National Cyber Security Centre
*Ministry of Security and Justice*

# Cyber Security Assessment Netherlands

## CSAN 2016

# Cyber Security Assessment Netherlands

## CSAN 2016

## 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 organisations with a vital function in society by providing them with expertise and advice, threat response and with actions to strengthen 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.

## National Coordinator for Security and Counterterrorism

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

## 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)
- General Intelligence and Security Service (AIVD)
- Dutch National Police (National High Tech Crime Unit)
- Public Prosecution Service
- Representatives of critical infrastructure organisations, members of the Information Sharing and Analysis Centres (ISACs) and other NCSC partners
- NCTV
- National Management Organisation for Internet Providers *(Nationale Beheersorganisatie Internet Providers)*
- Internet Standards Platform *(Platform Internetstandaarden)*
- Bits of Freedom
- Consumers' Association
- ICT Netherlands *(Nederland ICT)*
- Dutch Payments Association
- Confederation of Netherlands Industry and Employers (VNO-NCW)
- Scientific institutions
- Universities
- Experts in the field of cybersecurity

The contributions of these parties have, together with substantive reviews, publicly accessible sources, a survey, information from the critical infrastructure and analyses from the NCSC, contributed to the substantive quality of this assessment.

# Table of contents

*Professional criminals have evolved into sophisticated actors and carry out long-lasting and high-quality operations*

*Digital economic espionage by foreign intelligence services puts the competitiveness of the Netherlands under pressure*

*Ransomware is commonplace and has become even more advanced*

*Advertising networks have not yet shown the ability to cope with malvertising*

# Summary

**The Cyber Security Assessment Netherlands (CSAN) 2016 offers insight into interests, threats and resilience, as well as related developments in the field of cybersecurity. This CSAN focuses primarily on the Netherlands, for the period from May 2015 to April 2016. The CSAN is published annually by the National Cyber Security Centre and is drawn up in cooperation with public and private partners.**

**In the past year, state actors and professional criminals formed the largest threat for the Netherlands in the field of cybersecurity.** Over the reporting period, they have caused many incidents, or have attempted to do so. Also, the threat that emanates from these groups is huge, and has grown in the past year.

**Criminals have, over the past year, focused massively on ransomware and the degree of organisation of criminal campaigns is continually increasing.**
On a regular basis, organisations in society must deal with computers and data that have been made inaccessible by ransomware. For criminals, campaigns with ransomware are easy to carry out. Criminals take into account the purchasing power of victims: sometimes more ransom is demanded if (large) organisations are infected. Thus, ransomware, in recent years, has developed into the tool of choice for professional criminals to make money. The classic measures of regular backups and network segmentation can limit the impact of ransomware attacks. In addition to short actions aimed at making money quickly, professional criminals are expanding their methods: **professional criminals have evolved into sophisticated actors and carry out long-lasting and high-quality operations. In the past year, several long-running campaigns were observed, using advanced forms of spear phishing. With this, both the investments and the proceeds of the campaigns have increased.** In the past, this way of working was the domain of state actors.

State actors have, over the past year, carried out a great deal of digital espionage on the leading Dutch sectors. **Digital economic espionage by foreign intelligence services puts pressure on the competitive position of the Netherlands.** In addition to economic espionage, foreign intelligence services actively collect political information via digital pathways. The Dutch government suffers regular digital attacks. **Political espionage undermines politics and government and is therefore a threat to the democratic legal order.** Abroad, manifestations by state actors have been observed that deploy sabotage and other (military) cyber capabilities. The threat has increased for the Netherlands. State actors have deployed digital attacks abroad more frequently to achieve their strategic objectives, to influence conflicts and, in some cases, to support an armed struggle. Cybersecurity measures taken can also protect against a digital component of hybrid attacks.

**Encryption has received much attention over the past year.** The interests of the parties are sometimes at odds with each other. In the discussion on the relevance of encryption, the interests of detection and national security must be balanced against the security of the internet and the privacy of its users. In the Netherlands, the government has published its official position on encryption. The government endorses the importance of strong encryption for internet safety, in support of the protection of the privacy of citizens, for confidential communications of government and businesses and for the Dutch economy. **The government has sent its position on encryption to the House of Representatives. The government is of the opinion that it is not currently appropriate to take legal measures to restrict the development, availability or the use of encryption.**

**Hacktivists and terrorists in the field of cybersecurity pose less of a threat than state actors and professional criminals, but**

**these actors have developed over the past year.** There have been no terrorist attacks recently using digital resources. However, they do generate a lot of media attention with small-scale digital attacks which require little knowledge or skill. Hacktivists have, over the past year, focused on the online publishing of sensitive corporate information and personal information.

**Cyber vandals and script kiddies are a growing threat.** They can carry out digital attacks with accessible tools and at low cost. Think of booter services to perform DDoS attacks; these are forms of cybercrime-as-a-service. This criminal industry has expanded over the past year. Standard solutions are being offered online and continuously improved. Ready-to-use exploit kits are traded on underground market places. In these, malware is offered as a service, including a help desk that is available 24/7. The amount of malware on mobile devices is increasing greatly. These devices are an interesting target because an increasing number of (financial) activities take place on them. They often remain vulnerable because updates are not installed or because sometimes no updates are available when devices are several years old.

**Just like last year, many DDoS attacks have been observed in the past year.** These attacks are primarily carried out by criminals, hacktivists, cyber vandals and script kiddies. In addition to running these attacks and thus bringing websites, infrastructures and systems down, DDoS attacks are also used for extortion. Often, these are empty threats. **Many organisations have, over the past year, taken measures collectively or organisationally, against DDoS attacks.** These measures are effective for many attacks, but do require investments. Private parties are working collectively on various initiatives to be able to implement DDoS protection more easily and cheaply by working together.

**Chain dependencies and the connectivity of industrial control systems make critical processes in Netherlands vulnerable.** A chain is only as strong as its weakest link. Moreover, the blending of industrial control systems and office automation introduces, alongside of the many benefits, vulnerabilities into this chain.

**SMEs, compared to larger companies, take relatively few measures in the field of cybersecurity.** This is the case while a large part of the Dutch economy is formed by small and medium-sized enterprises. The low resilience of SMEs in the field of cybersecurity can have a negative impact on the Dutch economy.

**Keeping devices and software up to date remains a challenge.** Organisations are vulnerable because systems updates are not installed in due time. In organisations with industrial control systems, the systems are often vulnerable and updates are not carried out regularly. This is usually due to a concern that updating will lead to loss of productivity. **There is room for improvement in the Netherlands in the field of protective measures:** companies often have no good idea of measures that are necessary.

Advertising networks do not seem to be able to cope with malvertising yet. This method of malware distribution remains popular and is a growing problem that is not easy to solve: the manner in which ads are bought in real time and presented to the user happens out of sight of website owners. Currently, advertising networks do not thoroughly check the content of their ads. Combined with the fact that many systems do not have the latest updates, this provides a large attack surface. **Effective protection against malvertising without affecting the revenue model of websites requires fundamental measures in the way advertising networks operate.**

In recent years, various parties have worked hard to reduce the number of rogue websites that are hosted in the Netherlands. **Hosting providers, the science community and the police have worked together over the past year to reduce bad hosting in the Netherlands.** Improvement is visible, but there are still parties that engage in bad hosting.

**In addition to technical vulnerabilities, the Achilles' heel of digital security, people also remain vulnerable.** Malicious parties continue to improve their attempts to get users to act. **Social engineering continues to be popular and is most successful when it comes to specific activities via spear phishing. The transfer of generic skills to identify threats and to act on them is difficult. Information campaigns are failing to pass these on .** Campaigns to raise security awareness work best when they focus on a defined problem, such as internet banking.

In the past year, the **Coordinated Vulnerability Disclosure Manifesto** was drafted. Signatories of this manifesto endorse the importance of the vulnerability-disclosure process (responsible disclosure) and appreciate the interaction with researchers and the hacker community. In May 2016, the manifesto was signed by 29 parties from home and abroad during the high level meeting, organised during the Dutch EU Presidency.

Internet service providers in the Netherlands have established the Dutch Continuity Board (DCB), which works on measures to limit the impact of DDoS attacks on Dutch critical infrastructure and to make services that have been disrupted available again as soon as possible. The government has, over the past year, taken steps to become more digitally secure and to make the Netherlands digitally safer. The central government has taken action so that recipients have more certainty about the sender of e-mails from the government. **The Platform for Internet Standards has launched the website internet.nl, enabling users to make sure that internet connections, websites and e-mail use modern (security) standards.** Also, the new Personal Data Protection Act came into force on 1 January 2016. **With the new law, the data breach reporting obligation entered into force.** All parties are now required to report possible personal data incidents to the Dutch Data Protection Authority. The fines that may be imposed, can encourage the taking of measures against the leaking of this information.

# Key findings

The summary gives a concise and complete picture of interests, threats and resilience in the field of cybersecurity. In addition, notable observations from the reporting period are contained in four key findings. These key findings are described below.

### Professional criminals have evolved into sophisticated actors and carry out long-lasting and high-quality operations

Campaigns by professional criminals are becoming more and more sophisticated. In the past, the digital attacks and associated campaigns by criminals were often of short duration and focused on earning quick money by targeting a great number of parties. Criminals have, in the past year, implemented a number of campaigns where huge investments have been made and which show a high degree of organisation. In addition, spear phishing by criminals is becoming ever more sophisticated and therefore more credible. Spear phishing is thus becoming increasingly difficult to fight with security awareness. Prolonged campaigns with large investments and advanced spear phishing were, in the past, the terrain of state actors.

### Digital economic espionage by foreign intelligence services puts the competitiveness of the Netherlands under pressure

The past year has seen many digital attacks on companies in the Netherlands in which the motive was economic espionage. Espionage for economic purposes is harmful to the position of the Netherlands. These attacks focused on acquiring technology that sometimes still has to prove its value. Two thirds of the affected companies were unaware of these attacks.

### Ransomware is commonplace and has become even more advanced

The use of ransomware by criminals in the past year has become common. Infections are everyday occurrences and affect the entire society. Whereas in the past the same price had to be paid per infection, the price is now determined on the basis of the type of affected organisation. In addition, the malware itself is more sophisticated: in addition to files on the local disk, nowadays databases, backups and files on network drives are encrypted.

### Advertising networks have not yet shown the ability to cope with malvertising

The distribution of malware via ads on major websites is a problem. Advertising networks have not yet been able to find solutions to this problem. The wide range of advertising networks provides, along with the large number of systems from which the latest updates are missing, a large attack surface. Operators of these websites and advertising networks themselves do not have full control over the ads. This makes it possible for malware to be spread. The complete ad blocking in the browser affects the business model of website owners. To protect users against malvertising without blocking all ads, fundamental changes are needed in the way these networks work.

# Insight into threats and actors

Table 1 provides insight into the threats that the various actors have posed over the period between May 2015 and April 2016 to the targets 'governments', 'private organisations' and 'citizens.' Professional criminals and state actors remain a major threat to government, private organisations and citizens. Threats that are indicated in red may increase while the level is already high.

Threats that, compared the CSAN 2015, have grown or shrunk, are indicated by an arrow. The threat posed by cyber vandals and script kiddies has grown in terms of disruption of IT. They have many tools at their disposal to carry out attacks relatively easily, including DDoS attacks. Theft of information by these actors is a limited threat to all targets. The threat of theft and publication of obtained data by hacktivists has grown, while this threat by internal actors has shrunk, compared to last year.

## Table 1 **Threat matrix**

| | Targets | | |
|---|---|---|---|
| **Source of the threat** | **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 | Digital espionage | Digital espionage | Digital espionage |
| | Offensive cyber capabilities | 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 obtained information ↗ | Theft and publication of obtained information ↗ | |
| | 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 with respect to CSAN 2015.*

| | | |
|---|---|---|
| *No new trends or phenomena are recognised that pose a threat.*<br>*OR*<br>*(sufficient) measures are available to remove the threat.*<br>*OR*<br>*No appreciable manifestations of the threat occurred during the reporting period.* | *New trends and phenomena are observed that pose a threat.*<br>*OR*<br>*(limited) measures are available to remove the threat.*<br>*OR*<br>*Incidents have occurred outside the Netherlands and there have been several minor incidents in the Netherlands.* | *There are clear developments which make the threat expedient.*<br>*OR*<br>*Measures have a limited effect, so the threat remains substantial.*<br>*OR*<br>*Incidents have occurred in the Netherlands.* |

# Introduction

The Cyber Security Assessment Netherlands is published annually by the National Cyber Security Centre. The CSAN is realized in close cooperation with a large number of parties, both public (police, intelligence and security services and the Public Prosecution Service) and scientific organisations and private organisations (companies in the critical processes and the parties represented in the ISACs).

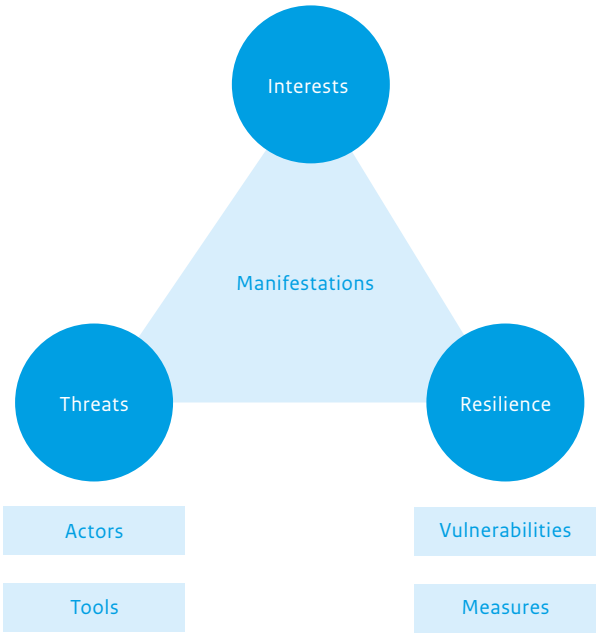
The CSAN 2016 offers insight into the interests, threats and resilience, as well as the related developments, in the field of cybersecurity. It focuses primarily on the Netherlands, for the period from May 2015 through April 2016. The intention is for policy makers, in government and the critical processes, to enhance the digital resilience of the Netherlands or to improve current cybersecurity programmes.

The CSAN is a factual description, with interpretations based on insights and expertise from government services and organisations in the critical processes 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 barely changed with respect to the previous editions have been described in brief or not at all.

## Readers' guide

The key questions of the CSAN 2016 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 triangle of interests, threats and resilience is a model for the chapter format of the CSAN.




Chapter 1 describes which matters have manifested themselves during the reporting period within the triangle of interests, threats and resilience. It gives an overview of relevant manifestations in the Netherlands. Foreign manifestations are mentioned where they are relevant to the Netherlands, although the Netherlands need not be directly affected.

Threats are discussed in the chapters about actors and tools. The abilities, characteristics and methods of actors are described in Chapter 2. Chapter 3 describes the tools that these actors use and their development.

The resilience of the Netherlands can reduce the chance that a threat will manifest itself and can limit the impact of manifestations. Chapter 4 describes the vulnerabilities. Chapter 5 describes the measures taken to reduce those vulnerabilities and to strengthen resistance and resilience.

Chapter 6 discusses the Dutch interests and focuses on the changes in these interests over the past year and what their impact is on cybersecurity.

The appendices provide an overview of the incidents handled by the NCSC, an assessment of cybersecurity within the various sectors and explain the abbreviations used.

*Ransomware is commonplace and infections are everyday occurences*

# 1 Manifestations

**The number of infections with ransomware has increased significantly since the previous reporting period. Successful digital espionage is second to none and is a significant threat to national security. The data breach reporting obligation has been in force since 1 January 2016. In the first quarter of 2016, the Dutch Data Protection Authority received over a thousand reports of data breaches.**

## Activities aimed at monetary gain

### Ransomware is commonplace and has become even more advanced

Ransomware[1] has boomed since the previous reporting period. Organisations and individuals throughout society have much to do with computers and data made inaccessible by such malware.

The number of ransomware infections has increased significantly, according to representatives from various sectors who were interviewed for this CSAN. For example, the energy sector is faced with infections several times a month. These lead only to limited disruptions of office automation and do not reach process automation. Also, the healthcare and telecom sectors are facing extraordinary increases in the number of infections. Managed service providers, which often provide the automation for other sectors, find that a majority of their clients deal with more than one infection per year.

During the reporting period, the police received 124 notifications and reports of infections with ransomware. At least 35 of these notifications and reports were specifically about cryptoware. These numbers are probably only a fraction of the total number of incidents with ransomware. Problems when recording official reports, inconsistency in registration and unfamiliarity with the possibility of reporting and filing official reports, are the cause that not all incidents can be found in these statistics. Figures from Statistics Netherlands support this: in 2015, 11 percent of the Dutch population fell victim to cybercrime; official reports were filed in only a small number of the cases.[2]

Various sectors indicate that the mode of infection with ransomware is changing. Previously, these were only random infections. Now, the energy sector, water management organisations and managed service providers indicate that they are regularly confronted with person or organisation-targeted phishing e-mails by which attackers try to install ransomware. Other sectors, especially the banking sector, see, however, very little targeted phishing to install ransomware infections.

Organisations find that ransomware infections still occur largely because workers read their private e-mail at their workplace. For this, workers use the web mail functionality of their private e-mail. In this e-mail, there are, for example, links to a website that infects the computer of the employee.

Various sectors have different experiences with the distorting effect of ransomware. The managed service providers and the energy sector see infections with ransomware today as 'business as usual.' They routinely restore back-ups. This leads to reduced disruption to the organisation. The insurance industry indicates that ransomware infections are experienced as very disruptive for the organisation.

Also, the nature of ransomware by which infections take place, has changed lately. In this reporting period, manifestations have been observed in which backups and network drives were encrypted. Where ransomware initially encrypted the files on the computer of the end user, it is now searching further into the network. User-accessible network drives are also encrypted so the consequences of infection are felt by much larger areas of the organisation.

Services in hospitals abroad have been interrupted several times by ransomware infections. In the Netherlands, as far as we know, this has not yet happened.

A hospital in the German city of Neuss was the victim of ransomware that encrypted patient information, as was announced in February 2016.[3] The malware, 'normal' consumer ransomware, was distributed via an e-mail attachment. Operations had to be postponed and e-mail communication was suspended. RP Online, a German news website, stated that five other German hospitals kept it to themselves that they had incurred the same infection.

At Hollywood Presbyterian Medical Center in Los Angeles, ransomware disrupted the functioning of the computer network in February 2016.[4] The hospital stated that the ransomware did not gain access to patient data. CT scanners, laboratory robots and drug supplying machines were, however, sabotaged. The hospital eventually paid the ransom of 17,000 dollars.[5]

It is certainly not always possible to find the perpetrators of a ransomware infection. In September 2015, in Amersfoort the Dutch police succeeded, in collaboration with Kaspersky, in arresting two suspects of 18 and 22 years old. They were accused of infecting tens of thousands of computers worldwide with Coinvault ransomware.[6]

## The increase in malvertising feeds discussion on the need for adblockers

This year, as well, was not unusual for visitors of regular websites to be confronted with malware in the ads displayed. This is not only found in obscure corners of the internet, but also on very popular Dutch websites. The method used for these attacks suggests that the perpetrators are usually criminals.

In June 2015, Fox-IT discovered that a number of news websites, including De Telegraaf website, were distributing malware through the displayed ads.[7] The infected ads came from the advertising networks Rubicon and AppNexus. These ads used the Angler exploit kit to infect visitors of the websites with malware.

Also in April 2016, Fox-IT detected a malvertising campaign on Dutch websites. This time, there were at least 288 different websites, including very popular websites such as Nu.nl, Buienradar and Marktplaats.[8] Here, too, the attackers used the Angler exploit kit to infect users with malware.

Malvertising on popular Dutch websites adds to the debate about whether or not it is appropriate to block ads via an adblocker. The growing use of adblockers has led to the creation of providers of anti-adblock services for website owners. Ironically, it was PageFair, an anti-adblock service, which was used for a malvertising campaign in November 2015. More than five hundred websites that make use of this service offered, for an hour and a half, malware through displaying ads.[9]

## Innovative criminals steal financial resources and goods

Banks have become more resilient against banking malware, as the police have noticed. Man-in-the-browser attacks targeted at end users no longer work as well, thanks to fraud detection by banks. Logically, cybercriminals have therefore gone looking for other work methods, tools and targets. This could explain why the use of banking trojans continues to decrease and the use of ransomware and RATs (Remote Access Tools) continues to increase. For example, we now see attacks on banking systems themselves rather than on the account holders. This happened, for example, in Carbanak[10] and in attacks on foreign banks in which attackers gained access to systems by which transactions are deposited on the SWIFT network.

RATs are very popular among criminals. During the reporting period, the police received 40 notifications and reports of incidents with RATs. That is remarkable, because the deployment of an RAT is very labour intensive for a criminal.[11] Criminals use RATs to search within computer networks of organisations for valuable systems and information. There are also online market places where anyone can purchase these activities as a service.

Phishing campaigns where users are prompted to fill in passwords or pay an amount of money are still common. For example, in November 2015, an attacker pretended to be the Central Fine Collection Agency (CJIB).[12] The attacker sent bogus fines to people and manipulated them to pay as soon as possible. Victims thought they were sending money to the CJIB, but it was sent to the criminal.

Multiple organisations are being faced with much more targeted and advanced social-engineering attacks. Managed service providers indicate that their clients are regularly confronted with complex and highly targeted phishing attacks. The success ratio of such attacks is quite high. Representatives of multinationals and the transport sector add that they are seeing a huge rise in the number of spoofed e-mails. This includes e-mails in which the attacker pretends to be the CEO or CFO of the company. This form of fraud is also known as CEO or CFO fraud. In this way, the attacker tries to authorise large transactions into his account.

The transport sector also says that they observe that criminal organisations recruit their staff to supply information from internal IT systems. If, for example, they reveal the location of a container full of expensive smart phones, it will be much easier for the other criminals to seize them.

In February 2016, unknown persons stole 81 million dollars from the central bank of Bangladesh by hacking into their systems.[13]

They supposedly gained access to the SWIFT transactions system at the bank. This system is used for international inter-banking payment transactions. BAE Systems, an information security company, claims to have discovered what malware was used in the attack.[14] It seems that this malware specifically targets the SWIFT Alliance software suite, which is used by the Bangladesh Bank. Reuters reports that the Tien Phong Bank in Vietnam was previously targeted in vain by the same attackers.[15] In addition, the Ecuadorian Banco del Austro fell victim to this in the same way.[16]

### Banking and managed service providers are able to repel advanced phishing attacks[17]

A Dutch bank was, in the past period, faced with a very persistent and dedicated phisher. Through physical interceptions, this attacker was able to obtain a limited number of tokens (fewer than ten) belonging to the bank's corporate clients. Such tokens are used to authorise wire transfers. If the attack had succeeded, this could have led to considerable damage. The bank and the managed service provider, together, were able to discover the attack and to block the tokens before the attacker could exploit them.

## Activities aimed at acquiring information

### Digital espionage is second to none

Digital espionage is, from a historical perspective, second to none and is a significant threat to national security. According to the AIVD and MIVD, the observed attacks are only the tip of the iceberg. The total number of cases of digital espionage is many times greater. In the past year, the intelligence services have observed a great deal of digital espionage on Dutch companies in the defence industry and on such leading sectors as high-tech, chemical, energy, life sciences & health and the water sector. It has been established that the attackers were looking for highly specialised technology and sometimes even experimental technology that has yet to prove its market value.

This shows that structural and detailed attention is paid to innovation initiatives in the Netherlands. These technologies are essential for the current and future revenue models of the affected companies. This illustrates the structural and comprehensive digital espionage threat against the innovation and competitive ability of the Dutch business community. Dutch efforts in the fields of research and development are a popular target for digital espionage by state actors. This allows them to keep their economies moving, but also to modernise their armed forces more quickly.

The extent of the economic damage from digital espionage on Dutch companies is difficult to establish. It also turns out that about two-thirds of the affected companies were not aware of these attacks up to the moment of notification by intelligence services.[18] On Wednesday 15 June 2016, the Volkskrant published an article[19] about the hacking of the Dutch-German defence company Rheinmetall. This company had supposedly been attacked by Chinese hackers since 2012. According to the Volkskrant, the hack was discovered in late 2015 by the security company Fox-IT.

