory Control And Data Acquisition (SCADA), are measurement and control systems used to control industrial processes or building management systems, for example. Industrial control systems collect and process measurement and control signals from sensors in physical systems and steer the corresponding machines or devices.
Identity fraud	The intentional abuse of another person's identity data for the purpose of committing fraud.
Incident	An incident is an IT disruption that limits or eliminates the expected availability of services, and/or is the unauthorised publication, acquisition and/or modification of information.
Information security	The process of establishing the required quality of information (systems) in terms of confidentiality, availability, integrity, irrefutability and verifiability as well as taking, maintaining and monitoring a coherent set of corresponding security measures (physical, organisational and logical).
Integrity	A quality characteristic for data, an object or service in the context of (information) security. This is synonymous with reliability. Reliable data is correct (legitimate), complete (not too much and not too little), prompt (on time) and authorised (edited by a person who is authorised to do so).
Internal actor	An individual or a group in an organisation causing cyber security incidents from within.
Internet of Things	The phenomenon in which the internet is not only used to grant users access to websites, e-mail and the like, but also to connect devices that use the internet for functional communication.
IP	The Internet Protocol (IP) handles the addressing of data packages so that they arrive at their intended destination.
IPv4/IPv6	IPv4 is a version of IP with an address space of over 4 billion addresses. IPv6 is its successor, with 3.4 times 10 ³⁸ possible addresses, i.e. fifty billion times billion times billion addresses per person on earth.
ISAC	An Information Sharing and Analysis Centre (ISAC) is an alliance between organisations to facilitate the exchange of (threat-related) information and joint resistance. The NCSC facilitates several ISACs for critical infrastructure sectors in the Netherlands.
Malvertising	The spreading of malware by offering it to an advertising broker, for the purpose of infecting large groups of users via legitimate websites.
Malware	A contraction of 'malicious' and 'software'. Malware is currently used as a generic term for viruses, worms and Trojans, amongst other things.
MitM	Man-in-the-middle (MitM) is a method of attack whereby the attacker is situated between two parties, for example an internet shop and a customer. The attacker masquerades as the shop to the customer and as the customer to the shop. As intermediary, the attacker is able to eavesdrop on and/or manipulate the information exchanged.
MIVD	Military Intelligence and Security Service

NCTV	National Coordinator for Security and Counterterrorism, part of the Ministry of Security and Justice.
NHTCU	National High Tech Crime Unit (Dutch National Police)
NTP	The Network Time Protocol (NTP) is a popular protocol used for automatically setting the time in a system.
Patch	A patch may comprise repair software or contain changes that are directly implemented in a program with the purpose of repairing or improving it.
Phishing	An umbrella term for digital activities with the object of tricking people into giving up their personal data. This personal data can be used for criminal activities such as credit card fraud and identity theft. Spearphishing is a version of phishing that is directed against one person, or a very specific group of persons, deliberately targeted for their position of access in order to achieve an as big as possible effect without being noticed.
PKI	A Public Key Infrastructure (PKI) is a set of organisational and technical resources with which one can process a number of operations in a reliable manner, such as encrypting and signing information and establishing the identity of another party.
PoS	A Point-of-Sale (PoS) is a computer that records sales transactions.
Ransomware	Type of malware that blocks systems and the information they contain and only makes them accessible again against payment of a ransom.
RAT	A Remote Access Tool (sometimes referred to as a Remote Access Trojan, RAT) is used to gain access to the target's computer in order to control it remotely.
Resilience	The ability of people, organisations or societies to resist negative influences on the availability, confidentiality and/or integrity of (information) systems and digital information.
Responsible disclosure	Practice of responsibly reporting any security vulnerabilities found. Responsible disclosure is based on agreements usually entailing that a reporter will not share his discovery with third parties until the vulnerability has been repaired, and the affected party will not take legal action against the reporter.
SCADA	See ICS.
Script kiddie	Actor with limited knowledge who draws on tools which have been devised and developed by others, for cyber attacks motivated by mischief.
Sensitive information	Information about critical infrastructure that could be used, if this information were to be disclosed, to make plans and commit offences with the object of disrupting or destroying critical infrastructure systems.
SIDN	Stichting Internet Domeinregistratie Nederland, or Foundation for Internet Domain Registration in the Netherlands
Skimming	The illegitimate copying of data from an electronic payment card such as a debit card or credit card. Skimming often involves the theft of PIN codes with the ultimate aim of making payments or withdrawing money from the victim's account.
Social engineering	A method of attack that exploits human characteristics such as curiosity, trust and greed with the objective of obtaining confidential information or to induce the victim to perform a particular action.
Spearphishing	See phishing.
SPF	Sender Policy Framework is a protocol used by the owner of a domain name to indicate which servers are allowed to send legitimate e-mails on behalf of his domain. The owner of the domain name publishes the list of authorised servers in a DNS record.

SQL injection	A method of attack used by an attacker to influence communication between an application and the underlying database, with the main objective of manipulating or stealing data from the database.
State actor	A state actor acts on behalf of a national government.
Steganography	A technique that is used to hide data by including them in another data flow, such as in images or audio files.
TCP	Transmission Control Protocol
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.
Threat	<p>The Cyber Security Assessment Netherlands defines purpose and threat as follows:</p> <ul style="list-style-type: none"> • The higher purpose (intention) may be strengthening an organisation's competitive position; political/national gain, social disruption or threatening a person's life. • In the Assessment, threats are categorised as follows: digital espionage, digital sabotage, publication of confidential data, digital disruption, cyber crime and indirect disruptions.
TLS	Transport Layer Security is a protocol for the purpose of setting up a secure connection between two computer systems. TLS forms the basis of the https protocol. TLS is the successor to Secure Sockets Layer (SSL).
Tool	A method or computer program used by an attacker to exploit or increase existing vulnerabilities.
Two-factor authentication	A method of authentication requiring two independent proofs of an identity.
UDP	User Datagram Protocol
USB	Universal Serial Bus (USB) is a specification of a standard for the communication between a device (generally a computer) and a peripheral.
USB stick	Portable storage medium which is connected to a computer via a USB port.
VPN	A Virtual Private Network (VPN) is an isolated, encrypted connection between a device and a particular server on the internet. This can be used to gain safe company or internet access from untrusted networks.
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 approach it without the proper authorisation.
Watering hole	A watering hole attack is aimed at a location where many intended victims gather. The attacker spreads his exploit or malware via a website that they regularly visit by abusing a vulnerability in this website or a CMS on which the website is based.
Web application	The entirety of software, databases and systems involved in the proper functioning of a website. The website is the visible part.
Zero-day vulnerability	A zero-day vulnerability is a vulnerability for which no patch is available yet because the developer of the vulnerable software has not yet had time to make a patch.



Publication

National Cyber Security Centre
PO Box 117, 2501 CC The Hague, the Netherlands
Turfmarkt 147, 2511 DP The Hague, the Netherlands
+31 70 751 55 55

More information

www.ncsc.nl
csbn@ncsc.nl

November 2015