State actors, in particular foreign intelligence services, actively collect digital political information in the Netherlands. Political espionage undermines political and governmental authority and is therefore a threat to the democratic legal order. The Dutch Government suffers regular digital attacks. The goal of the attacks is to obtain information about political decision-making and positions, the development and content of political-economic plans, agenda items for political meetings and Dutch views and tactics about negotiations in various fields.

In addition to the Dutch Government, political or ethnic minorities in Netherlands are also victims of digital attacks. These attacks are carried out by foreign intelligence services, such as intelligence services from their countries of origin. This is certainly the case if these minorities, in the eyes of their country of origin, constitute a threat to the stability and legitimacy of the regime.

### The Netherlands as a digital transit port for state actors

The Netherlands has a huge amount of bandwidth, one of the world's largest internet hubs and numerous options for renting servers. As a result, the Netherlands is an obvious transit port for digital attacks and it plays an important role in their implementation and dissemination.

Over the past year, several companies and government agencies in various countries in Europe, the Middle East, Asia and North America have been targeted by digital espionage attacks, including those that went via the Netherlands.[20] These attacks focused on political-strategic, military-strategic and economic information. As a result, Dutch IT systems unwittingly play a role in curtailment of civil liberties, evasion of export restrictions, infringement of intellectual property rights and theft of confidential government information.

Among the victims are (partnerships between) government agencies, ministries and the (defence) industry. These are digital attacks on office environments, mobile platforms and industrial control systems.

### Theft of information manifests itself hugely outside of the Netherlands

The past year was marked by a number of targeted hacks, capturing huge amounts of personal data. All these incidents occurred outside the Netherlands. That does not mean that Dutch society is immune from this type of attack. The healthcare sector, for example, indicates that it has seen a clear increase in phishing for login details. They have evidence that the goal of these attacks is financial in nature.

It remains to be seen which part of the data breaches is visible to the outside world. Fear of reputational damage can lead to organisations keeping the discovered data breaches a secret. The data breach reporting obligation, in force since January 2016, requires that all breaches of personal data be reported to the Dutch Data Protection Authority. The AP has reservations, however, as to whether all breaches are reported.[21]

In June 2015, the U.S. Office of Personnel Management (OPM) made it known that it had been the victim of a hack. With the hack, the data of four million government employees was stolen. Later that month, it was announced that the data of 21.5 million employees and applicants had been stolen.[22] This included information concerning security screenings of American government personnel. The attacker could exploit such data for counter-espionage and for pressuring or blackmailing government employees. There was speculation about China's involvement in the hack, but the Chinese government has said that it is not responsible for the attack.[23] Later, the Chinese government arrested a number of hackers who, according to them, had carried out the hack.[24]

With the hack on Ashley Madison, a website for people looking for an affair, the personal data of more than thirty million people was stolen.[25] The hackers demanded that the website be shut down and threatened with publication of the user data. When the website was not taken off-line, the hackers published the data of 32 million users, mostly men.[26] Presumably, other attackers then used the data in this dataset to blackmail those involved.[27] According to the Toronto police, the hack even drove two of the website users to suicide.[28]

The hack on Ashley Madison was not the only ideologically motivated leak during this period. From the Italian company Hacking Team, hundreds of gigabytes of internal business data were made public via BitTorrent and Twitter after a hack.[29] In 2012, Reporters Without Borders named Hacking Team "enemy of the internet", because it supplied tools to authoritarian regimes to suppress their populations. The breached data is widely seen as a confirmation of the earlier suspicions about Hacking Team's controversial clientele. Meanwhile, the Italian government has withdrawn the broad license of Hacking Team to export their products.[30]

In June 2016, reports appeared in the media[31] stating that hackers had stolen data from computers owned by the United States Democratic Party. The hackers specifically targeted the Democratic National Committee. E-mail and instant messages of Democrats were reportedly leaked. A security company linked the events to a Russian actor.[32] Later, the hack was claimed by an unknown individual, who tried to claim responsibility by disclosing selected documents.[33]

In August 2016, unknown hackers calling themselves the Shadow Brokers alleged to have compromised a U.S. espionage campaign. Through an intrusion, they claimed to have stolen espionage malware.[34] This malware was published in order to strengthen their claim that it came from U.S. intelligence services. Some undisclosed material was being offered for sale via a public auction.[35] The files contained espionage malware, tools that allow attacks on firewalls (including those of Cisco, Fortigate and Juniper).

## Activities aimed at disruption

### Warding off DDoS attacks is costly but increasingly more effective

During the reporting period, organisations were frequently the target of DDoS attacks. The managed service providers and organisations from the central government say it is increasingly possible to take effective measures against ordinary-sized DDoS attacks. However, the possible measures are costly. That makes doing business online more expensive. Also, it is unclear how long the race between attackers and defenders will favour the (wealthy) defenders.

Numerous Dutch organisations were inaccessible online during this period, due to DDoS attacks. During the reporting period, the police received 150 notifications and official reports of DDoS incidents. Schools are regularly victims of an attack.[36] The attack is usually directed against any PC at the school a student attends, but it affects the router and internet connection of the entire school.[37] Individual end users are affected, such as online gamers whose competitors make it impossible in this way for them to play the game. A gamer's internet service provider can certainly be hindered by this.[38] These attacks are often aimed at disrupting a single connection, but can have an impact on all of a provider's connections.

On two consecutive evenings in August 2015, the DNS servers of internet service provider Ziggo were the target of a DDoS attack. Because of this, nearly two million Dutch citizens temporarily had no internet. In October, the police arrested five boys in connection with the DDoS attacks.[39] Four of them were under the age of 18, the fifth was 21 years old.

It is not uncommon for Dutch organisations to be extorted with DDoS attacks. Attackers perform a small DDoS attack and report their intention to stage a much larger attack at a later date. Only if the organisation pays, will the attack be called off. A well-known group that extorts in this way is DD4BC (DDoS for bitcoin). In none of the Dutch cases known at the NCSC during the reporting period did failure to pay lead to a larger attack after the deadline. Managed service providers indicate that, every week, they are confronted with attempts at extortion of their customers with DDoS attacks.

### Digital sabotage and influence

In the Netherlands, there have not been incidents of successful sabotage involving state actors. The transport sector does indicate that regular incidents occur involving disgruntled or recently-fired employees who misuse their IT authorisations to cause considerable damage.

Abroad, there have been much more serious forms of sabotage attacks. The most effective was, no doubt, the attack on Ukrainian electricity companies, whereby between 700,000 and 1.4 million people came to be without power. The perpetrators hacked into the systems of the electricity companies, after which they could obstruct the operation of the system. After about six hours, the power supply was restored.

Intelligence agencies find that state actors increasingly use digital tools to achieve their strategic objectives, to resolve (international) conflicts and to support, in some cases, an armed struggle. Examples of this trend are the conflicts in the Ukraine and Syria, where such means are used regularly.

Alongside of digital espionage, this is also reflected in digital sabotage and activities to influence public opinion. The deployment of digital espionage, sabotage or influencing with these objectives is cost effective. Moreover, the internet has the potential to carry out such operations relatively anonymously. That complicates attribution.

### Defacements are widely used for propaganda

Many websites are still defaced on a daily basis. In order to do this, a vulnerability in the web application is used in order to alter the content that a visitor sees. Generally, a defacement is not a sign that the core processes of an organisation are digitally at risk.

Defacements are usually performed with an ideological motive, or to display certain skills or to brag. Ideological defacements, for example, are regularly carried out by sympathisers of ISIS. Such attacks are not seen as terrorist activities in themselves, but only as propaganda. They are, of course, criminal offences.

## Manifestations with unintentional damage

### Failure of IT can have a major impact

Even without people attacking the systems, they can fail to function. This happens, for example, when a system becomes overloaded or an administrator makes a mistake.

In May 2015, there was a short malfunction at the Amsterdam Internet Exchange (AMS-IX). As a result, various websites and other services depending on transmission via the AMS-IX were temporarily hard to reach or out of commission. Because AMS-IX is one of the largest internet hubs in the world, the effects were noticeable not only in the Netherlands, but also abroad. The malfunction was caused by a human configuration error during maintenance work.[40]

Also, with software in new places, such as in thermostats, malfunctions may occur. That usually happens in devices from the Internet of Things. The smart thermostat Nest by Google had a malfunction in January 2016.[41] It turned out that the control of the individual thermostats depended on the proper functioning of the Google systems. Due to the malfunction of these systems, all Nest users were unable to operate the thermostat.

During the attacks in Brussels in March 2016, so many people tried calling and texting that it overloaded the mobile telephone network. The authorities advised people to use text message or data services and not to call.[42] They hoped that the network would, in that way, remain available. The communications system of the Belgian police also suffered from the malfunction. Agents decided therefore to make temporary use of WhatsApp.[43]

### Data breaches often arise by mistakes

The data breach reporting obligation has been in force in the Netherlands since 1 January 2016. Within the framework of the Telecommunications Act, telecom companies already had an obligation to report to the Netherlands Authority for Consumers & Markets. In the first quarter of 2016, the Dutch Data Protection Authority received over a thousand reports of data breaches. Nearly 90 percent of these reports were made in the context of the recently amended Personal Data Protection Act. So before 2016, organisations would not have been obligated to report these data breaches.[44]

Various security issues caused the customers files of, among others, IT service provider Invers,[45] household appliance chain Brabantia[46] and two Dutch hospitals to be compromised during this period.[47]

Human error and negligence also played a role, in this period, in municipalities and the healthcare sector. Private data of thousands of residents from Oegstgeest and Rotterdam was, for a time,

available to everyone; an employee of the municipality of Rotterdam had linked confidential information to a personal computer.[48] A former employee of an application provider contracted by Oegstgeest had stored confidential information on his laptop.[49] In December, an unprotected external hard drive was taken from a researcher from the Antoni van Leeuwenhoek hospital. The hard drive contained patient information and medical data.[50]

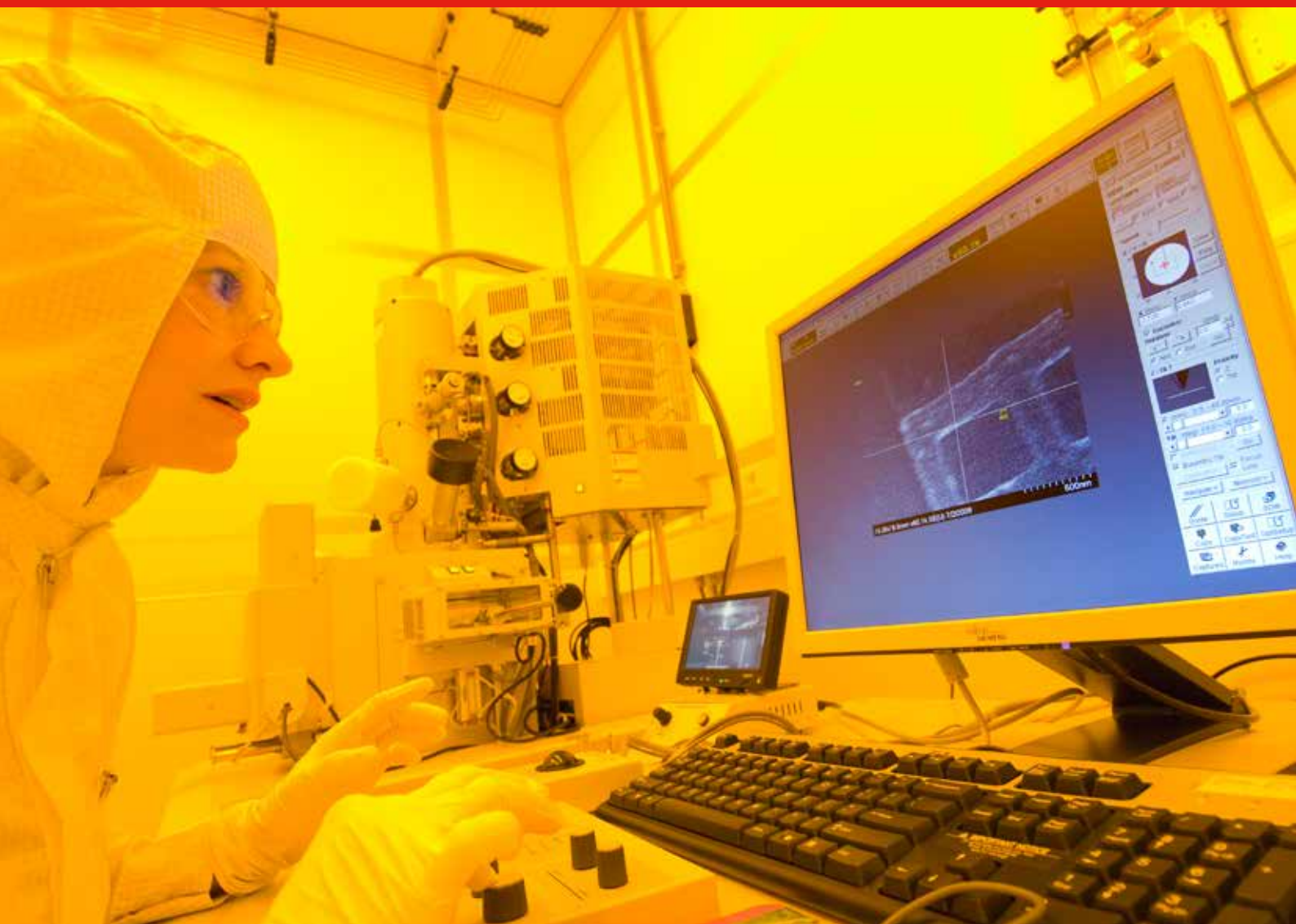
The healthcare sector indicates that data breaches are extremely common there. This is not just about malicious offences such as theft of equipment, but also about errors. A doctor inadvertently sends, for example, the medical file of a patient to another patient.

Central government organisations even indicate that data breaches generally result from human error and not from hackers. Some examples they mention are typos in an e-mail address or attachments of personal data that may not be shared by e-mail.

## Notes

1 In this report, cryptoware, unless explicitly described, is under the collective name: ransomware.
2 http://download.cbs.nl/pdf/veiligheidsmonitor-2015.pdff
3 https://www.security.nl/posting/460845/E-mail+besmet+computers+Duits+ziekenhuis+met+ransomware, consulted on 4 July 2016.
4 http://www.theregister.co.uk/2016/02/15/ransomware_scum_tear_up_tinsel_town_hospital_demand_record_36m/, consulted on 4 July 2016.
5 http://venturebeat.com/2016/02/17/los-angeles-hospital-paid-hackers-17000-ransom-in-bitcoins/, consulted on 4 July 2016.
6 https://www.politie.nl/nieuws/2015/september/16/11-cybercriminelen-aangehouden.html, consulted on 4 July 2016.
7 https://blog.fox-it.com/2015/06/15/large-malvertising-campaign-targeting-the-netherlands/, consulted on 4 July 2016.
8 https://blog.fox-it.com/2016/04/11/large-malvertising-campaign-hits-popular-dutch-websites/, consulted on 4 July 2016.
9 Source: https://blog.pagefair.com/2015/halloween-security-leak/, consulted on 4 July 2016.
10 See CSAN 2015 for a more detailed description of Carbanak.
11 Source: police.
12 https://www.security.nl/posting/450641/Politie+waarschuwt+voor+nepmails+van+CJIB, consulted on 4 July 2016.
13 http://www.reuters.com/article/us-usa-fed-bangladesh-idUSKCN0XI1UO, consulted on 4 July 2016.
14 http://baesystemsai.blogspot.nl/2016/04/two-bytes-to-951m.html, consulted on 4 July 2016.
15 http://www.reuters.com/article/us-vietnam-cybercrime-idUSKCN0Y60EN, consulted on 4 July 2016.
16 http://www.reuters.com/article/us-cyber-heist-swift-specialreport-idUSKCN0YB0DD, consulted on 4 July 2016.
17 Source: the involved managed service provider.
18 Source: AIVD and MIVD.
19 http://www.volkskrant.nl/buitenland/nederlands-duits-defensiebedrijf-gehackt-door-chinezen~a4320398/, consulted on 4 July 2016.
20 Source: AIVD and MIVD.
21 http://nos.nl/artikel/2104842-privacywaakhond-datalekken-worden-niet-gemeld.html
22 https://www.opm.gov/cybersecurity/cybersecurity-incidents/, consulted on 11 July 2016.
23 http://www.welivesecurity.com/2015/12/03/opm-data-leak-not-state-sponsored-says-china/, consulted on 11 July 2016.
24 https://www.washingtonpost.com/world/national-security/chinese-government-has-arrested-hackers-suspected-of-leaking-opm-database/2015/12/02/0295b918-990c-11e5-8917-653b65c809eb_story.html, consulted on 11 July 2016.
25 http://nos.nl/artikel/2047968-gegevens-miljoenen-vreemdgangers-gehackt.html, consulted on 11 July 2016.
26 http://nos.nl/op3/artikel/2052728-hackers-zetten-32-miljoen-vreemdgangers-online.html, consulted on 11 July 2016.
27 http://www.zdnet.be/nieuws/171086/hackers-chanteren-ashley-madison-gebruikers/, consulted on 11 July 2016.
28 http://www.volkskrant.nl/buitenland/-twee-zelfmoorden-na-hack-ashley-madison~a4128352/, consulted on 11 July 2016.
29 https://www.security.nl/posting/434642/Italiaanse+spyware-ontwikkelaar+HackingTeam+gehackt, consulted on 11 July 2016.
30 https://nakedsecurity.sophos.com/2016/04/08/hacking-team-loses-global-license-to-sell-spyware/ , consulted on 11 July 2016.
31 http://nos.nl/artikel/2111102-russische-hackers-maken-data-democraten-buit.html, consulted on 19 August 2016.
32 http://www.darkreading.com/attacks-breaches/russian-hackers-breach-democrats-to-steal-data-on-trump/d/d-id/1325909, consulted on 19 August 2016.
33 http://www.nu.nl/internet/4278512/hacker-guccifer-20-claimt-verantwoordelijkeid-hack-democratische-partij.html, consulted on 19 August 2016.
34 http://www.nu.nl/internet/4307673/hackersgroep-claimt-nsa-spionagesoftware-hebben-gestolen.html, consulted on 19 August 2016.
35 http://nos.nl/artikel/2126368-de-nsa-is-mogelijk-gehackt-maar-door-wie.html, consulted on 19 August 2016.
36 http://nos.nl/artikel/2073898-ddos-aanvallen-treffen-scholen-we-haalden-de-boeken-weer-uit-de-kast.html, consulted on 4 July 2016.
37 Source: interview with Michel van Eeten.
38 Source: police.
39 https://www.politie.nl/nieuws/2015/oktober/7/11-vijf-jongeren-aangehouden-na-aanvallen-op-ziggo.html, consulted on 4 July 2016.
40 https://ams-ix.net/newsitems/194, consulted on 4 July 2016.
41 http://tweakers.net/nieuws/107255/nest-kampte-met-grote-storing-wereldwijd.html, consulted on 4 July 2016.
42 https://twitter.com/CrisiscenterBE/status/712207222718259200, consulted on 4 July 2016.
43 http://www.nieuwsblad.be/cnt/dmf20160326_02205315, consulted on 4 July 2016.
44 Source: Dutch Data Protection Authority.
45 http://www.telegraaf.nl/binnenland/24934680/Invers_lekt_gegevens.html, consulted on 4 July 2016.
46 http://www.brabantia.com/nl/statement-beveiligingsincident, consulted on 4 July 2016.
47 https://www.security.nl/posting/458824/Datalek+bij+drie+ziekenhuizen+treft+ruim+158_000+pati%C3%ABnten, consulted on 4 July 2016.
48 http://www.rotterdam.nl/persoonsgegevens, consulted on 4 July 2016.
49 https://www.oegstgeest.nl/fileadmin/redacteuren/20160309_Vragen_en_antwoorden_DEF_tbv_website.pdf, consulted on 4 July 2016.
50 http://www.avl.nl/topmenu/over-avl/nieuws/persbericht-externe-harde-schijf-onderzoeker-antoni-van-leeuwenhoek-ontvreemd/, consulted on 4 July 2016.

*Professional criminals have developed their skills and are able to execute advanced operations*



# 2 Threats: Actors

**Professional criminals and state actors are still the greatest threat to Dutch digital security. Over the past period, the attack vectors of these parties often remained basically the same compared to previous years. In the future, criminals will continue to expand and deploy ransomware as a revenue model, while making it more targeted. The targeted collection of personal data without the consent of the owner is, for various actors, an increasingly attractive scenario. Also, for malicious parties (without specific knowledge and skills) it is becoming increasingly easier to carry out digital attacks. They can make use of low-threshold tools and affordable forms of cybercrime-as-a-service.**

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

Criminal actors form, in various ways, a serious threat to Dutch digital security. They have a great impact on both individuals and organisations, as well as the Dutch government. The purpose of professional criminals is financial gain. They achieve this by carrying out digital attacks or by threatening to carry out digital attacks (extortion).

During the past period, criminals have shown that they are able to carry out advanced campaigns that require a high degree of organisation. Campaigns such as Carbanak and attacks on banks for the purpose of gaining access to systems that can be used to deposit SWIFT transactions, show that professional criminals are now also focusing on an approach in which a long-term and large-scale campaign is set up. With such campaigns, criminals make, in the medium term, more money than with shorter actions. In the past, activities with such a degree of organisation were only seen among state actors.

In April 2016, the police and the Public Prosecution Service shut down a large encrypted communications network and seized computers from the company that supplied phones and related services in order to communicate via encrypted messages, so-called PGP phones.[51][52] The police often find these phones in criminal investigations into drug trafficking and liquidations. This shows that professional criminals use advanced technical tools to protect communications.

### Criminals are becoming more purposeful in extortion

Moreover, the actions of criminals are becoming more drastic for victims.[53] For example, criminals are increasingly focusing on digital extortion. Ransomware is the most obvious example of this. In the previous reporting period, the use of ransomware by criminals has really taken off in popularity and has continued unabated during this period. The ransomware digital attack methods are becoming more sophisticated and tactics to install the ransomware on the system of victims are increasing in sophistication.

Although the police have observed more targeted attacks in the past period, the ransomware used by criminals in the Netherlands has, thus far, been mainly untargeted. This means that they do not focus on encrypting and extorting specific systems. Both individuals and organisations are affected by this type of extortion. However, there are indications that criminals more often use ransomware to target organisations[54][55][56] Sometimes, they use an adjusted (higher) ransom demand for this and they focus on

vulnerable targets where continuity is important, such as hospitals and care facilities.[57][58] This was the case, for example, in an American hospital where 40 bitcoins (USD 17,000) were paid to the attackers to get the systems operational again as quickly as possible.[59] This was not only worrisome because the patient data was encrypted, even medical equipment was not functioning as a result of this attack.[60]

Criminals are exploiting the successful use of ransomware further by expanding the diversity of their targets. The example of the American hospital also shows that criminals do not only attack standard systems. Also systems such as medical equipment, data bases[61] and even backup files[62] may be vulnerable to these attacks.

In addition to ransomware, Dutch organisations have been victims of DDoS extortion campaigns more often during the past period. In these campaigns, DDoS attacks are used by criminals as part of a blackmail scenario. Via e-mail, criminals threaten with a DDoS attack unless bitcoins are paid to the sender. The DDoS attacks are not always actually carried out.[63] DD4BC[64][65] and the Armada Collective[66] are known criminal groups which use this method, although there are indications that other criminals make use of these names to reinforce the threat of a DDoS attack.[67][68]

Furthermore, it was also observed in the reporting period that criminals extort individuals with stolen data from digital attacks. This is, for example, what happened after the hack on the customer base of the Ashley Madison site.[69] People from the customer base were then approached by the criminals.[70] Organisations, too, are sometimes extorted with stolen data from digital attacks.[71] In the past period, the criminal group Rex Mundi threatened, for example, to put the customer databases of various Dutch and Belgian organisations online if the organisations concerned refused to pay.[73][73]

## Existing revenue models remain in vogue among criminals

While there is a group of professional criminals who, with a high degree of organisation, carry out sophisticated campaigns, existing revenue models are still in use.[74] This can be observed in both ransomware and in other types of criminal malware, such as banking malware. The use of this latter form of malware is decreasing in the Netherlands.[75]

Sometimes malware source codes are (intentionally or unintentionally) made public, making it possible for criminals to adjust this to their own needs. The result is that multiple versions of the original malware quickly appear.[76][77] In addition, it is becoming more common that criminals can adapt their malware for specific targeted attacks: thus, they model their attacks more often to their intended victim.[78]

The level of expertise and skills of criminals is extremely varied. There are specialists who are characterized by a high level of professionalism and innovative capacity. Through the professional services sector that has originated for digital crime in recent years, there is also an ever-growing group of active criminals with a relatively low level of expertise and skills.[79] The CSAN 2014 and 2015 already argued that it is no longer necessary for a criminal to possess digital skills in order to carry out digital attacks.

The fact that cybercrime-as-a-service is becoming increasingly professional and customer-friendly has become clear again in the past period through the appearance of various types of ransomware-as-a-service,[80][81] malware instruction videos on YouTube[82] and ransomware codes on GitHub.[83] This adds to the ease with which criminals without specific knowledge and skills can use malware and ransomware against their victims.

## The tracking down of criminals remains a challenge

Dutch hosting remains popular among cybercriminals. In 2015, the police and the Public Prosecution Service observed that the number of IP addresses on which they must act on the basis of international requests for assistance, increased from 214 in 2014 to 383 in 2015.[84] Also, various anonymisation techniques are gaining popularity among criminals. In this way, they try to keep criminal activities, communication and money flows out of sight of the investigative services. Criminal forums are often posted behind proxies and DDoS protection services, to hide the actual location of servers.[85] The police note that command & control servers used in, for example, ransomware campaigns are placed in the Tor network in order to be untraceable. In addition, the use of so-called bitcoin mixers is gaining in popularity: services that try to anonymise bitcoin funds even further by changing them. In this way, the traces of the virtual money and the senders and receivers of transactions cannot be discovered.

In addition to this, illegal bitcoin changers can, via ads on underground market places, be brought in at a high rate (8-12 percent instead of about 0.5 percent at bona fide changers) to anonymously withdraw money at an agreed time and place. In January 2016, the FIOD dismantled a criminal network with multiple bitcoin changers. In March 2016, the police also arrested a bitcoin changer who was laundering what was probably millions of euros of bitcoins in this way.

It is clear that there is a large, global, anonymous market for digital crime. However, the local police are also increasingly seeing locally formed, physical partnerships. Instead of maintaining only remote contact via (anonymous) digital channels, some criminals certainly do have contact with each other; they know each other and get together for some of the targeted operations. A well-known example is the Dyre malware campaign, for which a criminal group was housed together in an office building in Russia.[86]

### Marketplaces for cybercrime-as-a-service

Standard solutions for performing cybercrime are continuously being developed and resold. This reselling is called commodification. Campaigns or operations are often carried out by ad hoc coalitions of specialists.[87] Larger and knowledgeable coalitions keep, as much as possible, a grip on the entire operation.[88]

Underground market places are still used to exchange or trade tools for committing cybercrime.[89] They use hidden services, so as to hamper detection.

Services offered include ready-to-use malware, stolen credit card information, social media and e-mail account information, DDoS attacks (DDoS-as-a-service), RATs and online manuals for committing cybercrime.

Reliability and quality are seen as a competitive advantage. There are service providers with a help desk that offer support during office hours or even 24 hours a day.[90] They give the guarantee that the delivered data or products will live up to the expectations. To avoid scams, trusted intermediaries are also deployed who only release the money to the seller when the customer has indicated that he is satisfied.[91]

The Angler exploit kit possibly uses a model where a user is charged per successful malware installation.[92] Other exploit kits, such as Sweet Orange, seem to offer both a subscription service as well as the possibility to buy the kit for an unlimited period.[93] Exploit kits are sometimes also sold under certain conditions, for example that they may only be used for targeted attacks and not for wide phishing attacks.[94] Another condition is that they should not be used in countries where the service provider wants to stay under the radar.[95] The service provider may also demand a portion of the proceeds, such as 30 percent for CTB locker.[96]

## State actors

The greatest digital threat to national security comes from state actors, in particular from foreign intelligence services.[97] The Dutch government, national security and economy are threatened by the activities of these state actors. Digital attacks have become a real alternative to conventional (intelligence) tools because of the low cost, limited risk of failure and the high yields (in the amount of information).

The method is increasing in complexity, attackers are becoming more resourceful and are developing ever better ways to prevent the problem of identification and attribution. The Dutch intelligence and security services have observed, in the past period, structurally extensive espionage attacks aimed at Dutch government agencies, scientific institutes and companies in key sectors. States also use the military potential of the digital domain by deploying offensive cyber activities. This has not yet been specifically observed in the Netherlands.[98]

### States are investing in offensive cyber capabilities

As in previous years, states are investing heavily in developing their offensive digital capabilities.[99] It is often the intelligence services who harbour these capabilities and covertly deploy them. States have increasingly used digital attacks to achieve their strategic goals, to influence national or international conflicts and, in some cases, to support an armed struggle.

The military use of digital capabilities, digital attacks with the aim of tampering and manipulation of representation, is increasingly used to supplement conventional tools. Although the manifestations of such attacks hardly appear in public sources, it should be noted that some states carry out preparatory acts for collecting information, influencing the capacity for political and military operations or maintaining an infrastructure for future operations. This has not yet been observed in the Netherlands. Disturbing here are the exploration of critical infrastructure, the installation of malware to gain access for future operations, or investments in hacker collectives that make such acts possible.

### States are organising their cyber capabilities

The degree of organisation behind digital attacks by foreign state actors is often large; the division of labour and specialisation are in development. The Dutch intelligence and security services have, during several attacks, observed that various actor groups were involved in the implementation of digital attacks. For instance, it has been repeatedly established that the different stages of a digital attack were contracted out to various third parties. These parties specialise in needs determination, tool development, implementation or infrastructure management.

Infiltration, on the one hand, and exploration and evasion, the other hand, were also contracted out to various groups, also to private parties. The Dutch intelligence and security services have determined several times that employees of seemingly private IT companies carry out digital attacks or purchase and manage infrastructure on the instructions of foreign governments. These activities focus on Dutch government agencies, scientific institutes and companies in top sectors. This segmentation in the design and implementation of digital espionage encourages the specialisation and continuity (in the form of strike power) of digital attacks.

## Terrorists

As yet, in the digital field, still no concrete terrorist threat against national security has been observed. They have, thus far, never staged an attack (deadly or otherwise) with digital tools. They do, however, still cause social unrest with small-scale digital attacks for which little knowledge or skills are needed. These types of attacks have increased over the last period.

### Advanced digital capabilities of jihadists have not yet manifested themselves

Most terrorist threats come, at present, from jihadists and ISIS sympathisers. Although it was determined in the previous reporting period that the capabilities of jihadists in the digital field are growing, this has, so far, not yet manifested itself in large-scale or technically sophisticated attacks with a terrorist or jihadist motive.

Jihadists generally concentrate on hiding and encrypting their channels of communication. They often point out the importance of safety awareness to their supporters. They are also developing new applications and news forums[100 101 102] in order to spread their message further. In doing so, they seem to be looking for a balance between security and recruitment: instead of moving their communications completely to underground channels,[103] jihadists, for recruitment and propaganda purposes, benefit from having their message remain accessible to some degree for interested parties.[104 105]

Jihadists regularly claim that they have managed to obtain sensitive data via digital attacks. The data which they then make public are, however, in most cases still data that can be found on the internet,[106] or are the result of simple hacks which require little capacity and few resources.[107] These are, in particular, data from American soldiers and government employees,[108 109] but, in the past reporting period, they also published lists of European government employees,[110 111] including outdated information about Dutch citizens[112] Jihadists generally publish details of government employees, with the call to supporters to use this information for attacks. Thus far, it has not happened that personal data published by jihadists has been used to carry out attacks.

Although jihadists have the financial means and the intent to carry out digital attacks, it is clear from their previously carried out attacks that these attacks are not technically advanced yet and require little knowledge and manpower. Jihadists are trying to attract third parties to increase knowledge and capabilities in the field of digital attacks.[113]

Incidents or attacks are often a catalyst for online defacements by various parties, such as the digital responses to the attacks in Paris by both supporters of ISIS and supporters of Anonymous. In conflicts such as those in the Ukraine and the attacks in Paris, it is clear that ISIS sympathisers are more likely to focus on defacements, DDoS attacks and hacks of social media accounts.

The names 'Caliphate Cyber Army'[14 115] and 'Islamic Cyber Army'[116 117] recently seem to appear more prominently in digital attacks. Sometimes these names are used interchangeably.[118] Also, some names that are associated with jihadist digital attacks have announced that they plan to unite.[119] The identity of those behind these names is not known, nor is it known whether they are used by the same person or are interchangeable. Also, it is not known how many people are behind this, so that it is currently impossible to draw conclusions about the possible impact of these mergers. In June 2016, media reports were published which reported that attacks in the name of Cyber Caliphate and ISIS were carried out by parties allied to Russia.[120]

## Hacktivists

### Hacktivism increases during international conflicts

Hacktivists claim that they carry out digital attacks based on an ideological motive. Both their motives and their capabilities can be very diverse. In many cases, hacktivists carry out DDoS attacks on government targets,[121 122] media[123 124] and organisations.[125 126] The number of digital attacks by hacktivists increases during international conflicts and attacks. These activities have, thus far, had no major consequences for national security. It is possible that digital attacks and publications by hacktivists will generate media attention in the future.

Hacktivists have been focusing more recently on doxing. One example of doxing is the disclosure of Ku Klux Klan accounts by hacktivists.[127 128] Also, the names and login details of an Israeli defence organisation were hacked and released onto the internet.[129] Doxing by hacktivists is not yet common in the Netherlands.

### The capabilities of hacktivists vary

The capabilities of hacktivists are extremely varied. Sometimes attack techniques are used that require little knowledge and skills. Sometimes, the digital attacks are more sophisticated in nature, as with the compromising of sensitive business data.[130 131] Also, in the past period, cases of sabotage by hacktivists have been identified: in February, it was announced that unknown persons had hacked a NASA drone and tried to have it crash into the sea.[132]

Hacktivists are more active during international conflicts and attacks. After attacks, hacktivists often announce digital attacks against supporters of ISIS.[133 134] After the attacks in Paris and Brussels, this led to an increase in defacements and DDoS attacks on various sites, done by both hacktivistic persons and groups who use the name Anonymous, as well as Jihadist sympathisers.[135 136] These attacks had only a limited impact for the Netherlands.

### Anonymous as a digital threat

Anonymous is a loose and unorganised collection of individuals with varying interests who use the name 'Anonymous' for their digital activities. Anonymous is most commonly associated with digital activities of an activist nature. They often call for digital attacks on various organisations and bodies.[137] [138] Also, people under the name Anonymous sometimes make business or personal data public and call for physical protests.[139] [140]

However, the name Anonymous is not always associated with hacktivism. People who associate themselves with Anonymous often do this based on different motives. As a result, their objectives vary considerably and they have a wide variety of targets. While some people are actually ideologically motivated, others carry out actions 'just for fun.'

Because everyone is free to call themselves Anonymous, the name is used by parties and persons who stage digital attacks without ideological motives.[141] This was the case last year with the DDoS attack on Ziggo[142] and, presumably, during the attack on the Volkskrant.[143] In the media, there is often the incorrect image that Anonymous is a fixed group that carries out digital attacks with clear objectives. This image shows up, in particular, when people announce, on behalf of Anonymous, that they will deactivate social media accounts and websites of pro-jihadist parties.

The impact of digital attacks carried out under the name Anonymous differ as much as the motives and targets. Sometimes, it happens that attackers manage to shut down sites for a while. Also, the disclosure of personal data causes regular disruption to organisations and governments. The impact of the deactivation of social media accounts and websites of pro-jihadist parties is probably not particularly great: often, after they have been deactivated, people just set up a different account.

# Cyber vandals and script kiddies

## Growing threat through better availability of tools

The threat from cyber vandals and script kiddies is increasing. The reason for this increase is the growing availability of accessible tools for digital attacks. Cyber vandals and script kiddies carry out digital attacks as pranks, as a challenge, or to demonstrate their own capabilities. The police have also noted that suspected cyber vandals and script kiddies are often minors. The young suspects and their parents are often not aware of the damage done and the consequences[144] Cyber vandals have varying levels of knowledge. The knowledge level of script kiddies is usually low. Both of them carry out targeted as well as untargeted attacks.

It is becoming easier for cyber vandals and script kiddies to carry out DDoS attacks by using so-called booter services, which make it possible to carry out DDoS attacks via a website (DDoS-as-a-service). These services are easy to find on the internet and are easy to use. Thus, an effective attack can be carried out even with little money[145] and knowledge. Examples of this type of attack are the DDoS attacks on Ziggo[146] and de Volkskrant.[147]

One example of targeted attacks by cyber vandals and script kiddies were the hacks by the group 'Crackas with attitude' on the American heads of intelligence services John Brennan[148] and James Clapper[149]. After these hacks, data of CIA and FBI employees was posted on the internet. Later, a 16-year-old Brit was arrested for both hacks.[150] [151] Furthermore, online gaming platforms are always popular targets,[152] especially during the Christmas holidays.[153] [154] [155]

## Attribution of, in particular, DDoS attacks and defacements remains difficult

The distinction between cyber vandals, script kiddies, ISIS sympathisers and hacktivists is not always easy to make. With DDoS attacks and defacements, in particular, the responsibility for an attack is sometimes claimed by a specific party. However, the specified reasons are not always the real motivation behind the attack. A well-known example is the attack on the website of Malaysia Airlines in the previous reporting period, in which script kiddies pointed to ISIS.[156] This year, with the DDoS attacks on Ziggo and de Volkskrant, we saw references to Anonymous, a name that is usually associated with hacktivism.[157] There was also a severe DDoS attack on the BBC, carried out by a party that said it engages in anti-jihadist activities.[158]

The same attack is often claimed by several people or parties on different forums.[159] [160] The real reason for the attack then remains unclear.

# Internal actors

## Threat from internal actors remains stable

There is no indication that, during this period, the threat by internal actors has changed compared to previous years. This threat may come from malicious employees who, from financial, political or personal motives, deliberately manipulate systems or leak data. Threats by internal actors, however, can also come from unintentional actions and carelessness.

Although, in the recent period, some reports were published abroad about deliberate actions by internal actors,[161] [162] this was not such a problem in the Netherlands. In August 2015, an employee of a supermarket chain was sentenced because he had infected almost a hundred company laptops.[163]

The biggest internal threat in Dutch organisations, however, has been the result of oversight and human error. This ranged from employees who lost their (unsecured) data carriers to set-up errors, such that customer data could be accessed via the internet. For example, the Indian visa provider BSL enabled the data of Dutch applicants to leak out through a simple programming error.[164] A Dutch telecom shop unintentionally left login data of customer files on a screen, and it was then simple for a researcher to access them.[165] Via SQL injection, it was revealed that most of the staff of the European Space Agency used very weak passwords of, sometimes, only three characters long.[166]

# Cyber researchers

Cyber researchers look for vulnerabilities in IT environments for the purpose of exposing low levels of security. They often use the media to publish their findings and increase cybersecurity awareness. Publicity about the vulnerabilities can make organisations (temporarily) vulnerable because attackers can take advantage of the research findings. During the past reporting period, there was no significant threat observed in the Netherlands by Dutch publications about vulnerabilities.

In public and private areas in recent years, several agreements have been made with cyber researchers to share their research results more easily, without sacrificing the security of organisations. One result of these agreements are the guidelines that help organisations develop a practice of responsible disclosure in order to facilitate detectors and develop rapid solutions for vulnerabilities.[167]

## Bug bounty programme is gaining popularity

Also, there is a trend among organisations to observe the implementation of so-called bug bounties. These are rewards that, under certain conditions, are promised to researchers who uncover security vulnerabilities. This year, for example, the Pentagon[168] and General Motors[169] joined the bug bounty programme.[170] In the Netherlands, several companies make use of bug bounties, including several Dutch banks[171] [172] [173], Fox-IT[174] and Gamma[175].

Although cyber researchers continue to publish research from which malicious parties can benefit, both the guidelines to come to a practice of responsible disclosure and the bug bounty programme contribute to a gradual decrease in the threat from research publications.

# Private organisaties

Threats by private organisations may take three forms: organisations may affect the confidentiality of systems for financial gain, organisations can carry out cyber attacks in order to improve their competitive position and organisations can use the data they collect about their customers for commercial purposes or sell it to third parties. Carrying out digital attacks to improve one's competitive position usually falls under the heading of industrial espionage. There is no indication that the threat from private parties has changed compared to the previous reporting period.

During the past period, some cases of industrial espionage have been observed abroad. In the United States, for example, a supplier of linens confessed that the company's employees had hacked a competitor for financial gain.[176] Also, an employee of an American baseball team confessed to having hacked a database of a rival team.[177] Furthermore, it was revealed via the leaked documents from the compromised dating site Ashley Madison that management was able to infiltrate a competitive dating site.[178] In the Netherlands, there have not been any comparable cases thus far.

## Table 2 Actors and their intentions

| Actors | 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 |

## Personal data is an increasingly attractive target for various actors

In recent months, there have been several reports in the international media on the theft and/or publication of personal data. Often this involves data from public sources which can be found on the internet, but also data from protected databases are attractive targets for attackers. The targeted collecting and then placing on the internet of personal data without the consent of the owner is also known as 'doxing.' Although not all the collected data will always be released online, personal data form an attractive target for various actors.

- State actors are typically focused on personal data of government employees for suspected espionage purposes. In the media, there is the predominant image that a state actor is, for example, responsible for the hack on the United States Office of Personnel Management (OPM), during which the personal data of more than 21 million government employees were said to have been stolen.[179] The stolen data were never made public online. It is currently not known how exactly this data is being misused.
- Criminals collect data in order to attempt to exploit them for financial gain. Not only are personal and payment data popular products, but also medical data and account information. A previously mentioned example is the hack on Ashley Madison.[180]
- Jihadist groups regularly claim to have stolen sensitive data and personal data from government systems and then publish them on the internet. Often, however, this information is publicly available information which jihadist supporters may have obtained by performing targeted searches for government data on the internet.
- Hacktivists steal and publish personal and business information for ideological reasons. Although it is difficult to identify the real motives, publishing sensitive business or personal information is often accompanied by an ideological justification. Here, it is not certain whether this claim was the real reason for the data theft.

# Conclusion and looking ahead

Criminals and state actors are still the greatest digital threat to national security. Digital attacks carried out by these actors are the most sophisticated and tend to have the greatest impact on victims and society.

With state actors, there is an evolving division of labour and specialisation. The method is increasing in complexity, attackers are becoming more resourceful and are developing ever better ways to prevent the problem of identification and attribution.

The criminals' revenue models continue to be successful and have proved popular in the past year. Ransomware will be further expanded in the future and used in a more targeted manner. Here, hospitals and healthcare institutions are popular targets.

Besides the further development of existing business models, criminals are more often modelling their attacks to their intended victim. The past year has seen a number of major campaigns, proving that professional criminals are expanding their area of activity. Groups of professional criminals have a high degree of organisation and conduct sophisticated campaigns. Investments in such campaigns are high but this seems to be paying off: the proceeds from the known cases are high.

Jihadists still generate a lot of media attention with small-scale digital attacks which require little knowledge or skill. Although the digital capabilities of jihadists continue to grow, they have, thus far, never staged an attack with digital tools. The expectation is that (small-scale) attacks with jihadist motives will increase in number and that jihadists will become more involved in the publication of personal data.

Recently, hacktivists have been more focused on publishing sensitive business or personal information (without the consent of the owner). Theft and/or publication of personal data are, however, not only attractive for hacktivists. Also cyber vandals, script kiddies, criminals, jihadists and state actors focus, for various reasons, on stealing these data. This trend will continue in the future.

The threat from cyber vandals and script kiddies is increasing. The reason for this increase is, primarily, the growing availability of accessible tools for digital attacks. The availability and affordability of cybercrime-as-a-service also play a role here. As a result, an increasing number of people are able to carry out these attacks. It is expected that, in particular, DDoS attacks will increase in number.

In the area of internal actors and private organisations, there is no indication that the threat has changed compared to the previous reporting period. In these actors, as well, no new trends or phenomena have been observed which pose threats. Threats posed by cyber researchers will probably further decrease due to a number of trends.

## Notes

51 https://www.om.nl/vaste-onderdelen/zoeken/@94086/groot-crimineel/, consulted on 13 July 2016.
52 http://www.nrc.nl/next/2016/04/21/informatieschat-op-criminele-gsms-1614033, consulted on 13 July 2016.
53 https://www.europol.europa.eu/latest_news/iocta-2015-europol-annual-report-cybercrime-threat-landscape-published
54 http://arstechnica.com/security/2016/02/la-hospital-latest-victim-of-targeted-crypto-ransomware-attack/, consulted on 4 July 2016.
55 http://blog.trendmicro.com/trendlabs-security-intelligence/businesses-held-for-ransom-torrentlocker-and-cryptowall-change-tactics/, consulted on 4 July 2016.
56 Source: Fox-IT.
57 https://www.technologyreview.com/s/600838/hollywood-hospitals-run-in-with-ransomware-is-part-of-an-alarming-trend-in-cybercrime/, consulted on 4 July 2016.
58 http://arstechnica.com/security/2016/03/kentucky-hospital-hit-by-ransomware-attack/, consulted on 4 July 2016.
59 https://www.security.nl/posting/461521/Amerikaans+ziekenhuis+betaalt+17_000+dollar+aan+ransomware, consulted on 4 July 2016.
60 http://www.theregister.co.uk/2016/02/15/ransomware_scum_tear_up_tinsel_town_hospital_demand_record_36m/, consulted on 4 July 2016.
61 http://www.securityweek.com/cybercriminals-encrypt-website-databases-%E2%80%9Cransomweb%E2%80%9D-attacks, consulted on 4 July 2016.
62 https://www.security.nl/posting/464735/FBI+waarschuwt+voor+ransomware-aanval+die+back-ups+wist, consulted on 4 July 2016.
63 http://securityaffairs.co/wordpress/41775/cyber-crime/protonmail-paid-ransom-ddos.html, consulted on 4 July 2016.
64 http://www.computerweekly.com/news/4500246707/DD4B-cyber-extortion-gang-targets-key-European-sectors, consulted on 4 July 2016.
65 https://blogs.akamai.com/2015/05/dd4bc-escalates-attacks.html, consulted on 4 July 2016.
66 https://blogs.akamai.com/2015/11/operation-profile-armada-collective.html, consulted on 4 July 2016.
67 http://news.softpedia.com/news/unknown-copycat-using-armada-collective-name-for-ddos-for-bitcoin-extortions-497297.shtml, consulted on 4 July 2016.
68 http://www.securityweek.com/dd4bc-armada-collective-inspire-cyber-extortion-copycats, consulted on 4 July 2016.
69 See Chapter 1 for further explanation of the hack on Ashley Madison.
70 http://www.zdnet.be/nieuws/171086/hackers-chanteren-ashley-madison-gebruikers/, consulted on 4 July 2016.

71 http://tweakers.net/nieuws/104536/hackers-zetten-inloggegevens-van-bitdefender-klanten-online.html, consulted on 4 July 2016.
72 http://tweakers.net/nieuws/104290/rex-mundi-heeft-financiele-gegevens-duizenden-belgen-buitgemaakt.html, consulted on 4 July 2016.
73 http://nos.nl/op3/artikel/2011495-hacker-s-rex-mundi-al-drie-jaar-een-etterende-wond.html, consulted on 4 July 2016.
74 http://www.csoonline.com/article/2931535/data-leak/check-point-reports-explosion-in-unrecognizeable-malware.html, consulted on 4 July 2016.
75 Source: police.
76 https://www.security.nl/posting/434682/Bouwdoos+van+malware+die+Nederlandse+banken+aanviel+gelekt?channel=rss, consulted on 4 July 2016.
77 https://securityintelligence.com/tinba-worlds-smallest-malware-has-big-bag-of-nasty-tricks/, consulted on 4 July 2016.
78 Source: police.
79 Source: police.
80 Source: police.
81 http://arstechnica.com/security/2016/01/researchers-uncover-javascript-based-ransomware-as-service/, consulted on 4 July 2016.
82 https://www.security.nl/posting/438203/Organisatie+luidt+noodklok+over+malware-video%27s+op+YouTube, consulted on 4 July. 2016.
83 http://feeds.webwereld.nl/~r/Webwereld/~3/AzkSM1zMpU0/88019-open-source-ransomware-vrijelijk-beschikbaar-op-github, consulted on 4 July 2016.
84 Source: police.
85 Source: police.
86 http://tweakers.net/nieuws/108009/verspreiding-financiele-dyre-malware-gestopt-door-russische-autoriteiten.html, consulted on 4 July 2016.
87 Source: police.
88 Source: interview with Michel van Eeten.
89 https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report, consulted on 4 July 2016.
90 https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report, consulted on 4 July 2016.
91 https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report, consulted on 4 July 2016.
92 Source: police and https://blogs.sophos.com/2015/07/21/a-closer-look-at-the-angler-exploit-kit/, consulted on 4 July 2016.
93 http://www.drchaos.com/sweet-orange-web-exploit-kit/, consulted on 4 July 2016.
94 http://news.softpedia.com/news/New-MS-Word-Exploit-Kit-Adds-Statistics-Tool-to-Track-Success-of-the-Campaign-477568.shtml, consulted on 4 July 2016.
95 Source: police.
96 Source: police.
97 Source: AIVD and MIVD.
98 Source: AIVD and MIVD.
99 Source: AIVD and MIVD.
100 http://www.nytimes.com/2016/01/15/world/middleeast/a-news-agency-with-scoops-directly-from-isis-and-a-veneer-of-objectivity.html?_r=0, consulted on 4 July 2016.
101 http://www.mirror.co.uk/news/technology-science/technology/hidden-isis-android-app-lets-6203483, consulted on 4 July 2016.
102 http://securityaffairs.co/wordpress/24978/cyber-crime/al-qaeda-encryption-tools.html, consulted on 4 July 2016.
103 http://www.csoonline.com/article/3004648/security-awareness/after-paris-isis-moves-propaganda-machine-to-darknet.html, consulted on 4 July 2016.
104 http://www.tandfonline.com/doi/abs/10.1080/00396338.2016.1142085, consulted on 4 July 2016.
105 https://www.security.nl/posting/466258/Onderzoek%3A+terroristen+nauwelijks+aanwezig+op+Tor-netwerk, consulted on 4 July 2016.
106 http://www.thedailybeast.com/articles/2015/03/23/isis-hackers-googled-their-hit-list-troops-names-were-already-on-public-websites.html, consulted on 4 July 2016.
107 http://www.dataleakes.net/feds-charge-ardit-ferizi-aka-th3dir3ctory-with-creating-hit-list-of-american-military-govt-employees-for-isis/, consulted on 4 July 2016.
108 http://www.nu.nl/internet/4106100/zet-informatie-1400-amerikaanse-militairen-en-ambtenaren-online.html, consulted on 4 July 2016.
109 http://www.dataleakes.net/jihadist-leaks-addresses-of-army-sgt-dillard-johnson-navy-seal-rob-oneill/, consulted on 4 July 2016.
110 http://www.ubergizmo.com/2015/12/islamic-cyber-army-responds-to-isis-day-of-trolling/, consulted on 4 July 2016.
111 https://ent.siteintelgroup.com/Dark-Web-and-Cyber-Security/site-6-1-15-ishd-calls-for-attacks-on-10-italian-army-personnel.html, consulted on 4 July 2016.
112 http://www.telegraaf.nl/binnenland/26069079/__74_Nederlanders_op_dodenlijst_IS__.html
113 Source: AIVD and MIVD.
114 https://ent.siteintelgroup.com/index.php?option=com_customproperties&view=search&task=tag&tagId=787&Itemid=1355, consulted on 4 July 2016.
115 http://www.washingtontimes.com/news/2016/mar/15/islamic-state-hackers-post-kill-list-minnesota-cop/, consulted on 4 July 2016.
116 http://www.techworm.net/2015/09/isis-affiliates-to-launch-cyber-attacks-on-united-states-to-celebrate-911.html, consulted on 4 July 2016.
117 http://abcnews.go.com/US/fbi-warns-isis-inspired-cyber-attacks-911-anniversary/story?id=33684413, consulted on 4 July 2016.
118 SITE Intel Group, Pro-IS Hackers Forward Purported Info of Military Personnel Prominent Government Figures, 21 November 2015.
119 http://www.ibtimes.co.uk/isis-cyber-army-grows-strength-caliphate-hacking-groups-merge-telegram-1553326, consulted on 4 July 2016.
120 http://observer.com/2016/06/false-flags-the-kremlins-hidden-cyber-hand/, consulted on 4 July 2016.

121 http://www.nu.nl/internet/4173614/anonymous-hackt-ijslandse-overheidswebsites-walvisvangst.html, consulted on 4 July 2016.

122 http://spd.rss.ac/aHRocDovL25ld3Muc29mdHBlZGlhLmNvbS9uZXdzL2Fub255bW91cy10YWNrcy11cy1kZXBhcnRtZW50LW9mLWFncmljdWxodXJlLXRvLXByb3Rlc3QtYWdhaW5zdC1tb25zYW50obyooOTU4NTUuc2hobWw, consulted on 4 July 2016.

123 http://www.rcfp.org/browse-media-law-resources/news/online-attacks-against-media-websites-are-increasing-and-costly, consulted on 4 July 2016.

124 https://www.hackread.com/anonymous-ddos-zimbabwe-herald-website/, consulted on 4 July 2016.

125 http://www.scmagazineuk.com/anonymous-attacks-two-japanese-airports/article/447817/, consulted on 4 July 2016.

126 http://www.bbc.com/news/technology-35306206, consulted on 4 July 2016.

127 http://www.ibtimes.co.uk/anonymous-hackers-threaten-reveal-identities-1000-ku-klux-klan-members-opkkk-1525758, consulted on 4 July 2016.

128 http://www.nu.nl:80/internet/4157261/anonymous-begint-met-publiceren-namen-ku-klux-klanleden.html, consulted on 4 July 2016.

129 https://ent.siteintelgroup.com/Dark-Web-and-Cyber-Security/anonsec-allegedly-hacks-israel-missile-defense-association.html, consulted on 4 July 2016.

130 http://tweakers.net/nieuws/109245/hackers-stelen-gegevens-van-anti-ddos-dienstverlener-staminus.html, consulted on 4 July 2016.

131 https://www.theguardian.com/technology/2015/jul/06/hacking-team-hacked-firm-sold-spying-tools-to-repressive-regimes-documents-claim, consulted on 4 July 2016.

132 http://www.ibtimes.co.uk/nasa-hack-anonsec-attempts-crash-222m-drone-releases-secret-flight-videos-employee-data-1541254, consulted on 4 July 2016.

133 http://news.softpedia.com/news/anonymous-announces-payback-for-the-isis-paris-attacks-496184.shtml, consulted on 4 July 2016.

134 http://www.independent.co.uk/life-style/gadgets-and-tech/news/paris-attacks-anonymous-launches-its-biggest-operation-ever-against-isis-promises-to-hunt-down-a6735811.html, consulted on 4 July 2016.

135 http://www.eteknix.com/major-isis-messaging-forum-taken-anonymous/, consulted on 4 July 2016.

136 http://www.zdnet.com/article/isis-supporter-cyber-caliphate-takes-over-54000-twitter-accounts/#ftag=RSSbaffb68, consulted on 4 July 2016.

137 http://www.rtlz.nl/tech/anonymous-haalt-website-trump-offline-verspreid-geen-haat, consulted on 4 July 2016.

138 http://grapevine.is/news/2015/11/28/anonymous-shuts-down-almost-all-icelandic-govt-websites-for-13-hours/, consulted on 4 July 2016.

139 http://nos.nl/artikel/279137-anonymous-verklaart-de-oorlog-aan-wall-street.html, consulted on 4 July 2016.

140 http://edition.cnn.com/2015/11/06/europe/uk-anonymous-london-march/, consulted on 4 July 2016.

141 http://news.softpedia.com/news/anonymous-hacks-european-space-agency-just-for-fun-497551.shtml, consulted on 4 July 2016.

142 http://nos.nl/artikel/2052851-weer-urenlange-storing-bij-ziggo-door-ddos-aanval.html, consulted on 4 July 2016.

143 http://www.volkskrant.nl/tech/volkskrant-nl-kort-uit-de-lucht-door-ddos-aanval~a4125596/, consulted on 4 July 2016.

144 Source: police.

145 See Table 2 for prices on underground market places.

146 http://www.volkskrant.nl/economie/ddos-aanval-op-ziggo-klanten-blijkt-letterlijk-kinderspel~a4158438/, consulted on 4 July 2016.

147 http://www.volkskrant.nl/tech/volkskrant-nl-kort-uit-de-lucht-door-ddos-aanval~a4125596/, consulted on 4 July 2016.

148 https://www.theguardian.com/technology/2015/oct/19/cia-director-john-brennan-email-hack-high-school-students, consulted on 4 July 2016.

149 http://www.theguardian.com/us-news/2016/jan/13/hacker-breaks-into-personal-email-of-us-director-of-national-intelligence, consulted on 12 July 2016.

150 https://www.washingtonpost.com/world/national-security/british-teen-arrested-in-hacking-of-top-us-intelligence-officials/2016/02/12/7b87351e-d1a5-11e5-b2bc-988409eee911b_story.html, consulted on 12 July 2016.

151 http://www.nu.nl/internet/4213760/britse-politie-arresteert-tiener-fbi-hack.html, consulted on 12 July 2016.

152 http://tweakers.net/nieuws/104593/dota-2-gametoernooi-tijdelijk-stilgelegd-vanwege-ddos-aanval.html, consulted on 12 July 2016.

153 http://news.softpedia.com/news/phantom-squad-starts-christmas-ddos-attacks-by-taking-down-ea-servers-498078.shtml, consulted on 12 July 2016.

154 http://www.csmonitor.com/World/Passcode/2015/1224/Lizard-Squad-plans-Christmas-Day-encore-with-Xbox-PlayStation-attacks, consulted on 12 July 2016.

155 http://www.engadget.com/2015/12/30/steams-christmas-privacy-issues-affected-34-000-users/, consulted on 12 July 2016.

156 http://www.bloomberg.com/news/articles/2015-01-26/malaysia-air-website-hacked-with-phrase-isis-will-prevail-, consulted on 12 July 2016.

157 http://www.ad.nl/ad/nl/1012/Nederland/article/detail/4125550/2015/08/20/De-Volkskrant-getroffen-door-hackeraanval.dhtml, consulted on 12 July 2016.

158 http://www.bignewsnetwork.com/news/239915393/anti-isis-hackers-say-they-took-down-bbc-website-during-testing, consulted on 12 July 2016.

159 http://www.emerce.nl/nieuws/alleen-nederlanders-achter-aanval-ziggo, consulted on 12 July 2016.

160 http://www.techworm.net/2015/12/hacking-group-skidnp-takes-down-phantom-squads-website.html, consulted on 12 July 2016.

161 https://www.security.nl/posting/462079/Ontslagen+systeembeheerder+saboteert+fabriek, consulted on 12 July 2016.

162 http://www.newsobserver.com/news/business/article32944404.html, consulted on 12 July 2016.

163 https://www.security.nl/posting/440098/Jumbo-medewerker+hackte+bijna+honderd+bedrijfslaptops, consulted on 4 July 2016.

164 http://tweakers.net/nieuws/104706/indiase-visumverstrekker-bls-liet-gegevens-nederlandse-aanvragers-uitlekken.html, consulted on 4 July 2016.

165 http://sijmen.ruwhof.net/weblog/608-personal-data-of-dutch-telecom-providers-extremely-poorly-protected-how-i-could-access-12-million-records, consulted on 4 July 2016.

166 http://webwereld.nl/security/90837-esa-wachtwoorden-zo-simpel-als-123, consulted on 4 July 2016.

167 https://www.ncsc.nl/actueel/nieuwsberichten/leidraad-responsible-disclosure.html

168 http://www.wired.co.uk/news/archive/2016-03/02/hack-the-pentagon-bug-bounty, consulted on 4 July 2016.

169 https://hackerone.com/gm

170 https://hackerone.com/internet-bug-bounty

171 https://hackerone.com/abnamro

172 https://hackerone.com/dnb_nl

173 https://hackerone.com/ing

174 https://hackerone.com/foxit

175 https://hackerone.com/gammanl

176 https://www.security.nl/posting/453200/IT-directeur+Amerikaans+bedrijf+hackte+server+concurrent, consulted on 4 July 2016.

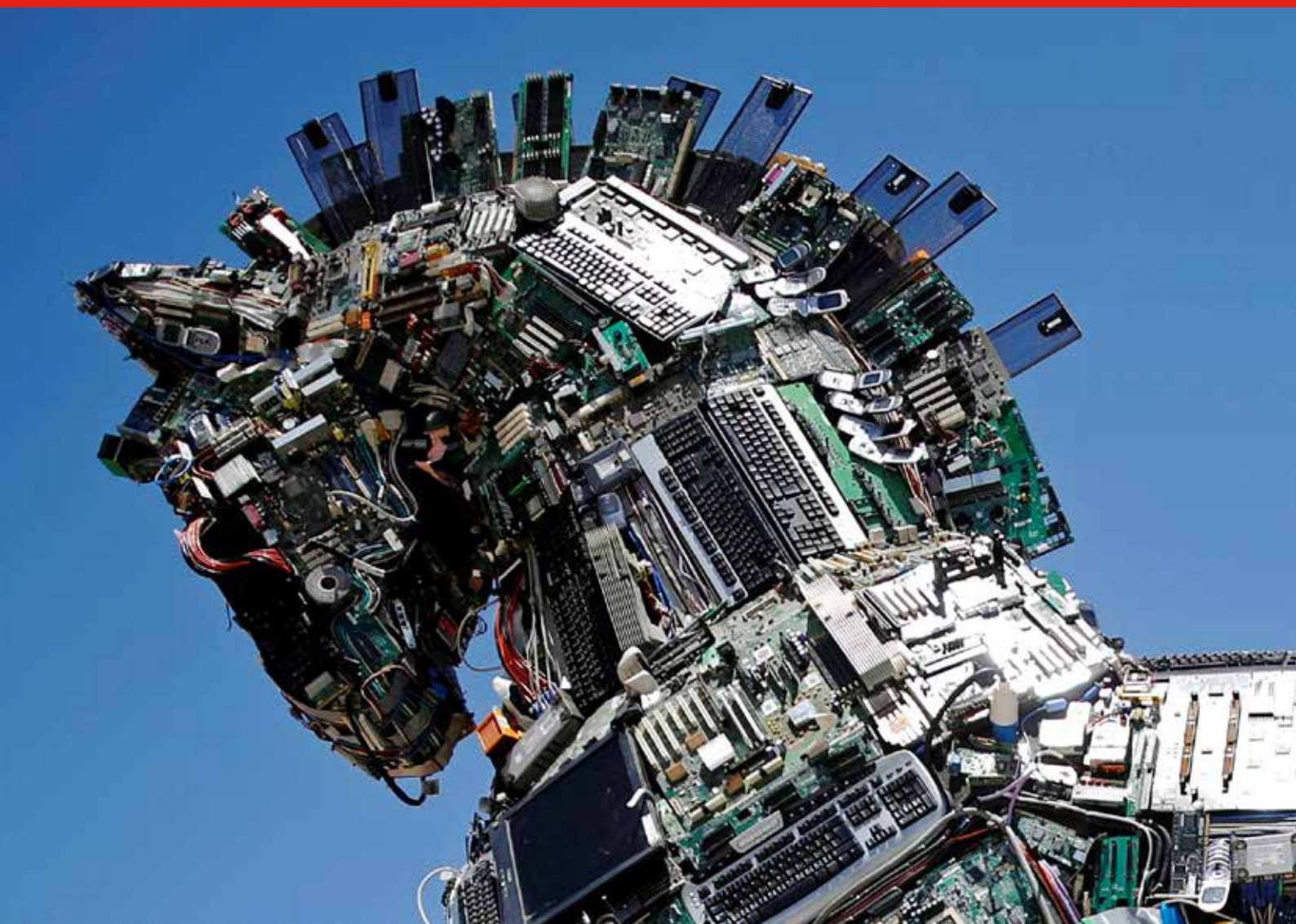
177 https://nakedsecurity.sophos.com/2016/01/12/ex-cardinals-exec-yes-i-hacked-rival-astros-database/, consulted on 4 July 2016.

178 http://krebsonsecurity.com/2015/08/leaked-ashleymadison-emails-suggest-execs-hacked-competitors/, consulted on 4 July 2016.

179 https://www.washingtonpost.com/news/the-switch/wp/2015/07/15/the-opm-leak-exposed-more-than-a-million-fingerprints-heres-why-that-terrible-news/, consulted on 4 July 2016.

180 http://www.zdnet.be/nieuws/171086/hackers-chanteren-ashley-madison-gebruikers/, consulted on 4 July 2016.

*Advertising networks have not yet shown the ability to cope with malvertising*



# 3 Threats: Tools

**Actors continue to expand the effectiveness of existing tools. For instance, makers of ransomware are continually increasing the pressure they put on victims. Malware and communications by malware can be hidden better and better. The amount of new malware for mobile platforms is also increasing. Actors try to infect trusted sources and advertising networks in order to be able to spread malware. The development of ready-made resources and cybercrime-as-a-service is continuing.**

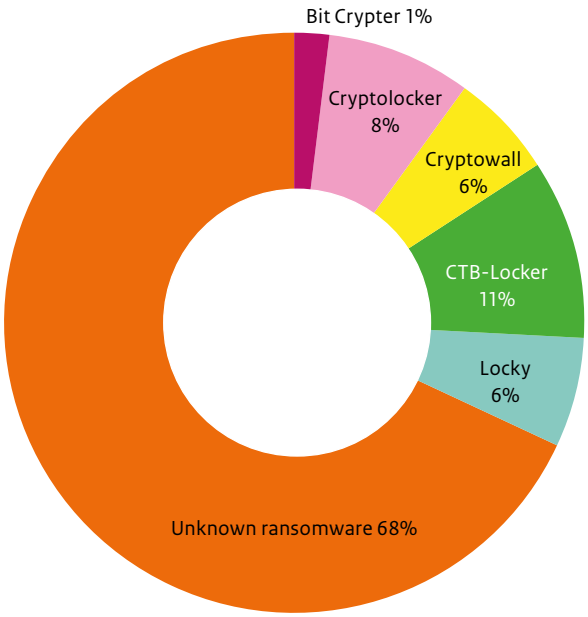
When carrying out digital attacks, actors make use of tools to exploit or enhance vulnerabilities. This chapter discusses these tools and the methods used.

## Malware

### Ransomware remains a major problem

In the CSAN 2015, ransomware was already referred to as a growing problem. The further development and dissemination of ransomware is continuing. New variants of ransomware appear frequently and the proceeds that criminals are able to generate are high. In almost all cases, all of the victim's files are encrypted and thus made inaccessible. Only if the victim pays is the encryption undone. In exceptional cases, the victims get lucky. Sometimes, the key can be retrieved by an implementation error in the encryption or by rounding up the infrastructure of the cryptoware. Then the files can be decrypted free of charge. In the Netherlands, too, developers of cryptoware have proven to be active. For example, two Dutch citizens were arrested who were suspected of making and distributing the Coinvault cryptoware.[181]

Figure 1 **Reports of ransomware in the Netherlands**[182]



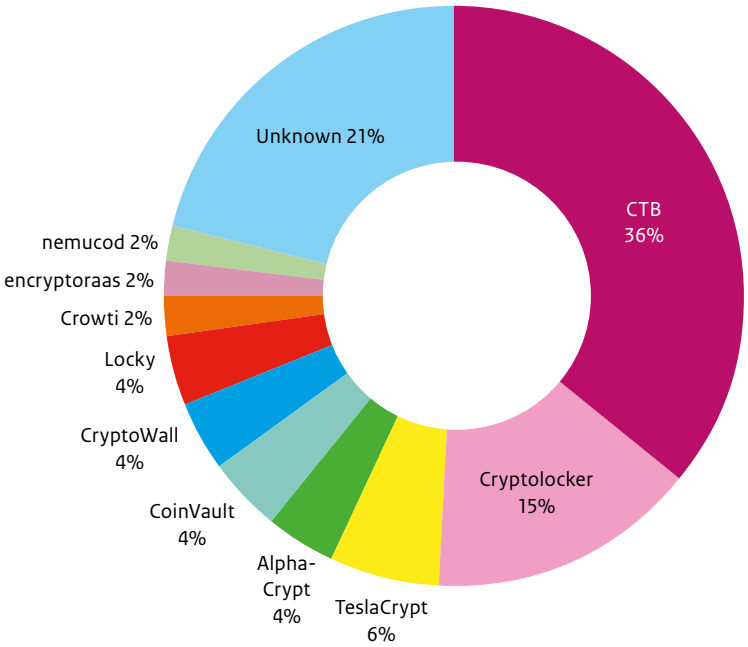

**Source: police.**

Ransomware is affecting an increasing number of platforms that had previously not been bothered by it. For example, Mac OS X, is now affected by the KeRanger ransomware.[183] As more everyday devices become equipped with processors and connectivity, the risk of a ransomware infection for such devices is increasing. For instance, the number of ransomware infections on Android is also increasing.[184] Symantec has conducted a proof-of-concept with ransomware that could infect a smart-watch via a smart-phone to which it was connected. [185] There is now also a proof-of-concept of ransomware that can infect smart TVs.[186]

Ransomware is not only used against end-users' systems but also directly against servers. This is done by exploiting vulnerabilities on those servers.[187] In this way, the server itself can be taken hostage. The server can also be used to gain a foothold within the network of an organisation. From there, further action can be taken.[188] In this way, the attacker can explore which (network) disks or files are the most valuable. These can later be encrypted. Then, the highest possible ransom can be demanded.[189]

As in previous years, in the past year, ransomware was found that encrypted backup files,[190] network drives and databases. Criminals also threatened to publish personal data if they were not paid.[191] It is unclear whether this actually happened.

Figure 2 **Ransomware infections reported to the NCSC**




**Source: NCSC. Period from January 2015 through April 2016.**

## Spreading malware by infecting trusted sources

If mobile device users install software solely from legitimate sources, such as the Apple, Google and Microsoft app stores, they run a lower risk of a virus or malware infection. Although checks are carried out, app stores are not free from malware. Actors try to spread malware by using the trust that users have in these channels.

A watering hole attack is an example of such a strategy. There are several methods to infect legitimate software with malware. First of all, the software vendor's website can be compromised. The malware is processed into the software offered on the website and then downloaded by users. Examples are the websites of Linux Mint[192] and Transmission[193]. Both were compromised and the software was distributed with malware. In some cases the software was also digitally signed with stolen secret key material. This enables the software to be trusted by the operating system.[194]

Another method is to infect development environments (integrated development environments, IDE) and compilers, which are used to make programs and apps to convert program code into system instructions. In China, infected copies of the Apple Xcode IDE have been disseminated. This version is known as XcodeGhost. All of the legitimate apps developed with this automatically had malware included. Thus, they could end up infected in the Apple App Store.[195] Ultimately, this affected dozens of apps that were used by a total of hundreds of millions of people worldwide.[196] More than 36,000 Dutch people are said to have been affected by one of the bogus apps.[197]

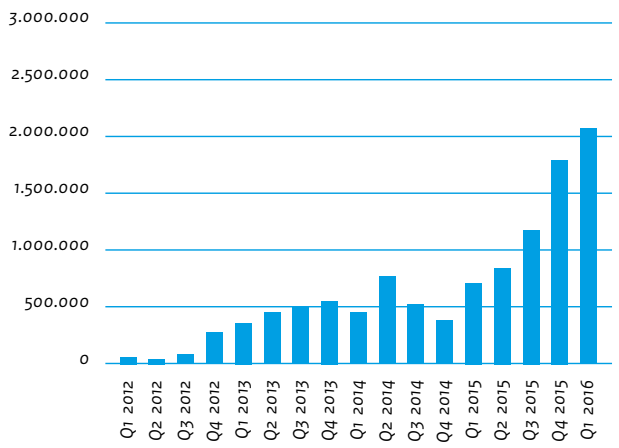
Finally, it is also possible that new equipment already has malware installed. This is a phenomenon that has been going on for many years and still occurs.[198] The infection can even occur at the manufacturer itself, or be caused by resellers who purposefully supply equipment with malware. This development was particularly visible in Android telephones and tablets from China.[199] Replica products, in particular, have an increased risk of malware infection.

## The amount of malware for mobile platforms is increasing

Mobile devices, such as smart phones and tablets, are taking an ever more central position in the daily lives of users. They are being used for an increasing number of (financial) activities. Many manufacturers of mobile devices often provide updates for only a limited period. This makes large groups of users vulnerable to newly found vulnerabilities.

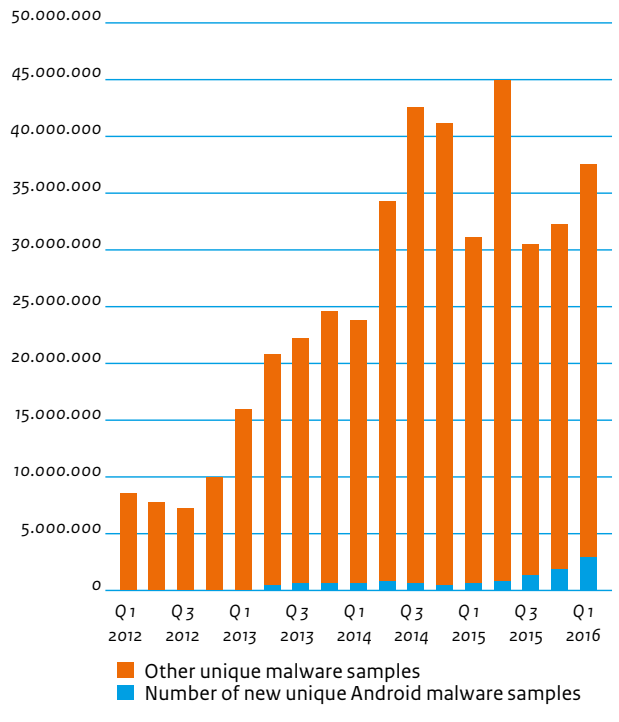
AV-Test's figures show that the number of new Android malware samples more than tripled in the period from January 2015 to March 2016. Also, the share of new Android malware within the total of new malware has more than tripled and now comes to 6.8 percent. This shows that the mobile platforms are an increasingly attractive target for malware. The growth of the number of unique malware samples for all platforms, including mobile platforms, fluctuated greatly in 2015. For example, a strong growth in the number of unique malware samples could be seen in the second quarter of 2015.

Figure 3 **Number of new unique Android malware samples**




**Source: AV-Test.**

Figure 4 **Number of new unique malware samples**




**Source: AV-Test.**

For the time being, it seems that infection of mobile devices mainly takes place via bogus apps in the alternative app stores, infection of jailbroken devices and infection of development environments (such as XcodeGhost). It is not known how most infections take place. A cause of infection can also lie within the relational sphere. An acquaintance then installs spyware on the device of someone he/she knows.[200]

## Although the amount of malware for iOS is relatively low, it is growing steadily

iOS systems remain generally resistant to malware, but the number of attack vectors used and the amount of malware targeting these systems is increasing[201] The biggest risk is when an iOS device is jailbroken by the user. As a result, apps from an untrusted source are allowed. Also, non-jailbroken iOS devices have, in the past, proved vulnerable. This development is continuing.

Earlier in this chapter, the use of a compromised version of Xcode was discussed. The apps developed with this had malware included that ultimately ended up in the Apple App Store. Another case involving malware that came with iOS apps was an ad-library that was used in many iOS apps. This made it possible to obtain sensitive information from the iOS device.[202]

In addition, there is misuse of the possibility for companies to install applications outside of the Apple App Store on iOS devices (enterprise provisioning). These apps are often signed with stolen digital certificates or certificates from less reliable developers. For infection, it is necessary that the user agrees with the installation of the application and connects the iOS device to a computer.

Another method used is the seducing of users to install a profile for mobile device management on an iOS system. Such a profile makes it possible to control iOS devices remotely within business environments. Attackers who manage to have the user install such a profile, can redirect network traffic to a system that is controlled by the attacker. The attacker can then install applications remotely.[203]

A new development is that malware can actively use vulnerabilities in iOS to install itself without an explicit user action on the iOS device being required. One example is the AceDeceiver malware. This still, by the way, requires a USB connection to an infected computer in order for the iOS device to be infected.[204]

With Android malware, the use of overlays is a more common means of stealing login information from users.[205] Users think they are using a legitimate app, but the malware steals the user's screen input.

# Tools

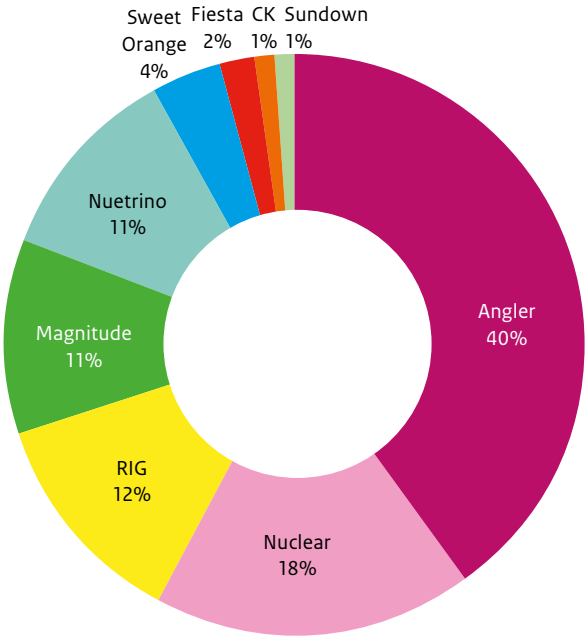
## Exploit kits continue to be developed

There are software developers who offer ready-to-use and user-friendly exploit kits to infect users with malware, such as the Angler exploit kit. Another well-known exploit kit is BlackEnergy. This is associated with disruptions at Ukrainian power plants.[206] There are not only exploit kits for regular computers, but also for devices such as routers.[207] Exploits for exploiting vulnerabilities can also be included with the exploit kit, but new exploits can also be purchased from a third party. 86 percent of the exploits that are used in exploit kits take advantage of a vulnerability in Flash Player.[208]

Exploits for vulnerabilities are traded on the internet, both on underground forums[209] and by commercial companies.[210] In particular, so-called zero-day vulnerabilities, vulnerabilities of which the public still is not aware, are traded for large amounts.

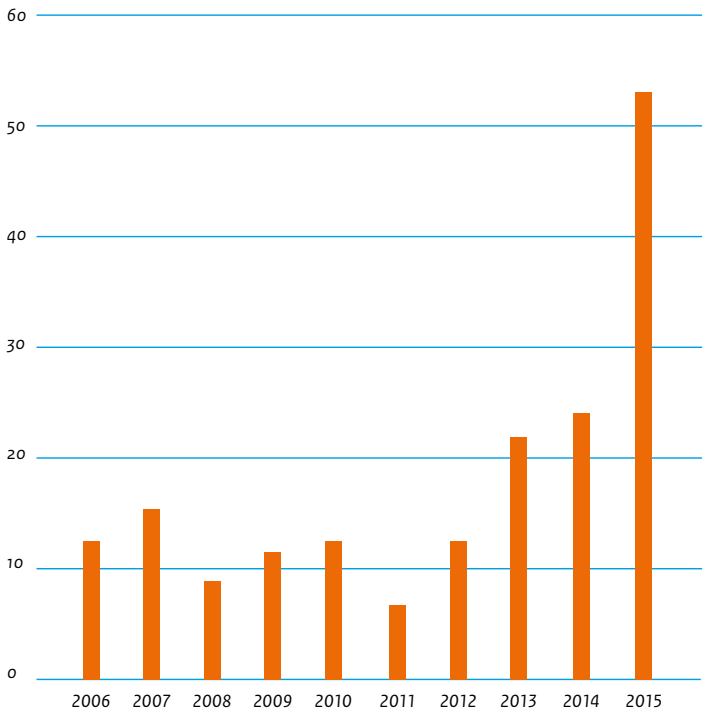
The number of published zero-day vulnerabilities rose sharply in 2015.[211] There is no clear explanation for this. When abuse of zero-days is detected and becomes known, an update generally becomes available. Of the 54 known zero-days in 2015, four Android, ten Adobe Flash Player, six Microsoft Windows, two Internet Explorer, two Microsoft Office and ten software for industrial control systems were affected. The other zero-days were for other software.[212]

Figure 5 **Share of various exploit kits in 2015**




Source: Trustwave.

Figure 6 **Total number of known zero-day exploits per year**




Source: Symantec.

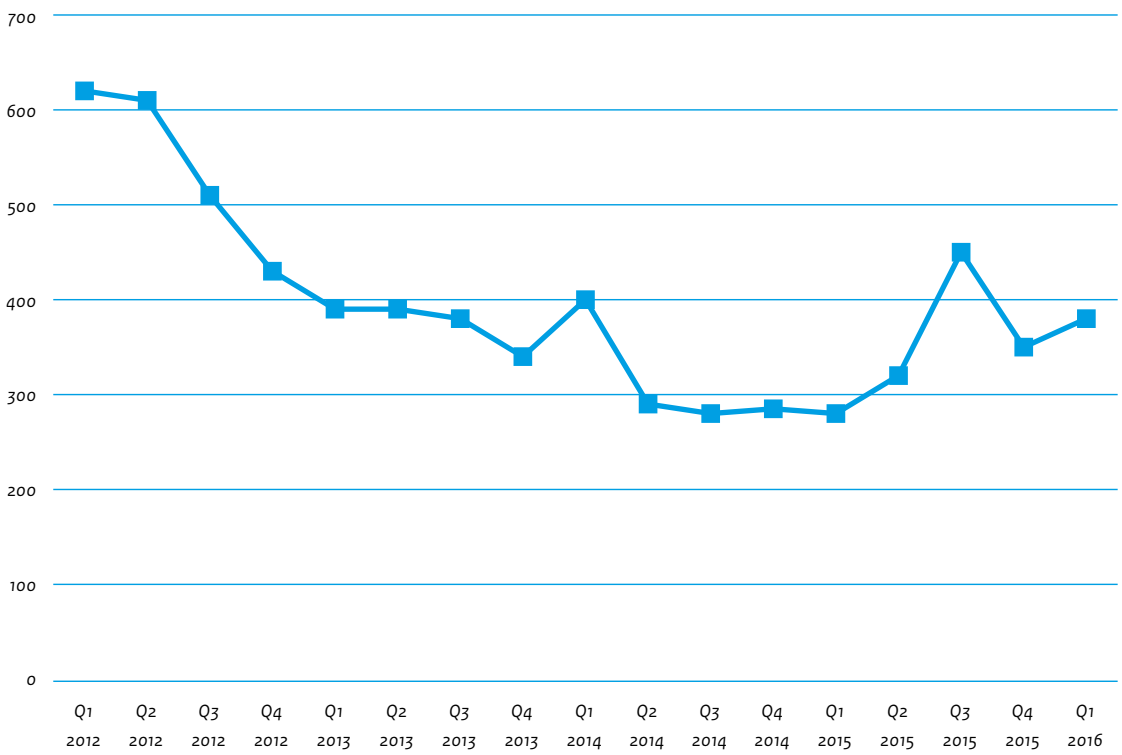
In addition to the above-named parties, there are parties that focus on the development of ransomware or a banking trojan to con money from victims. Other well-known alternatives are RATs. These allow for, among other things, information from the victim's system to be stolen.

The number of published exploits per quarter remained constant, after a strong decline in 2012. However, an upward trend is again observable in 2015.

## Remote Access Tools continue to be a popular tool for cybercrime

RATs remain a popular tool because of their wide applicability to enable different types of crime. Because an attacker takes over virtually all features a normal user also has available on the system, there are many attack possibilities. The development of RATs is continuing. For example, there are RATs that work on various operating systems without having to be adjusted.[213] A RAT can be purchased on underground market places starting for as little as $5.[214] RATs have, in the past year, once again proven to be an accessible and versatile tool for actors.

Figure 7 **Number of published exploits per quarter**




**Source: Exploit-DB.**

# Denial-of-Service attacks

## Attackers continue to discover new amplification methods

Attackers continue to discover new methods to make a DDoS attack as effective as possible by increasing the amount of data sent to the victim. The main method here is amplification. With this, attackers send out a small request to a service, with a forged sender address that is the same as the address of the victim. This is followed by a large-scale answer. The required level of knowledge and skills for an attacker is limited because of the number of accessible websites (booter services) that offer DDoS-as-a-service.[215] This trend from the previous CSAN is continuing.

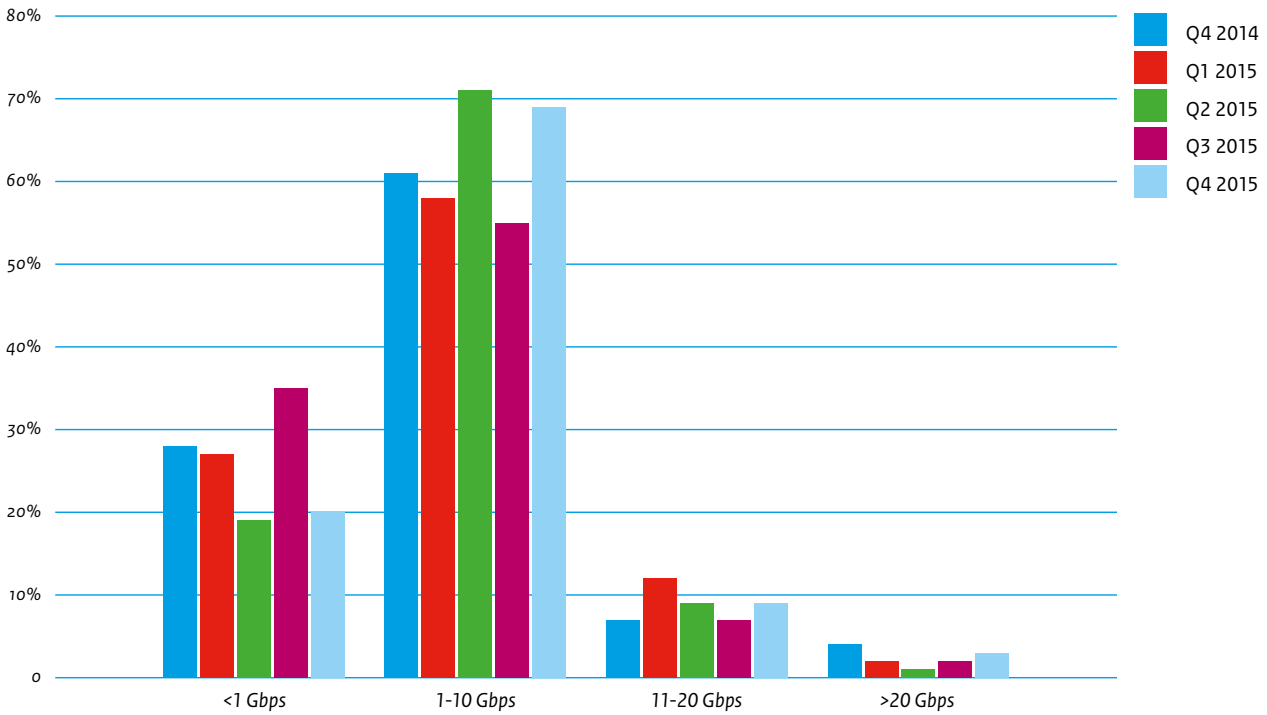
During the past year, as well, attackers have continued to search for new forms of amplification. Amplification attacks have been observed by abuse of NetBIOS, RPC, Sentinel[216], RPC Portmapper[217], DNSSEC[219], TFTP[219], Bittorrent[220]en RIPv1[221]. This shows that very different network services and associated protocols are susceptible to abuse. This includes services for file transfer, domain names and routing. Many of the abused protocols are not new. Attackers have found, in these old protocols, previously unknown possibilities to exploit them for amplification attacks.

Devices connected to the internet, such as routers, IP cameras, network hard drives and network printers are also misused to carry out DDoS attacks.[222] These devices are often taken over because the management system is accessible via the internet and lacks a strong password. At the same time, simply the fact that a service is available on such a device via the internet can be exploited to carry out an attack. With the increase of the number of (unmanaged) devices connected to the internet, this problem is likely to increase.

## Size, volume and duration of DDoS attacks are again breaking records

From reports of DDoS attacks worldwide, it appears that records have been broken again. The largest reported attacks involved 500 gigabits per second.[223] Attacks of this magnitude, however, remain exceptional. In addition to the extent of the attack, as expressed in gigabits per second, and the duration of the attack, it is the volume - the number of packets that is sent per second - that is relevant to the impact of the attack.[224] Processing large numbers of packets sometimes has a greater impact on routers and other network devices than the processing of an attack that is large in size and for which much bandwidth is required. Attacks with many packets per second require more memory in networking equipment. As a result, other connections are not set up or set up with a delay. The volume of DDoS attacks is expressed in millions of packets per second.

Figure 8 **Size of DDoS attacks**




**Source: National anti-DDoS Wash (NaWaS) of the National Management Organisation of Internet Providers (NBIP).**

Figures from the National Anti-DDoS Wash (NaWas) of the National Management Organisation of Internet Providers (NBIP) show that, with respect to the size of the attacks on the parties affiliated with them, the relative distribution has basically remained the same. The 1-10 Gbps range continues to represent the majority. Attacks of more than 20 Gbps remain an exception.

Most attacks on participants in the NaWas remain short-lived, less than fifteen minutes. In about 10 percent of the cases, the attacks last more than an hour. With respect to the volume of attacks on participants in the NaWas, no data is available.

# Obfuscation: hiding criminal activity

## Malware can be hidden increasingly better

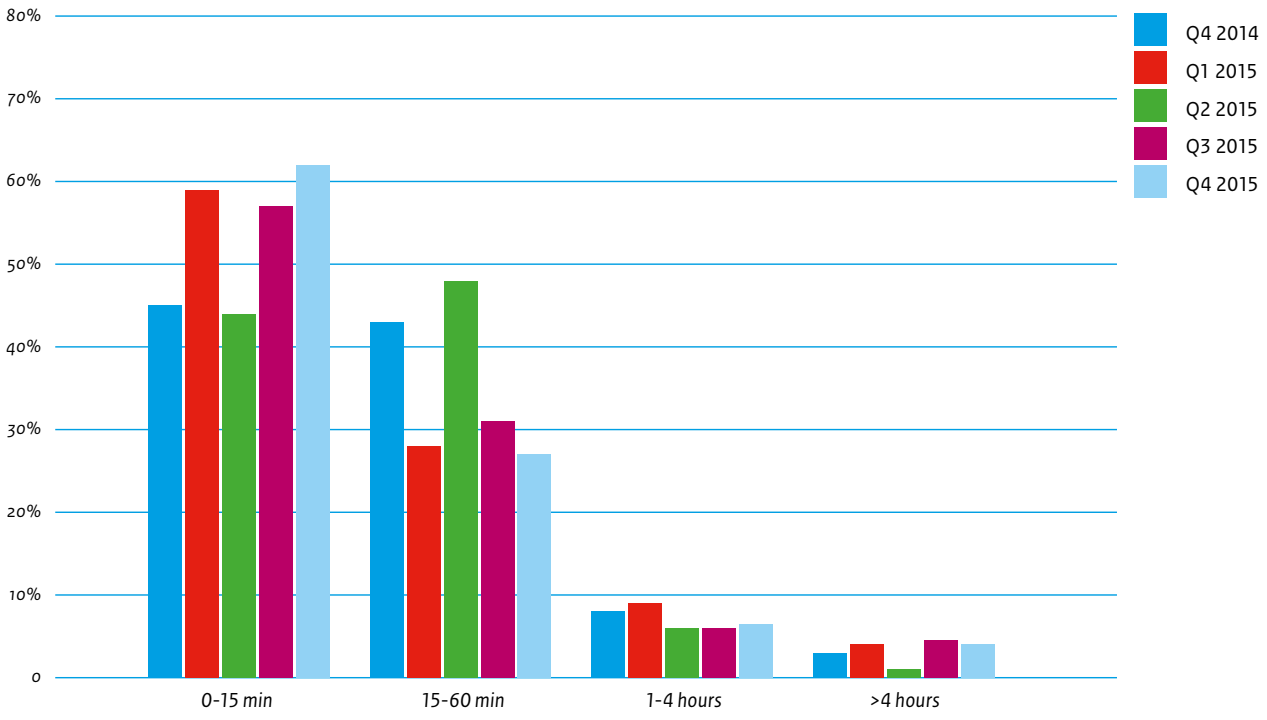
Attackers who want to use malware to steal information from the victim's system, have an interest in concealing this malware. This also applies to erasing all traces if the malware is, nonetheless, detected. Various techniques are used to achieve this goal.

The USBthief malware works only from the USB stick it was originally placed on. This malware leaves no traces on the compromised system.[225] The malware is encrypted with the hardwareID and disk properties of the USB stick. Because of this, it is, in principle, not readable without this USB stick. The file names of the malware files are also unique per USB stick. This complicates both detection and investigation by investigators.

The Cherry Picker malware, specifically designed for POS systems, is equipped with specific cleaner operations. That makes it possible to erase all traces of the malware once the purpose of the malware - collecting card information - is achieved.[226] In addition to this subtle approach, there is also malware that chooses, upon detection, to delete the entire hard drive and thereby erase all traces.[227] An alternative strategy is used by the creators of the Duqu 2.0 malware. Here, detection and leaving traces is prevented by having the malware be exclusively present in the working memory of the system and not having it make any changes to the system.[228]

Common firmware is an interesting target for attacks, such as the firmware of routers. Targeted attacks on firmware of (peripheral) equipment now seem to be used mainly by sophisticated criminal parties and state actors. It is important for the attacker here that the infection is not detected and remains intact after a reinstallation. Moreover, it is quite conceivable that this technology will also become available to other groups.[229]

Figure 9 **Duration of DDoS attacks**




**Source: National anti-DDoS Wash (NaWaS) of the National Management Organisation of Internet Providers (NBIP).**

### Malware infections of firmware

Firmware is software that is loaded into the memory of specific hardware and drives it directly, similar to an operating system for computers. This equipment, the hardware and the firmware loaded onto it, are closely connected with each other. One example is firmware for hard drives that actually takes over the saving of data onto the magnetic disk. Other examples include firmware for video cards, smart phones, smart watches, smart TVs, routers, IP cameras and mice. In the past, firmware could often only be loaded once by the manufacturer during production. Nowadays, it is often possible to update firmware at a later moment. Equipment now has increasingly more powerful processors and large amounts of memory, making it more possible for (parts of) full-fledged operating systems, Linux in particular, to be used as a basis for the firmware. This blurs the distinction between operating system and firmware and known vulnerabilities in the operating system can also affect many other types of devices, as well as computers. In this way, malware that was originally written for ordinary computers can also infect those other types of devices. The user often does not expect this. This could include, for example, cars[230] or industrial systems.

### Abuse of bona fide services remains popular

In the previous CSAN, abuse of services such as Dropbox, Pinterest and Google Docs for malicious purposes had already been brought to attention. The abuse of these services is attractive, because traffic to and from the services is often sent encrypted by default. Also, communication with the services is not in itself suspicious. Companies and organisations often do not block this traffic in advance.

This was also observed during the past period. Advanced criminal parties appear to use this technique. For instance, HAMERTOSS, the back door of a group that is called APT29, uses Twitter to mimic legitimate traffic and command-and-control (C2) to control the malware.[231] Also, Twitter Direct Messages can be used to control systems infected with malware.[232] Two Android malware families (OpFake and Marry) used Facebook as C2 infrastructure.[233] In addition, the alleged Chinese group admin@338 used Dropbox accounts as C2 infrastructure[234] and the Dridex malware exploited Pastebin for the storage of bogus VBScript that it uses in the attack process.[235]

The use of bona fide services offers attackers the advantage that users communicate with a trusted domain name. For instance, phishing attacks were carried out on Google accounts via Google Drive. That happened by copying a Google login page onto a Google Drive page.[236] This way, victims communicated with a real Google address (googledrive.com) and did not suspect any phishing. Also, technical measures can be circumvented in this way. For instance, a researcher circumvented restrictions in the Noscript Firefox extension by hosting the attack code in the Google Cloud. The googleapis.com domain is white-listed by default in this extension.[237]

Moreover, attackers also misuse well-known certificate authorities to legitimately obtain a certificate for their bogus services, for example for a phishing website.[238][239] For instance, certificates from the Let's Encrypt initiative, which aim to secure as many data connections as possible, can even be used to secure a phishing website.[240]

Finally, the TURLA group makes clandestine use of satellite communications in order to mask the location of C2 servers and to exfiltrate data. A great deal of satellite communication is sent unencrypted and may be received in a very large area. This allows a malicious person to hitch a ride on this signal so as to receive data without it being possible to establish the precise location of the malicious receiver. This makes it very hard to map out the C2 infrastructure and to find the perpetrators.[241]

Investigation services argue that the current special investigative powers, such as the interception and recording of communications, are barely effective anymore through encryption. For that reason, the Computer Crime III bill provides for the granting of the power to remotely infiltrate automated works under certain conditions, if a crime is committed.

## Attack vectors

### Malvertising remains a threat to internet users

Criminals continue to use malicious ads (malvertising) to infect internet users with malware. Many websites use advertising networks as agents for bringing together supply and demand of advertisers and websites, as well as the actual display of the ad. Due to the wide range of these advertising networks, they form an interesting channel for criminals to spread malware. Users with non-updated software are especially targeted.

Advertising networks have often been affected by malicious advertisements. As a result, websites with a global audience send malware to their visitors.[242] Together, these websites have more than two billion visitors per month and provide a large attack surface. Popular Dutch websites are also affected.[243]

Via real-time-bidding advertising networks, ads are shown to specific users (groups).[244] This method was also used during the previous reporting period. Additional techniques were deployed, such as fingerprinting.[245] With fingerprinting, the system of the possible victim is identified first. Malware (or a specific form thereof) is offered only after an assessment. In this way, malware is only offered to vulnerable systems. In addition, for example, malware is only supplied to computers with an IP address of an internet service provider for consumers. Also, the network packets can be used to determine which operating system the possible victim uses.[246]

All of these techniques together make it more cost efficient for the attackers to carry out such a campaign. In addition, it is becoming more difficult for researchers and advertising networks to trace current malware campaigns. For example, the malware is not offered to Linux machines and decoy systems, so-called honeypots.

Protection against malvertising is not easy. Spreading malware via the ads is possible because ads are purchased by large websites from advertising networks. These networks sell the ad space on a real-time basis and, because of the design of the advertising system, cannot check the ads for malware. When malware finds its way into the ads, systems that are not fully updated can be infected. Keeping systems up to date is, therefore, one method of combating infection by malvertising. Another measure is to use adblockers. This software blocks the ads as a whole. This has other disadvantages: ads are no longer shown to users, which affects the revenue model of websites.

## JavaScript used for malicious purposes

Popular Javascript libraries offer a lot of potential for attackers. All modern and popular web browsers support JavaScript. This creates a large attack surface with many users. At the same time, it is a powerful tool to add rich functionalities to websites. Simply turning off JavaScript support is, therefore, no solution.

Cloudflare described an example where Javascript libraries[247] and JavaScript in advertising networks[248] were used for implementing DDoS attacks. The past period, we see that JavaScript can be used for malicious purposes in several other ways. For instance, criminals tried to infect users' systems through JavaScript e-mail attachments.[249] On Github, a fully JavaScript-based bot appeared that can be controlled via Twitter.[250] In addition, it turns out that criminals also use JavaScript as droppers.[251] JavaScript is also used to find the identity of Chinese Tor and VPN users.[252] It is also used to attack the router of users and, for example, to change the DNS settings. As a result, traffic is intercepted and victims are sent towards phishing sites.[253]

## Use of stolen key material

One objective of digital certificates is to help the end user verify the authenticity of a source or service. When a service uses a trusted certificate in the correct manner, the application does not give any warnings to the end user: after all, the connection is trusted. If the certificate for the website is correct and has been issued by a trusted authority, it is more likely to create confidence in users, such as a green address bar in the browser.

Criminals try to exploit this trust in certificates by making their malicious activities look extremely trustworthy. In some cases, the criminals make use of stolen key material for the digital signing of malware, for example.[254][255][256] Allegedly, criminals sell such keys on the dark web for prices between 600 and 900 dollars.[258]

## Increase in misuse of open sources and social media

In the past reporting period, open information was misused more often. This involves information from previous incidents and doxing. This was the case, for example, when the data of 1,400 American soldiers and officials was placed online.[258]

Criminals are not only interested in information on social media. They also want to exploit these media. For instance, the Moose worm focused on home routers and other routers to break into communication with social networks. In this way, likes, views and followers are generated for accounts on these networks.[259] There is, possibly, money to be earned in this way.

## Phishing and spear phishing remain popular

Phishing campaigns remain a popular tool for stealing data of victims or infecting systems with malware. Phishing and spear phishing e-mails are getting better and better and ever more convincing. For instance, they use stolen name and address information to send personalised phishing e-mails. For receivers, phishing e-mail is often no longer distinguishable from legitimate e-mail from an organisation. The names and logos of many well-known large Dutch companies are exploited to mislead users.[260] For receivers, phishing e-mail is often no longer distinguishable from legitimate e-mail from an organisation. The names and logos of many well-known large Dutch companies are exploited to mislead users.[261] Also, in terms of tone, there is a similarity with the general communication of the relevant company in the given period.[262] In some cases, the communication style of the company during the presentation of quarterly results was analysed by criminals and copied to produce the most realistic phishing e-mail. The moment of the presentation of these figures was, moreover, seized by the criminals to carry out their phishing campaign.

# Conclusion and looking ahead

Ransomware continues to develop and remains an interesting tool for financial gain. Also, it is becoming more and more focused. For instance, there is filtering of the operating system users work with, as well as their location, IP address and software versions. In this way, actors also try to avoid detection by information security researchers.

The amount of malware on mobile devices is increasing sharply. It is expected that this trend will continue. Mobile devices are becoming increasingly important in everyday life and are used to carry out an increasing number of financial and other activities. This makes them increasingly interesting targets. Other everyday devices may, in future, also serve as attack vectors for, for example, ransomware.

Actors try to infect trusted software sources, such as app stores. This allows them to spread malware or to gain unauthorised access to the system that has been affected by it. The integrity of the entire product chain needs to be monitored in order to preserve the integrity of software and products and to prevent infections.

Malware can be hidden increasingly better and is now offered in a more focused manner in order to prevent (early) detection and keep a foothold in the system. As a result, actors remain under the radar as much as possible. The investments to exploit vulnerabilities in, for example, the firmware of peripheral and other equipment currently still seem high. As a result, it is not likely that there is large-scale exploitation. However, it does provide opportunities for highly targeted attacks against valuable targets.

Malvertising through advertising networks remains an effective method for disseminating malware using exploit kits. In the past period, this also affected popular Dutch websites. Because the method is so attractive to attackers, it is expected that this method of attack will continue to be used in the future.

New amplification methods will continue to further increase the effectiveness of DDoS attacks. In view of the large number of services and protocols to be exploited, it is expected that this trend will also continue in the future. The threshold for performing DDoS attacks remains low, so that, for example, young people use them against schools.

Finally, JavaScript continues to be used for malicious purposes. For it is supported by all modern and common browsers and, moreover, runs on the user's system. JavaScript thus offers the possibility to use the user's system directly for, for example, a DDoS attack. It also offers the opportunity to explore the user's system before any real malicious code is sent. It is expected that the number of methods for which JavaScript can be employed for malicious purposes will increase.

## Notes

181 https://www.politie.nl/nieuws/2015/september/16/11-cybercriminelen-aangehouden.html, consulted on 5 July 2016.

182 Source: police. Registrations in the period from May 2015 through April 2016.

183 http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/. For the Mac, there were already ransomware versions that exclusively blocked the browser, not the entire system itself. Through scams, they then tried to get money. https://blog.malwarebytes.org/exploits-2/2013/07/qa-about-the-latest-html-ransomware-affecting-mac-os-x-users/.

184 Source: police and http://www.welivesecurity.com/wp-content/uploads/2016/02/Rise_of_Android_Ransomware.pdf, consulted on 5 July 2016.

185 http://www.symantec.com/connect/blogs/dawn-ransomwear-how-ransomware-could-move-wearable-devices, consulted on 5 July 2016.

186 https://securityledger.com/2015/11/ransomware-works-on-smart-tvs-too/, consulted on 5 July 2016.

187 http://www.cio.com/article/3052553/server-software-poses-soft-target-for-ransomware.html#tk.rss_security, consulted on 5 July 2016. See also the Ransomweb, identified in CSAN 2015, which encrypts the database from a compromised web server. https://www.htbridge.com/blog/ransomweb_emerging_website_threat.html, consulted on 5 July 2016.

188 http://blog.talosintel.com/2016/04/jboss-backdoor.html, http://blog.talosintel.com/2016/03/samsam-ransomware.html, consulted on 5 July 2016.

189 Source: police.

190 https://blogs.technet.microsoft.com/mmpc/2016/03/17/no-mas-samas-whats-in-this-ransomwares-modus-operandi/, consulted on 5 July 2016.

191 https://www.secureworldexpo.com/new-ransomware-threatens-publish-personal-information, consulted on 5 July 2016.

192 http://blog.linuxmint.com/?p=2994, consulted on 5 July 2016.

193 http://researchcenter.paloaltonetworks.com/2016/03/new-os-x-ransomware-keranger-infected-transmission-bittorrent-client-installer/, consulted on 5 July 2016.

194 http://www.computerworld.com/article/3044728/security/cyberespionage-groups-are-stealing-digital-certificates-to-sign-malware.html, consulted on 5 July 2016.

195 https://blog.malwarebytes.org/mac/2015/09/xcodeghost-malware-infiltrates-app-store/, consulted on 5 July 2016.http://researchcenter.paloaltonetworks.com/2015/09/novel-malware-xcodeghost-modifies-xcode-infects-apple-ios-apps-and-hits-app-store/, consulted on 5 July 2016.

196 http://researchcenter.paloaltonetworks.com/2015/09/malware-xcodeghost-infects-39-ios-apps-including-wechat-affecting-hundreds-of-millions-of-users/, consulted on 5 July 2016.

197 http://www.rtlz.nl/tech/36000-nederlanders-downloadden-malware-app-app-store, consulted on 5 July 2016.

198 https://www.sophos.com/en-us/press-office/press-releases/2006/10/ipod-ships-with-virus.aspx, https://www.sophos.com/fr-fr/press-office/press-releases/2007/01/tomtom.aspx, consulted on 5 July 2016.

199 https://public.gdatasoftware.com/Presse/Publikationen/Malware_Reports/G_DATA_MobileMWR_Q2_2015_US.pdf, http://www.ibtimes.co.uk/amazon-selling-least-30-brands-cheap-chinese-android-tablets-infected-cloudsota-malware-1528442, consulted on 5 July 2016.

200 Source: police.

201 https://www.theiphonewiki.com/wiki/Malware_for_iOS, https://blog.fortinet.com/post/ios-malware-does-exist, consulted on 5 July 2016.

202 https://www.fireeye.com/blog/threat-research/2015/11/ibackdoor_high-risk.html, consulted on 5 July 2016.

203 http://www.theverge.com/2016/3/31/11336542/apple-corporate-iphone-security-sidestepper-attack-malware, consulted on 5 July 2016.

204 http://researchcenter.paloaltonetworks.com/2016/03/acedeceiver-first-ios-trojan-exploiting-apple-drm-design-flaws-to-infect-any-ios-device/, consulted on 5 July 2016.

205 https://securityintelligence.com/android-malware-about-to-get-worse-gm-bot-source-code-leaked/, consulted on 5 July 2016.

206 https://tweakers.net/nieuws/107138/stroomstoring-in-oekraine-werd-veroorzaakt-door-gerichte-inzet-malware.html

207 https://github.com/reverse-shell/routersploit, consulted on 5 July 2016.

208 https://www2.trustwave.com/rs/815-RFM-693/images/2016%20Trustwave%20Global%20Security%20Report.pdf

209 http://www.wired.com/2015/04/therealdeal-zero-day-exploits/, consulted on 5 July 2016.

210 http://betanews.com/2015/11/20/zerodium-reveals-price-list-for-zero-day-exploits/, consulted on 5 July 2016.

211 https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

212 https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

213 https://www.security.nl/posting/460316/Java-backdoor+besmet+440_000+computers+wereldwijd, consulted on 5 July 2016.

214 https://www.secureworks.com/resources/rp-2016-underground-hacker-marketplace-report, consulted on 5 July 2016.

215 See also CSAN 2015.

216 https://blogs.akamai.com/2015/10/netbios-rpc-portmap-and-sentinel-reflection-ddos-attacks.html, consulted on 5 July 2016.

217 http://blog.level3.com/security/a-new-ddos-reflection-attack-portmapper-an-early-warning-to-the-industry/, consulted on 5 July 2016.

218 https://www.stateoftheinternet.com/downloads/pdfs/2016-state-of-the-internet-threat-advisory-dnssec-ddos-amplification-attacks.pdf

219 http://researchrepository.napier.ac.uk/8746/, consulted on 5 July 2016.

220 http://arstechnica.com/security/2015/08/how-bittorrent-could-let-lone-ddos-attackers-bring-down-big-sites/, consulted on 5 July 2016.

221 https://blogs.akamai.com/2015/07/ripv1-reflection-ddos-making-a-comeback.html, consulted on 5 July 2016.

222 http://www.computerworld.com/article/2921559/malware-vulnerabilities/malware-infected-home-routers-used-to-launch-ddos-attacks.html, http://www.computerworld.com/article/2996079/internet-of-things/attackers-hijack-cctv-cameras-to-launch-ddos-attacks.html, consulted on 5 July 2016.

223 https://www.arbornetworks.com/images/documents/WISR2016_EN_Web.pdf

224 https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/2015-q3-cloud-security-report.pdf

225 http://www.welivesecurity.com/2016/03/23/new-self-protecting-usb-trojan-able-to-avoid-detection/, consulted on 5 July 2016.

226 https://www.trustwave.com/Resources/SpiderLabs-Blog/Shining-the-Spotlight-on-Cherry-Picker-PoS-Malware/, consulted on 5 July 2016.

227 http://blogs.cisco.com/security/talos/rombertik, consulted on 5 July 2016.

228 https://cdn.securelist.com/files/2015/06/The_Mystery_of_Duqu_2_0_a_sophisticated_cyberespionage_actor_returns.pdf

229 Virustotal.com, a website that analyses files in order to detect whether it is malware, has, since 2016, also offered the ability to monitor firmware. http://blog.virustotal.com/2016/01/putting-spotlight-on-firmware-malware_27.html.

230 http://money.cnn.com/2015/08/06/technology/tesla-hack/index.html, consulted on 5 July 2016.

231 https://www.fireeye.com/blog/threat-research/2015/07/hammertoss_stealthy.html, consulted on 5 July 2016.

232 https://github.com/PaulSec/twittor, consulted on 5 July 2016.

233 http://news.softpedia.com/news/two-mobile-banking-trojans-used-facebook-parse-as-c-c-server-497597.shtml, consulted on 5 July 2016.

234 http://news.softpedia.com/news/malware-that-hides-c-c-server-on-dropbox-detected-in-the-wild-496951.shtml, consulted on 5 July 2016.

235 https://blog.gdatasoftware.com/2015/06/24285-new-dridex-infection-vector-identified, consulted on 5 July 2016.

236 https://www.elastica.net/2015/07/elastica-cloud-threat-labs-discovered-latest-google-drive-phishing-campaign/, consulted on 5 July 2016.

237 http://labs.detectify.com/2015/06/30/using-google-cloud-to-bypass-noscript/, consulted on 5 July 2016.

238 http://news.netcraft.com/archives/2015/10/12/certificate-authorities-issue-hundreds-of-deceptive-ssl-certificates-to-fraudsters.html, consulted on 5 July 2016.

239 http://news.netcraft.com/archives/2015/10/13/fraudsters-use-paypal-office-com-ov-certificate-for-phishing.html, consulted on 5 July 2016.

240 http://www.infoworld.com/article/3019926/security/cyber-criminals-abusing-free-lets-encrypt-certificates.html , consulted on 5 July 2016.

241 https://securelist.com/blog/research/72081/satellite-turla-apt-command-and-control-in-the-sky/ , consulted on 5 July 2016.

242 https://www.security.nl/posting/464560/Advertenties+op+populaire+websites+verspreiden+ransomware , consulted on 5 July 2016.

243 https://blog.fox-it.com/2016/04/11/large-malvertising-campaign-hits-popular-dutch-websites/, consulted on 5 July 2016.

244 See also CSAN 2015.

245 https://blog.malwarebytes.org/threat-analysis/2016/03/ofp/, consulted on 5 July 2016.

246 http://www.pcworld.com/article/3030419/security/the-neutrino-exploit-kit-has-a-new-way-to-detect-security-researchers.html, consulted on 5 July 2016.

247 https://blog.cloudflare.com/an-introduction-to-javascript-based-ddos/, consulted on 5 July 2016.

248 https://blog.cloudflare.com/mobile-ad-networks-as-ddos-vectors/, consulted on 5 July 2016.

249 https://www.trustwave.com/Resources/SpiderLabs-Blog/Cryptowall-and-phishing-delivered-through-JavaScript-Attachments/, https://blogs.technet.microsoft.com/mmpc/2016/04/18/javascript-toting-spam-emails-what-should-you-know-and-how-to-avoid-them/, consulted on 5 July 2016.

250 https://github.com/Plazmaz/JSBN, consulted on 5 July 2016.

251 http://labs.bromium.com/2015/06/12/oh-look-javascript-droppers/, consulted on 5 July 2016.

252 https://www.alienvault.com/open-threat-exchange/blog/watering-holes-exploiting-jsonp-hijacking-to-track-users-in-china, consulted on 5 July 2016.

253 http://blog.trendmicro.com/trendlabs-security-intelligence/mobile-devices-used-to-execute-dns-malware-against-home-routers/, consulted on 5 July 2016..

254 http://www.theregister.co.uk/2015/06/15/duqu2_stolen_foxconn_cert/, consulted on 5 July 2016.

255 http://research.zscaler.com/2016/01/yet-another-signed-malware-spymel.html, consulted on 5 July 2016.

256 https://securityintelligence.com/certificates-as-a-service-code-signing-certs-become-popular-cybercrime-commodity/, consulted on 5 July 2016.

257 http://www.theregister.co.uk/2015/11/04/code_signing_malware/, consulted on 5 July 2016.

258 http://www.theguardian.com/world/2015/aug/13/isis-hacking-division-releases-details-of-1400-americans-and-urges-attacks, consulted on 5 July 2016.

259 http://www.welivesecurity.com/2015/05/26/dissecting-linuxmoose/ , consulted on 5 July 2016.

260 http://www.bbc.co.uk/news/technology-35996408, consulted on 5 July 2016.

261 See for a recent overview https://www.fraudehelpdesk.nl/sub-vragen/phishingmails/, consulted on 5 July 2016.

262 Source: interviews with various sectors.

*Security awareness among users cannot keep up with the development of social engineering*

# 4 Resilience: Vulnerabilities

**Vulnerabilities in software represent the Achilles' heel of digital security. Keeping all systems up to date is a challenge for both organisations and home users. At the same time, IT applications continue to grow and software vulnerabilities have an impact on the physical safety of users and public spaces, for example with vulnerabilities in the software in cars.**

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

### Lack of accountability of the chain makes IT vulnerable

The software industry seems to be developing more and more like an assembly industry[263] with, as a result, much re-use of existing components. Just as in the chain of aircraft construction, for example, it is desirable to have a number of things that can be precisely verified: where a part comes from, whether it is an original part (without modifications), where the part is used and what the state of repair is.

During the reporting period, there have been several incidents where this chain appeared vulnerable. A change in the NPM JavaScript Library (which is used by many web applications) deleted functionality that many of these applications were dependent on. This led those applications to suddenly stop working.[264]

In August 2015, vulnerabilities were discovered in pre-installed software on Lenovo products.[265] Lenovo made use of custom firmware which provided a clean Windows installation with Lenovo tools. After the discovery of a vulnerability, Lenovo decided to remove this mechanism. D-Link, a Taiwanese manufacturer, accidentally leaked a code-signing key online. This enabled malicious persons to provide software with a legitimate D-Link signature.[266]

It was also revealed that custom firmware with a back door for a number of Cisco routers was in circulation.[267] Juniper also announced that an internal audit revealed two serious problems in ScreenOS. These problems were said to have been introduced by an "unauthorised code" in ScreenOS which the company was not aware of.[268] Network equipment from these manufacturers is used almost everywhere in the world; attackers, therefore, have the potential to cause a great deal of damage.

### Security is not a core competence of software developers

Senior secondary vocational education courses and higher education degree programmes in software development pay little attention to software security.[269] Network security and platform security are mature professional competences; IT specialists who are trained to become software developers are assumed to have a basic knowledge of these forms of security. Software security, on the other hand, remains a subject confined to university education, specific programmes or electives that are taken only by IT students if they are interested in it.

Because this is a global phenomenon, there is no generally accepted standard that motivates developers to pay attention to it. Development organisations concentrate primarily on functionality and speed. This impasse means that software, upon completion, contains many vulnerabilities that can only be detected and remedied after the fact.

## Connectivity of industrial control systems is increasing

Industrial control systems (ICS)[270] are more often connected to IT networks and thus (directly or indirectly) to the internet. IT networks, however, often have a different, usually lower, confidence level with associated security measures than the level that has been set for the linked ICS. This can lead to situations in which these systems are vulnerable to attacks.

## Keeping all devices and software it up to date is a challenge

Many data breaches at companies are possible due to vulnerabilities that have been known for more than a year but have not yet been remedied by the affected organisation.[271] Many organisations, therefore, invest in a proper update policy, although some are still lagging behind. To update software on workstation PCs and servers, developers of operating systems now offer an increasing number of possibilities.[272] [273]

Many organisations use legacy systems, outdated systems for which no updates are issued. It is not always possible to modernise these systems or to set up a separate network for them. As a result, they remain vulnerable.[274] Devices other than computers are also not always equipped with a simple update mechanism. Organisations which allow employees, through a bring-your-own-device policy, to use their own smart phones and tablets to access corporate networks and information, cannot check whether users install updates on those (personal) devices. This complicates the control of vulnerabilities.

## Vulnerability to advanced threats is unknown

During investigations, it has been established by the intelligence services that the protection measures of many companies consist solely of the use of commercial anti-virus products. Many companies do not realise that attacks by sophisticated threats, such as state actors, go beyond the efforts of already known malware. These state actors commit frequent attacks in which they do not use files that are malicious in themselves,[275] but, through scans, these actors find vulnerabilities in systems which are then exploited.

Another trend is that foreign actors are increasingly focusing on social networks or the home environment of their targets. Where they previously used conventional methods for, for example, eavesdropping and tracking, now foreign actors are more focused on targeting digital tools. In recent years, there have been investments in detection within government and corporate networks, for example with the National Detection Network (NDN). Intelligence services have observed that, partly because of this, attackers have started focussing on networks that are less well-protected, such as home environments. In particular, the infection of mobile devices is popular; this provides access to various applications, but the phone itself can also act as a remote controllable microphone or camera. In intergovernmental organisations, several senior officials have been victims of such infections.[276]

## High-publicity vulnerabilities are commonplace

The previously identified trend of publicity campaigns surrounding technical vulnerabilities[277] is continuing.[278] Researchers establish a balance between creating sufficient awareness of a serious vulnerability, on the one hand, and the danger of exaggerating an everyday vulnerability, on the other hand.

The exaggeration of vulnerabilities can lead to the "Cry Wolf" effect.[279] Due to excess empty warnings, the attention can wane and one is no longer alert when something serious is going on. Badlock (see box) seems to have brought this risk to the attention of a broader public. The annoyance that has arisen from this may possibly be a reason to reconsider the marketing strategy that some security researchers apply.

### Badlock turns out not to be too bad

On 23 March 2016, the Badlock vulnerability was announced prior to publication on April 12.[280] The vulnerability was given a name, logo and website, but still no details were presented on the nature and severity of the vulnerability. It was only mentioned that the vulnerability was in SMB, a protocol to, among other things, share files over a local network that was used in Microsoft Windows and the open source software Samba.

System administrators took into account a serious vulnerability that had to be patched immediately at the time of publication.[281] After the details had been made known and updates had been published, security researchers were surprised: there was criticism on the hype that was created and the vulnerability was renamed Sadlock.[282] Although it was recognised that it was still a vulnerability that had to be taken seriously,[283] experts denounced the unnecessary deployment of manpower and the attention that this diverted from other, more serious vulnerabilities.[284]

# Developments on the users' side

## Mobile devices are often not provided with the latest updates

The market for smart phones and tablets is extremely innovative and competitive. Manufacturers therefore sometimes release new models several times a year, in order to stay ahead. This leads to a large number of different devices which, depending on when they were released, run on different versions of operating systems.

Because of the short period during which these devices are supplied by manufacturers, two years is the norm, many manufacturers quickly stop publishing updates for a particular older unit. Users of old devices can, therefore, no longer install updates. Software vulnerabilities are not repaired on those devices.

At the same time, there is a shift in internet use visible among home users. Originally, the PC or laptop was the preferred device in a household to use for internet access, but that role has now been taken over by tablets, smart phones and smart TVs.[285] The importance of keeping these other devices up to date is now, therefore, even greater.

## Awareness of users cannot keep up with the development of social engineering

Cybercriminals continue to improve their efforts to persuade users to perform actions. Users fall for phishing e-mails and telephone scams, although the percentage remains low in overall phishing campaigns. When social engineering is specifically focused on individual sectors, organisations or persons, this percentage increases significantly.[286] More targeted information is used to gain more trust from recipients, so that one victim within an organisation is often sufficient for attackers to achieve their goal.

Awareness campaigns for end users are mainly effective when they are aimed at changing behaviour in a specific situation. For instance, the campaign by the Dutch banks ('Hang op, klik weg, bel uw bank', 'Hang up, click close, call your bank) has been successful. This campaign has demonstrably contributed to behaviour change.[287] Campaigns conducted generically and aimed at recognising threats, such as phishing and social engineering in a broad sense, are less effective.

In this reporting period, there has been an increase in telephone scammers who try to convince victims that they have a problem with their computers. They are then persuaded to install some specific software. This is often malware, such as RATs, which allows a scammer to take control of the computer.

Initially, the scammers pretended to be Microsoft employees.[288] After many warnings were issued, the names of other organisations were also exploited for this purpose. In many cases, they used the names of telecom or internet service providers. Sometimes, they also spoke on behalf of a government agency.[289]

## Internet of Things is on the upswing and makes users physically vulnerable

The Internet of Things is no longer a prediction for the future. Many types of applications and devices are connected to the internet. Manufacturers seem insufficiently aware of the risks involved or lack the technical ability. That means that there are products on the market that still contain various software vulnerabilities.

Car manufacturers are now experiencing the problem of correcting software vulnerabilities. In the summer of 2015, the cars built by Ford, Range Rover, Toyota, Chrysler, Tesla and Chevrolet proved to be vulnerable.[290] Some models could not be automatically updated. In some cases, costly recalls were necessary. In September, Chrysler developed an update on a USB stick and sent it by mail to the car owners.[291]

This and other vulnerabilities in on-board computers of cars have a direct impact on road safety. Researchers have demonstrated that the brakes of a car can be controlled remotely. This can threaten the lives of the occupants if, for example, this happens on the highway.[292]

Many vulnerabilities can be prevented if security is given proper attention in the software development cycle. However, it remains necessary to have a good and safe update mechanism for future vulnerabilities. A recall can be extremely expensive. Sending a USB stick with a software update is no assurance that all users will also install it. In addition, criminals could exploit this. If the update is not digitally signed and is not verified, a criminal could, in the same way, send a malicious update to (specific) victims.

# Technical developments

## TLS remains the subject of vulnerabilities and measures

Transport Layer Security (TLS) is widely used in secure connections on the internet. The best known use of it is https, to allow website traffic to run through a secure connection. This ubiquitous use makes it, for security researchers, a prestigious action to discover vulnerabilities in TLS.

The reporting period again saw several new vulnerabilities and attack methods in TLS applications. The Drown vulnerability, in particular, was rather a sensation in March 2016.[293] With this, a server is exploited that offers the obsolete SSLv2 alongside of TLS. Although it has been recommended for years to disable SSLv2, several websites still appeared to be vulnerable to this attack method.[294] The chance that attacks based on Drown actually occur is limited, however, because of the complexity of the vulnerability.

### Adobe Flash Player allows for plenty of vulnerabilities, which have, as yet, not been resolved

In 2015, more than 330 vulnerabilities were repaired in Adobe Flash Player, including eight zero-day vulnerabilities.[295] The top ten most commonly used vulnerabilities by exploit kits is fully occupied by Flash Player.[296] Partly due to the advent of html5, which allows many features that were formerly developed in Flash to become available without plug-in in modern browsers, it seems that the raison d'être of Flash Player for playback of media is decreasing. The use of Flash Player for online games, for example via Facebook, however, is still popular due to the lack of alternatives.

On websites, the use of Flash is decreasing.[297] Popular websites such as Facebook[298] and YouTube[299] have switched to html5 to play videos. Also, Adobe itself is no longer focusing on the further development of Flash.[300] It is expected that, when the major browsers no longer offer Flash Player as a plug-in, the market penetration rate will decrease further. Flash will, however, not be disappearing yet. Online games and legacy software, among others, still rely on Flash.

### Malware is hidden in video cards and firmware

Detection of malware can be hindered by having parts of the malware run not in the ordinary memory of a computer, but in the firmware of peripherals and components within a computer. The techniques for this are advanced, and have mainly been demonstrated in the context of academic research. For instance, malware can be partially loaded into the video card of a computer system, so as to avoid detection.[301]

In addition, researchers have managed to install malware in the firmware of an lte modem[302], an SSD[303] and a hard drive[304]. This allows a malware infection to persist, even after reinstallation of the operating system. In the same way, vulnerabilities can be exploited in the firmware of standard computers, such as the BIOS[305] or its successor, UEFI.[306] Finally, firmware of routers can be infected, so that the malware does not disappear after a reboot.[307] Existing measures are often unable to detect this hidden malware.

### Reading out of memory via JavaScript: row hammering

Researchers have developed a proof-of-concept for a method to use JavaScript to manipulate the DRAM memory of a computer.[308] In order to do this, the row hammering attack technique is used, that allows sandboxing and other security mechanisms to be bypassed. In May 2016, researchers at the Vrije Universiteit in Amsterdam demonstrated[309] that this technique can be used on Windows 8.1 and higher to adapt memory blocks in a highly targeted manner. With this technique it is then possible to gain remote access to the system.

## Conclusion and looking ahead

The Netherlands is vulnerable to digital attacks. It is not always possible to trace the origin and safety level of software. Software is often unwittingly unsafely developed. As a result, they contain numerous vulnerabilities, while an increasing number of devices have software and are connected to the internet. Vulnerabilities in older software are not always resolved, which places challenges on organisations.

Large publicity campaigns for specific vulnerabilities create more awareness, but divert attention and give a distorted picture of the significant number of vulnerabilities that must be addressed annually. Due to the hype created around these high-publicity vulnerabilities, this trend may fade again in the long term.

End users have difficulty recognising fake e-mail and other forms of social engineering. Exploitation of this will continue to increase and awareness campaigns alone can no longer solve this. Additional measures are needed to enable users to protect themselves against attacks through social engineering.

The total vulnerability of the Netherlands continues to increase. This has to do with the increasing coupling of systems to the internet, in combination with the limited possibilities of software developers to develop safe software. Because software is penetrating into more and more devices as part of the Internet of Things, exploitation of software vulnerabilities will have an impact on the physical safety of users.

## Notes

263 https://vimeo.com/111043298, consulted on 13 April 2016.

264 http://www.theregister.co.uk/2016/03/23/npm_left_pad_chaos/, consulted on 26 May 2016.

265 http://www.theregister.co.uk/2015/08/12/lenovo_firmware_nasty/, consulted on 13 April 2016.

266 http://www.theregister.co.uk/2015/09/18/d_link_code_signing_key_leak/, consulted on 13 April 2016.

267 https://www.fireeye.com/blog/threat-research/2015/09/synful_knock_-_acis.html, consulted on 13 April 2016.

268 http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10713&cat=SIRT_1&actp=LIST, consulted on 13 April 2016.

269 Based on an assessment of competence lists for IT courses at senior secondary vocational education and higher professional education levels in the Netherlands.

270 The terms also include: process control systems, operational technology and SCADA systems.

271 Verizon 2016 Data Breach Investigations Report, http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf, consulted on 28 April 2016.

272 Microsoft Windows Update for Business, https://blogs.windows.com/windowsexperience/2015/05/04/announcing-windows-update-for-business/, consulted on 11 April 2016.

273 http://www.itwire.com/business-it-news/open-source/67655-linux-40-released-includes-live-patching, consulted on 11 April 2016.

274 Source: input to the NCSC from critical infrastructure organisations, see Appendix 2.

275 One (non-state) example is the threat "The PantomPantomPhantom Menace".

276 Source: AIVD and MIVD.

277 Cyber Security Assessment Netherlands 2015, https://www.ncsc.nl/binaries/content/documents/ncsc-nl/actueel/cybersecuritybeeld-nederland/cybersecuritybeeld-nederland-5/1/CSBN5.pdf, consulted on 12 April 2016.

278 https://www.security.nl/posting/465541/Update+voor+ernstig+lek+in+Samba+en+Windows+aangekondigd, consulted on 15 April 2016.

279 https://www.wodc.nl/onderzoeksdatabase/2056a-cry-wolf.aspx, consulted on 25 May 2016.

280 Badlock: "On April 12th, 2016, a crucial security bug in Windows and Samba will be disclosed. We call it: Badlock.", http://badlock.org/, consulted on 12 April 2016.

281 https://nakedsecurity.sophos.com/2016/04/12/badlock-revealed-probably-not-as-bad-as-you-thought/, consulted on 15 April 2016.

282 https://sadlock.org/, consulted on 15 April 2016.

283 https://labsblog.f-secure.com/2016/04/14/badlock-a-lateral-concern/, consulted on 15 April 2016.

284 https://www.trustwave.com/Resources/SpiderLabs-Blog/Microsoft-Patch-Tuesday,-April-2016/, consulted on 15 April 2016.

285 http://www.eenvoudigallesonline.nl/gebruik-van-mobiele-apparaten-in-nederland-de-cijfers/, consulted on 18 April 2016.

286 Source: input to the NCSC from the critical infrastructure, see Appendix 2.

287 Source: Dutch Payments Association.

288 https://www.fraudehelpdesk.nl/zoeken/antwoord/?antwoord_id=241&zoekopdracht=microsoft, consulted on 18 April 2016.

289 https://www.ncsc.nl/actueel/nieuwsberichten/wees-alert-op-social-engineering.html, consulted on 18 April 2016.

290 F-Secure Threat Report 2015, https://www.f-secure.com/documents/996508/1030743/Threat_Report_2015.pdf, consulted on 12 April 2016.

291 http://www.wired.com/2015/09/chrysler-gets-flak-patching-hack-via-mailed-usb/, consulted on 12 April 2016.

292 http://www.wired.com/2015/08/hackers-cut-corvettes-brakes-via-common-car-gadget/, consulted on 12 April 2016.

293 https://www.security.nl/posting/462943/Ernstige+kwetsbaarheid+in+ssl+raakt+33%25+https-servers, consulted on 18 April 2016.

294 http://www.rtlnieuws.nl/nieuws/binnenland/beveiliging-tientallen-gemeentesites-lek-persoonsgegevens-niet-veilig, consulted on 18 April 2016.

295 Common Vulnerabilities and Exposures, https://cve.mitre.org/, consulted on 7 January 2016.

296 NTT Group Global Threat Intelligence Report, https://www.solutionary.com/_assets/pdf/research/2016-gtir.pdf, consulted on 26 April 2016.

297 http://w3techs.com/technologies/details/cp-flash/all/all, consulted on 28 April 2016.

298 https://code.facebook.com/posts/159906447698921/why-we-chose-to-move-to-html5-video/, consulted on 11 April 2016.

299 http://youtube-eng.blogspot.com/2015/01/youtube-now-defaults-to-html5_27.html, consulted on 11 April 2016.

300 Welcome Adobe Animate CC, http://blogs.adobe.com/animate/welcome-adobe-animate-cc-a-new-era-for-flash-professional/, consulted on 11 April 2016.

301 http://www.securityweek.com/gpu-malware-not-difficult-detect-intel-security, consulted on 5 July 2016.

302 http://www.fiercecio.com/story/security-researchers-hide-malware-firmware-lte-modem/2015-08-10, consulted on 5 July 2016.

303 https://www.computable.nl/artikel/nieuws/security/5408780/250449/hackinggroep-herprogrammeert-ssd-firmware.html, consulted on 5 July 2016.

304 http://arstechnica.com/information-technology/2015/02/how-hackers-could-attack-hard-drives-to-create-a-pervasive-backdoor/, consulted on 5 July 2016.

305 http://www.wired.com/2015/03/researchers-uncover-way-hack-bios-undermine-secure-operating-systems/, consulted on 5 July 2016.

306 www.computerworld.com/article/2948177/malware-vulnerabilities/hacking-teams-malware-uses-uefi-rootkit-to-survive-os-reinstalls.html, http://www.securityweek.com/researchers-find-several-uefi-vulnerabilities, consulted on 5 July 2016.

307 http://news.softpedia.com/news/cisco-routers-infected-with-boot-resistant-malware-491835.shtml, consulted on 5 July 2016.

308 Rowhammer.js: A Remote Software-Induced Fault Attack in JavaScript, http://arxiv.org/pdf/1507.06955v1.pdf

309 http://www.cs.vu.nl/~kaveh/pubs/pdf/dedup-sp16.pdf

*Centralisation of IT services makes data easier to secure but more vulnerable to espionage*

# 5 Resilience: Measures

**The conscious use of technical and non-technical measures creates a stronger defensive position. Human beings are an important link in the security, but awareness seems to be at its peak. Cybersecurity has clearly found its place on the administrative agenda. That can be seen in many national and international measures.**

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

### Growing concerns about state actors

After the revelations by Snowden and the attack on Sony Pictures, an increasing number of people are concerned about attacks by state actors. Major parties, such as Facebook, Google and others, now warn users if they suspect that a user is being targeted by a state actor.[310]

In October 2015, the European Court of Justice declared the Safe Harbour framework invalid. This occurred after years of proceedings against Facebook by a group of users led by the Austrian Max Schrems. They argued that the revelations by Snowden showed that personal data of foreigners in the United States was insufficiently protected. This would demonstrate that the agreements in the Safe Harbour framework were not being complied with. The Safe Harbour framework, until then, formed the basis for most of the data exchanges between the European Union and the United States. On 12 July 2016, the European Commission adopted the EU-U.S. Privacy Shield.[311] This agreement between the EU and the U.S. is the successor to the Safe Harbour framework and aims to ensure adequate protection of personal data of persons in the EU that is stored in the U.S. With Privacy Shield, the Commission fulfils the requirements of the European Court of Justice that were declared invalid in the Safe Harbour framework with respect to the storage of personal data. Examples of these requirements are: obligations for companies that process data, guarantees concerning access by American investigative services to personal data, the possibility of arbitration and annual monitoring of the operation of Privacy Shield.

### Awareness-raising campaigns have varying degrees of effect

In the reporting period, there was again a great deal of attention for various awareness campaigns: European Cyber Security Month, Alert Online, 'Hang op, klik weg, bel uw bank' and Safer Internet Day. The Verizon Data Breach Investigations Report shows that awareness alone is certainly not enough. According to aggregated research, 30 percent of phishing e-mails are opened, 12 percent of people also open the attachment. This also happens very quickly; on average a receiver clicks on an attachment within four minutes after it is sent.[312]

### There threatens to be a shortage of cybersecurity professionals

The demand for cybersecurity professionals remains high. The Cyber Security Council (CSR) signalled that there threatens to be a major shortage of cybersecurity professionals. The CSR also noted that more attention should be paid to cybersecurity in general education. The CSR has advised the State Secretary of Security and Justice on this matter. [313]

### Tax and Customs Administration

The Tax and Customs Administration has a Security Operations Center (SOC). This SOC is responsible for the detection and investigation of vulnerabilities in the operational infrastructure, the interpretation of cyber threats and the advising of counter-measures to remove existing risks. During disasters, the SOC acts as the Computer Emergency Response Team of the Tax and Customs Administration.[314] In the reporting period:

- the office and data centre environment of the Tax and Customs Administration (more than 35,000 work stations and 5,600 servers) issued several reports via the internet. It concerned about 3,300 reports of viruses, 40 reports of hack and crack tools and over 4,700 reports of stopping malicious software;
- the first-line protection (firewalls) prevented nearly three billion attacks and the second-line protection (intrusion prevention facility) prevented more than 2.2 million attacks;
- there was a significant increase in the amount of incoming spam e-mails during the second half of 2015. This increase has continued into the first half of 2016;
- a large number of DDoS attacks have been observed. None of these attacks led to unavailability of information systems. The largest attack was 16 Gbit/s and took place in April 2016. There were 97 security incidents recorded of which four incidents were of the highest priority. The SOC examined all these security incidents and solved them, together with the relevant platform teams;
- 15 responsible disclosure reports were made, of which 12 were valid. All these reports were resolved. [315] In total, the Tax and Customs Administration awarded six cups. Two of these security incidents or vulnerabilities led to a possible breach of the integrity and confidentiality of the data managed by the Tax and Customs Administration. These incidents were reported in accordance with the law concerning the data breach reporting obligation;
- more than 7,100 reports were received of false Tax and Customs Administration e-mails. During this reporting period, the Tax and Customs Administration filed multiple reports against these phishing campaigns with the police;
- in collaboration with the NCSC and police, 32 phishing websites were dismantled. Of these, there were fifteen false DigiD websites.

# Technology

Although human beings are often considered to be the weakest link in the cybersecurity chain, technology is indispensable for guaranteeing cybersecurity. To stay safe, an aware user must also be supported by the correct, secure software. This section deals with the most important developments in this area over the past period.

To prevent long-term problems with legacy software, Microsoft has instigated a different strategy with Windows 10. Users of earlier versions of Windows automatically get a message that Windows 10 is available, free of charge. In addition, the default setting for Windows 10 is that updates will be installed automatically. Statistics show that the adoption of Windows 10 went faster than in previous versions of Windows, but Windows 7 still remains by far the most popular.[316]

In 2015, there were some incidents[317] [318] with pre-installed software on Windows machines which eavesdropped on, or even modified, traffic. In December 2015, Microsoft announced that it would block software that used man-in-the-middle techniques to display ads.[319] This measure started on 31 March 2016.

## Adoption of standards is increasing

The adoption of DNSSEC in the Netherlands and within the Central Government is still displaying a rising trend. In August 2015, 44 percent of the .nl-domains had DNSSEC. Within the Central Government, this was still 28 percent in the summer of 2015.[320]

Since the launch of internet.nl, many tests were carried out in the period from May 2015 through April 2016. Nearly 10,000 unique .nl-domains were tested. Of these, only 12 percent had a perfect score on the TLS test. Of the 2263 tested .nl-e-mail servers, 59 percent used SPF, 47 percent used DKIM and 18 percent used DMARC. Only 13 percent used all three measures.

From conversations with the various sectors, it appears that most companies recognise that digital security measures are needed. On average, the basic technical measures have also been taken. It is not always known whether these measures could be insufficient against targeted attacks.[321]

## Protection against malvertising by adblockers and patching

In an earlier chapter, we already discussed the fact that a significant part of malware infections occur through malvertising. The Netherlands Authority for Consumers & Markets (ACM) has pointed out this risk to the online advertising industry in the Netherlands. The ACM indicates that, if the risk becomes too great, a possible future advice would be to to use adblockers in order to protect end users.

In addition to adblockers, the updating of systems also offers protection against malvertising. Bogus ads use vulnerabilities in software to infect systems. If systems are equipped with the latest updates, bogus ads that use known vulnerabilities, can no longer infect these systems.

The large-scale use of adblockers can impact the revenue model of various websites. Adblockers have been available since the rise of pop-up ads in the 1990s. Especially the more tech savvy home users, used these adblockers. Thus, they had visually quieter pages and wanted to combat the privacy-unfriendly behaviour of the advertising industry.

Within the consulted sectors, a small number of companies are already installing adblockers for security reasons. For a number of other companies, this was not standard practice, certainly not in the security departments. They are, however, strongly advised to install adblockers themselves.

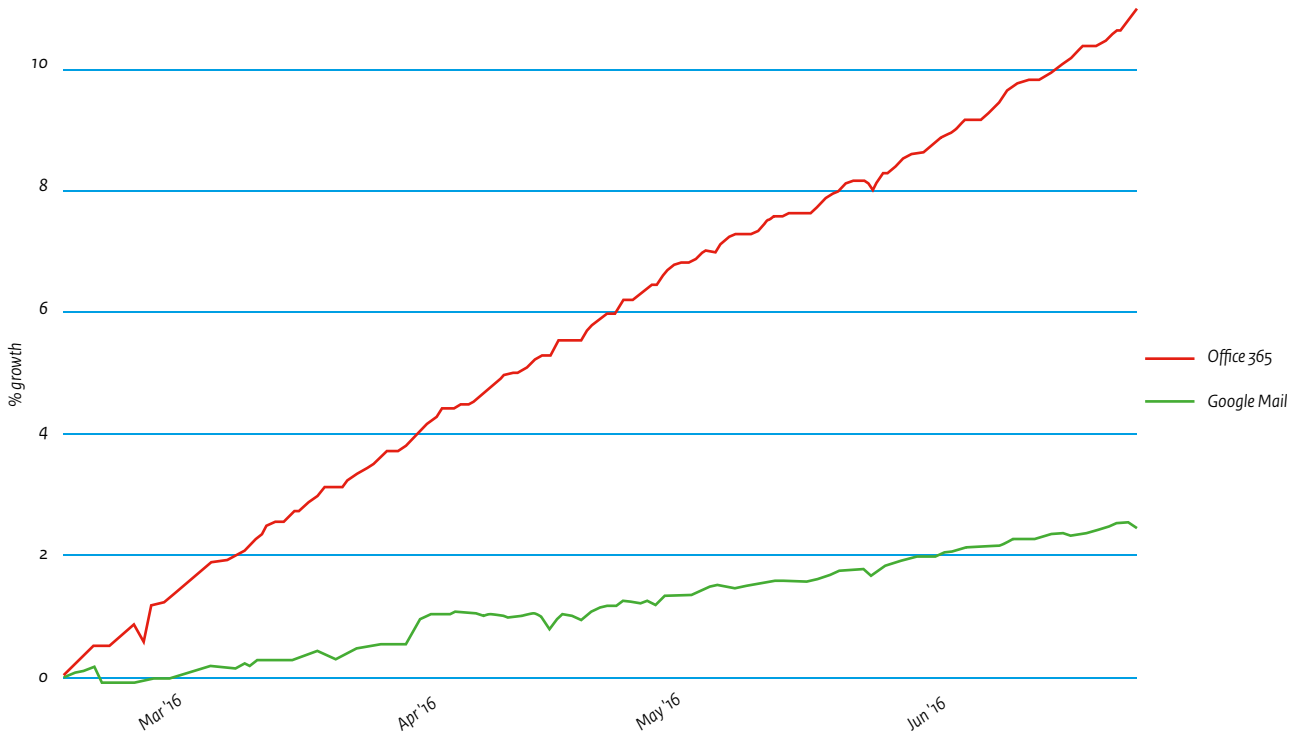
## Centralisation of IT services makes safeguarding simpler but also makes data more susceptible to espionage

Outsourcing of IT services, for example by the use of cloud services, is a trend that has been underway for some time. E-mail is one example of this. E-mail is, for organisations in small and medium-sized enterprises, complex to self-administer. Alternatives in the cloud are then attractive, due to low costs and limited management. A large and experienced provider can often offer e-mail better and safer than one's own IT Management department. The below observations on outsourcing of e-mail also apply to many other outsourced IT services.

E-mail outsourcing is increasingly common, both directly with cloud service providers and via full service providers. A cloud service provider manages e-mail but requires the domain name holder to set his DNS settings in such a way that the e-mail goes to the cloud service provider. A full-service provider sells the services of a cloud provider, but also manages the DNS zone for the client.

Figure 10 shows how the growth of two cloud service providers in a four-month period has progressed for .nl-domain names.[322] During this period the number of .nl-domain names remained almost identical. This creates the image that organisations increasingly outsource their e-mail to cloud service providers. This centralisation is considerable for .nl-domain names. Thirty percent of .nl-domain name holders have e-mail handled by one of the ten most popular e-mail handlers.[323] For .com-domain names, this centralisation is even stronger: there, for 50 percent of domain names, e-mail is handled by one of the ten most popular e-mail handlers. Because small organisations here are counted in the same way as large ones, these statistics are probably most representative of SMEs.[324]

Figure 10 **Growth of cloud service providers**

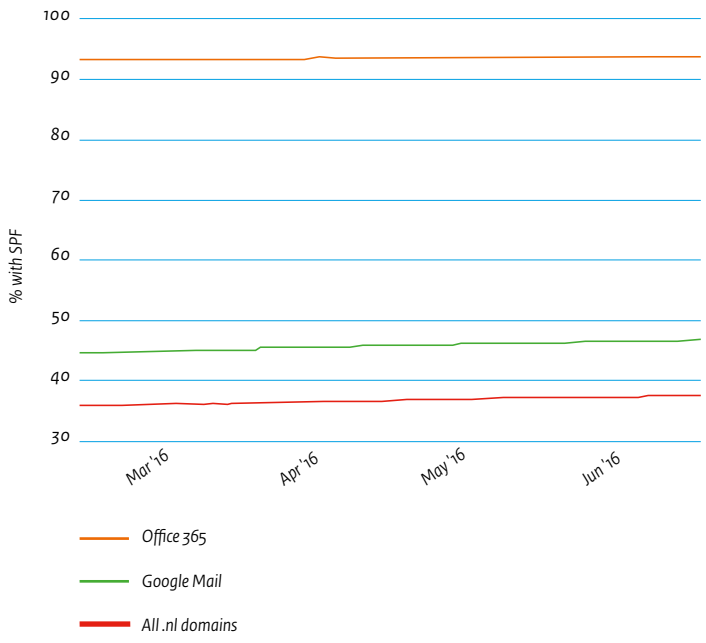



**Source: OpenINTEL.**

New security standards for e-mail are more easily adapted if organisations outsource their e-mail. Full service providers can, for example, introduce SPF in one go for all their clients. For them, the application of the standard is a one-time investment and a selling point. Also, cloud service providers make it easy for their customers with ready-to-use instructions for setting up standards such as SPF. Outsourcing e-mail to a cloud service provider, or possibly through a full-service provider, appears to provide a greater adoption of SPF. In Figure 11, we see that the customers of cloud service providers Microsoft and Google show a significantly higher SPF application than the rest of the .nl-domain name holders.

Centralisation of e-mail also has disadvantages. As early as in the annual report of 2015, the AIVD stated that the use of cloud services involves an additional risk of espionage. This risk also applies to full service providers. In addition, vulnerabilities in the software of cloud service providers and full-service providers immediately have greater consequences because more customers are dependent on the security of the service. In January 2016, two researchers found a vulnerability in Microsoft Office 365. This enabled them to log into accounts of other organisations.[325] This vulnerability was reported to Microsoft and repaired within hours. If the researchers had, however, kept the vulnerability a secret, they could have gotten access to a great deal of sensitive information in all kinds of organisations.

Figure 11 **Application of SPF on .nl-domain names**




**Source: OpenINTEL.**

## Measures against DDoS attacks

DDoS attacks have become part of the overall threat, as already described. Various measures can, however, prevent DDoS attacks, or at least combat its effects.

By setting up routers in networks properly, DDoS attacks can be prevented. This way, spoofed packets are easily stopped.[333] These packets are the source of many different forms of attacks. Unfortunately, filtering this is only effective if almost all networks set it up.

To counter the adverse effects of DDoS attacks, two initiatives were launched in the past year in the Netherlands: the Trusted Network Initiative (TNI)[334] and a collaboration of internet service providers, the Dutch Continuity Board (DCB). The aim of both initiatives is to minimise the impact of a DDoS attack on Dutch critical infrastructure. This allows services to be made available again to Dutch users as soon as possible. Most members of TNI ultimately decided to join up with DCB. The DCB project wants to be operational by the end of 2016.

### Is there a second crypto-war?

The public debate on encryption is not over yet. In September 2015, the American government tried to persuade public companies to cooperate in the field of encryption and decryption, so as not to hinder detection.[326] This was initially not well received.

In March 2016, the discussion escalated: the FBI tried, via a lawsuit, to force Apple's help to gain access to a phone belonging to a US terrorist.[327] Apple did not agree and said that the method would provide access to almost all iPhones. That is why Apple appealed and the company published an open letter.[328] In the public debate, Apple quickly gained the support of many large technology companies. Ultimately, the FBI dropped the case because access was gained to the telephone in a different way.

During this debate in the U.S., WhatsApp switched on end-to-end encryption for all users.[329] Thus, the content of the messages is, in principle, only accessible to the transmitter and receivers. WhatsApp is not the first messaging app that offers this, but it is the biggest with over one billion users worldwide.

The Dutch Data Protection Authority published an advisory for physiotherapists using a contact form on their website. If sensitive data (citizen service numbers or medical data) is to be filled in, then the entire website must use TLS.

Similarly, in June 2015 the US government decided to switch all government websites over to https.[330] The explanation indicates that web traffic has become a central part of our lives. Non-sensitive traffic does not exist on the internet. Therefore, the government should not depend on the good intentions of network administrators.

The launch of Let's Encrypt helped further advance the adoption of https and encryption. This free and accessible web certificate service became publicly available in late 2015. In the meantime, more than 2 million certificates have already been issued by Let's Encrypt.

In January, the government made its position on encryption public[331] It then became clear that the Dutch government supported encryption. The government is also against legal measures with respect to the development, availability and use of encryption algorithms. In January 2016, the French government followed the Dutch position and took the same position.

The Dutch government also contributes to the implementation of encryption by donating 500,000 euros to encryption projects (such as OpenSSL, LibreSSL and PolarSSL).[332]

## Developments in the Netherlands

Digital security is clearly visible on the Dutch policy agenda. A number of ongoing initiatives became more visible in the past year, such as Idensys and MijnOverheid.

The developments around Idensys (formerly the eID system) are now beginning to take shape. In July 2015, the Idensys Privacy Impact Assessment was published. It includes a number of recommendations.[335] In late 2015, this was further developed and several public and private organisations started with a pilot project[336]

The Dutch banks have also jointly set up a similar service: iDIN.[337] This allows customers to use their log-in method at the bank to identify themselves with other institutions. At this moment, there is a pilot project using this service with the Tax and Customs Administration.

The government is trying to communicate with citizens in an increasingly digital manner. To facilitate this, the 'MijnOverheid' project has been set up. A central website, mijnoverheid.nl, gives access to electronic communications with various government agencies. In November 2015, the legal foundation was laid for electronic communications from the Tax and Customs Administration via this website. An increasing number of government agencies are members of the Digital Message Box: in April 2016, already 119 municipalities, 23 pension funds and 28 other government agencies.

The National Detection Network (NDN) was, as early as 2015, named as an important partnership of the NCSC and other parties in the exchange of information on threats. The pilot projects received a positive evaluation at the end of 2015. The network will be further extended in 2016 and included in the standard services of the NCSC.

In the reporting period, the Dutch energy sector worked on a risk analysis of chain dependencies in the energy sector. This analysis showed the vulnerability of systems through these dependencies.[338]

### Internet Standards Platform calls for the application of standards

The Internet Standards Platform, a collaboration between the internet community and the Dutch Government, launched the website internet.nl in April 2015. This website checks to see if an internet connection, e-mail or web server complies with modern internet standards. The website internet.nl can test a server for the connection security of both web and e-mail traffic. Moreover, the site also indicates the extent to which this satisfies the 'comply or explain' list of the Standardisation Forum.

The website proved to be an effective means to help parties improve their use of modern internet standards. Of all the websites that were tested multiple times by visitors of internet.nl, almost fifty percent improved the score between the first and the most recent test.

In June 2015, new security requirements for e-mail traffic were added: in addition to DKIM (DomainKeys Identified Mail), SPF (Sender Protection Framework) and DMARC (Domain-based Message Authentication Reporting and Conformance) were added to the 'comply or explain' list. These are required to create safer e-mail and combat spam and phishing. For larger organisations, it is not easy to apply these standards; the NCSC factsheet 'Protect domain names from phishing'[339] can help with this.

The above measures help to authenticate the sender of e-mails. More is required in order to ensure integrity and confidentiality as well. For this, the traditional STARTTLS is used, which is also used by more than 90 percent of e-mail servers. Here, STARTTLS is only an effective measure against a passive, bugging attacker. In October 2015, therefore, the combination of STARTTLS with DANE was standardised.[340] This combination also protects against other possible attacks. In February 2016, it was also proposed to add this to the 'comply or explain' list.

## Consumers' Association instituted preliminary relief proceedings against Samsung

In the Netherlands, the Consumers' Association started the 'Update!' campaign. In this way, they want to take on Android telephone manufacturers who have a flawed updating policy. In the first action, the Consumers' Association pressed charges against Samsung about this. The Consumers' Association argued in preliminary relief proceedings that Samsung has, for at least two years after the purchase, a duty of care and must make updates available. The Court indicated in these proceedings that it saw no urgent interest and, therefore, refused to institute further proceedings. The Consumers' Association feels that the situation with respect to the Android update policy by various manufacturers is still worrisome.[341]

## Netherlands Clean increases awareness about bad hosting

Dutch hosting remains popular among professional criminals.[342] Many hosting providers indicate that they do not have visibility with respect to the actual users of their infrastructure, because they use a model of reselling. Some of their resellers facilitate criminal activities by offering the most anonymous hosting possible, at relatively high prices.

To raise the awareness of hosting providers for the malicious activities of their customers in their infrastructure, TU Delft has carried out measurements of bad hosting in the Netherlands within the framework of the Netherlands Clean project.[343] The measurements were based on, among others, public and private information, such as from the Internet Hotline against Child Pornography and the National Centre for International Legal Assistance (LIRC). They were further normalised according to the size of the hosting provider. The measurements were used to make an assessment of the 'badness' of all Dutch hosting providers.

MIn mid-2015, the Public Prosecution Office, the police and the ACM had meetings with the top 10 bad hosting providers. This was to point out their facilitating role in digital crime and the measures they can take against it. A second round of measurements showed that some hosting providers had improved. Some providers continued to score poorly in terms of bad hosting, or have even deteriorated. Along with other indicators, such as the lack of cooperation with the government and the absence of preventive measures, the results of Netherlands Clean provided insight into which providers must be given extra attention. In the near future, the police and the Public Prosecution Service are certainly going to concentrate on tackling these bad hosts. The ultimate goal of the Netherlands Clean project is, however, a change in behaviour of hosting providers. In doing this, the industry ensures, through self-regulation, the clean-up of the hosting infrastructure.

## Reporting obligations

On 1 January 2016, the new Personal Data Protection Act went into force. With this, the supervisory authority also got a new name: Dutch Data Protection Authority. The law also regulates that there is more authority, including the authority to issue fines for violations of the law. With this law, the Netherlands has given substance to the EU General Data Protection Regulation.

According to the new Data Protection Act, after 1 January, companies must report incidents involving the possible breach of personal data. In the first week of January, as many as twenty notifications were made to the new Dutch Data Protection Authority; by April, there were already a total of a thousand reports.

The data breach reporting obligation, however, is different from the reporting obligation under the Data Processing and Reporting Obligation (Cybersecurity) Bill. The latter reporting obligation applies to organisations in the critical infrastructure. Notifications about security incidents must be filed with the NCSC. This reporting obligation is part of a larger bill regarding the tasks of the NCSC, and is still being debated in the House of Representatives.

# International developments

## Regulation

In the summer of 2015, a consultation was held in the US on the practical details concerning export regulations with respect to intrusion software. In 2013, technology and tools with respect to intrusion software were added to the Wassenaar Arrangement list of dual-use goods. In the participating countries, an export license must, therefore, be applied for in order to export technology, software and tools for gaining access to other computers. The security sector in the United States responded en masse to the consultation. They indicated that the current definitions of intrusion software were very problematic.[344] Microsoft, for example, indicated that under this regulation, the company expects having to handle hundreds of thousands of licensing requests per year. The U.S. Government was instructed to again negotiate the addition[345] This export regulation has been in force in Europe since late 2013 and was also discussed at the latest NCSC One Conference.

Asus showed America that manufacturers do have some degree of responsibility for secure software. In February 2016, the manufacturer reached a settlement with the FTC on poor security in software for WiFi routers.[346] Asus has agreed to allow independent security audits for the next 20 years.

## Cooperation

In September 2015, the U.S. and China concluded a digital non-aggression pact. The treaty holds that the governments will not carry out economic espionage against each other. The treaty says nothing about traditional forms of espionage.

On 6 July 2016, the European Directive on network and information security (NIB) was adopted by the European Parliament. Member States have 21 months to implement the directive (plus an additional six months to designate providers of essential services). First of all, the Directive requires Member States to have their national cybersecurity capacity in order, secondly, to strengthen cooperation (national and EU) and, finally, to design security and notification requirements for providers of essential services.

# Responsible or coordinated vulnerability disclosure

One of the priorities of the Global Forum on Cyber Expertise is the further promotion of responsible disclosure. This was also high on the agenda during the Dutch presidency of the European Union. Nationally and internationally, there are various important developments in this area. The first development is that, internationally, the main term used is 'coordinated vulnerability disclosure'. The term 'responsible' is often seen as a value judgment, especially to the detector. 'Coordinated' endeavours to indicate that this is an equivalent process for both parties.

In the United States, several multi-stakeholder meetings have been held on possible regulations concerning vulnerability disclosure. The NTIA is organising these meetings together with industry representatives, researchers and government. They are organised around four themes: awareness and adoption, multi-vendor disclosure, economics and incentives and, finally, security and disclosure..

In an increasing number of sectors, it is common to have a vulnerability disclosure programme. After the experience with the Jeep incident[351] General Motors announced a general vulnerability disclosure programme for all products. Several airlines have also started disclosure programmes and offer air miles as a reward for reporting vulnerabilities.

The practice with respect to the professionalisation of vulnerability disclosure is also increasing. Several companies offer help in setting up or maintaining a vulnerability disclosure programme. It is also increasingly common for financial rewards to be given for notifications. Google alone paid out more than two million dollars in 2015[352]

In April 2016, the International Standardisation Organisation (ISO) made the document on vulnerability disclosure (ISO 29147) publicly available.[353] At this time, work is also being done on revising this standard from 2014 in order to process new insights in the field of vulnerability disclosure.

Rabobank and CIO Platform Netherlands have drawn up a Coordinated Vulnerability Disclosure Manifesto. Signatories of this manifesto endorse the importance of the vulnerability disclosure process and appreciate the interaction with researchers and the hacker community. This manifesto was published in May 2016. Twenty-nine companies in the Netherlands and abroad have already signed it.[354]

## Combating cybercrime

In the past year, there have been some major operations against cybercriminals in Netherlands, but also a number of large operations abroad.

In the spring of 2015, the police arrested two suspects. They were e-mailing spam with the subject 'incorrect invoice' to small and medium-sized enterprises. In that way, they were able to install RATs and they got access to the internet banking accounts of the companies. As a result of this investigation, in May 2016, the Public Prosecution Service and the police published an information sheet for SMEs in cooperation with the NCSC, SME Netherlands, ECP and the Dutch Payments Association.

A number of members of the Lizard Squad were convicted in the past year. The 17-year-old 'obnoxious' was convicted in May 2015, for, in particular, his swatting activities.[347] Also, in Norway, the 17-year-old 'zeekill' was convicted for more than 50,000 offences.[348]

In June 2015, a major international investigation into mobile banking malware was completed. Here, an important network of cybercriminals was rounded up. This resulted in the arrest of a total of 60 suspects worldwide, of which about forty in the Netherlands. Four main suspects were given prison sentences of 24 to 39 months in the Netherlands. Also, part of the infrastructure used was in the Netherlands and was dismantled.

In July 2015, the cybercrime forum Darkode was taken off-line as a result of a large, international operation.[343] The FBI worked together with Europol during the Shrouded Horizon operation. There were actions in 20 countries whereby 70 people were arrested.

In August 2015, Ziggo was hit by major DDoS attacks for two evenings. This caused a failure in the Ziggo network, resulting in about 1.8 million of the provider's customers having no internet access. In video messages on YouTube, the criminals threatened to carry out new attacks on Ziggo. KPN has also been the target of DDoS attacks. During the police investigation, the DDoS attack was claimed anonymously on the internet. The impression was that the guys wanted to show that they are capable of great things, such as shutting down the internet service provider. Five suspects were arrested. Four of them were minors (14-17 years of age).

In the previous CSAN, it was described how the police, in April 2015, succeeded in providing a series of protected decryption keys to ransomware victims. Through cooperation with anti-virus company Kaspersky, the police got a clearer picture of the suspects behind these criminal activities. In September, the police were able to arrest two men (18 and 22 years old) in Amersfoort.

Two Dutch suspects were arrested in October 2015. They made many victims by setting up fake web-shops for a short period (up to several days) online and selling desirable stuff (such as phones and carrier bikes) that were never delivered.

In January 2016, Europol announced that they had carried out a successful operation against the DD4BC group. This group had been very active during the past year in blackmailing companies with DDoS attacks. This group threatened thousands of companies. Often, no official reports were filed.

AbuseHub was already named in the previous CSAN. This is a collaboration between the various internet service providers to exchange information and, thus, to fight cybercrime. Since January of this year, this initiative has been further expanded with hosting providers. Via this platform, security risks and reported abuse are automatically passed on to clients without going through the hosting parties. The goal is to make it as difficult as possible for cybercriminals.

In the Netherlands, the FIOD has also acted to arrest the perpetrators behind a phishing operation. In January 2016, a 23-year-old man was arrested for this in Almere. He is suspected of, among other things, having sent phishing e-mails on behalf of the Director General of the Tax and Customs Administration.[350]

On social media, a message appeared on Tuesday 29 March and Wednesday 30 March 2016 that the Tax and Customs Administration website would be shut down. Because of this, many people would not be able to submit their tax returns in time. The cybercrime team of the Central Netherlands Police Unit, in collaboration with the High Tech Crime Unit, arrested a 17-year-old suspect. He threatened to shut down the website of the Tax and Customs Administration through a DDoS attack.

In April 2016, the police secured a company's network infrastructure. The owner was arrested for money laundering. The company sold, for an average of 1500 euros, BlackBerries with PGP software to encrypt messages. The membership fee amounted to 3,000 euros per year, on average. These phones are not suitable for making calls, only for sending messages. The police and the Public Prosecution Service suspect that most of the users use the phones to hide serious and organised crime.

## Conclusion and looking ahead

Cybersecurity has clearly found its place on the administrative agenda. This past year, this has resulted into various measures aimed at humans, technology and organisations. The demand for cybersecurity professionals remains high. This can lead to problems in the future.

The classic technical measures, such as backups and network segmentation, are again proving their worth because they reduce the impact of ransomware attacks. New measures that have been added to the 'comply or explain' list are also receiving more attention because they can be tested easily with the website internet.nl.

In the past year, measures concerning encryption were clearly part of the public debate. Measures have been taken for a better application of encryption, such as new obligations regarding TLS. In addition, Let's Encrypt is making certificates more accessible. At the same time, this makes the field of tension between the interests of security and detection even clearer. That has led to an international discussion. The Netherlands was the first country to speak out in favour of encryption. It does not take steps to limit the development, availability or use of encryption algorithms.

Vulnerability disclosure received a great deal of attention in the past year. An increasing number of organisations are implementing it. Internationally, this practice is becoming more and more acceptable. An increasing number of companies are speaking out publicly in support of this.

### Notes

310 http://www.securityweek.com/microsoft-warn-users-state-sponsored-attacks, consulted on 5 July 2016.

311 http://europa.eu/rapid/press-release_IP-16-2461_en.htm, consulted on 3 August 2016.

312 http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016/, consulted on 5 July 2016.

313 http://cybersecurityraad.nl/assets/csr_advies_cybersecurity_in_onderwijs_en_bedrijfsleven-vdef.pdf

314 Furthermore, the SOC has the task of issuing fraud indications to the anti-fraud teams within the Tax and Customs Administration. Through issuing these indications, many millions of euros in possible fraudulent transactions have been halted.

315 Since 18 February 2014, the Tax and Customs Administration has been using a responsible disclosure procedure, which has been published on the internet, see www.belastingdienst.nl/security.

316 http://gs.statcounter.com/#desktop-os-ww-monthly-201503-201603

317 https://blog.hboeck.de/archives/865-Software-Privdog-worse-than-Superfish.html, consulted on 5 July 2016.

318 http://en.community.dell.com/dell-blogs/direct2dell/b/direct2dell/archive/2015/11/23/response-to-concerns-regarding-edellroot-certificate, consulted on 5 July 2016.

319 https://blogs.technet.microsoft.com/mmpc/2015/12/21/keeping-browsing-experience-in-users-hands/, consulted on 5 July 2016.

320 https://www.forumstandaardisatie.nl/fileadmin/os/publicaties/Monitor_OSb_2015_Definitief.pdf

321 https://www.aivd.nl/actueel/nieuws/2016/04/21/aivd-jaarverslag-breed-palet-aan-dreigingen-voor-nederland, consulted on 5 July 2016.

322 The measurement for .nl-domain names was not implemented until early 2016. Therefore, several months beyond the reporting period have been included in the graph so as to provide more insight.

323 This top 10 is determined on the basis of the MX records of the examined domain names. It is conceivable that several of these suppliers link standard e-mail handling to the domain name, without also making e-mail boxes available for this.

324 The data in this section comes from research that is part of OpenINTEL (http://www.openintel.nl/), a joint project of SURFnet, the University of Twente and SIDN.

325 https://bratec.si/security/2016/04/27/road-to-hell-paved-with-saml-assertions.html, consulted on 5 July 2016.

326 http://motherboard.vice.com/read/the-white-house-thinks-it-can-make-a-deal-with-companies-to-break-encryption, consulted on 5 July 2016.

327 https://assets.documentcloud.org/documents/2714001/SB-Shooter-Order-Compelling-Apple-Asst-iPhone.pdf, consulted on 5 July 2016.

328 http://www.apple.com/customer-letter/, consulted on 5 July 2016.

329 https://blog.whatsapp.com/10000618/end-to-end-encryption, consulted on 5 July 2016.

330 https://https.cio.gov/

331 https://www.rijksoverheid.nl/documenten/kamerstukken/2016/01/04/tk-kabinetsstandpunt-encryptie, consulted on 5 July 2016.

332 https://www.tweedekamer.nl/kamerstukken/amendementen/detail?id=2015Z23825&did=2015D48058, consulted on 5 July 2016.

333 http://www.routingmanifesto.org/

334 https://tn-init.nl/

335 https://www.idensys.nl/fileadmin/bestanden/idensys/documenten/basisdocumentatie/pia/310715_Managementsamenvatting_van_de_finale_versie_van_de_PIA.pdf

336 https://www.rijksoverheid.nl/documenten/kamerstukken/2016/02/17/kamerbrief-over-verzoek-overzicht-lopende-pilots-e-id-met-vermelding-van-deelnemende-partijen, consulted on 5 July 2016.

337 http://www.betaalvereniging.nl/giraal-en-online-betalen/idin/, consulted on 5 July 2016.

338 https://www.cybersecurityraad.nl/actueel/digitale-ketenveiligheid-krijgt-veel-te-weinig-aandacht.aspx, consulted on 13 July 2016.

339 https://www.ncsc.nl/actueel/factsheets/factsheet-bescherm-domeinnamen-tegen-phishing.html
340 https://tools.ietf.org/html/rfc7672, consulted on 5 July 2016.
341 http://www.consumentenbond.nl/campagnes/updaten/updates-naar-android6/, consulted on 5 July 2016.
342 Source: police.
343 Source: police.
344 https://threatpost.com/security-researchers-sound-off-on-proposed-us-wassenaar-rules/113023/, consulted on 5 July 2016.
345 https://langevin.house.gov/press-release/white-house-responds-langevin-and-mccaul-wassenaar-concerns, consulted on 5 July 2016.
346 https://www.ftc.gov/news-events/press-releases/2016/02/asus-settles-ftc-charges-insecure-home-routers-cloud-services-put, consulted on 5 July 2016.
347 "Swatting" means tipping off the police anonymously, resulting in a SWAT team raiding an innocent victim.
348 http://www.dailydot.com/crime/lizard-squad-indicted-julius-kivimaki/, consulted on 5 July 2016.
349 http://motherboard.vice.com/read/the-mysterious-disappearance-and-reappearance-of-a-dark-web-hacker-market, consulted on 5 July 2016.
350 https://www.security.nl/posting/458110/FIOD+arresteert+man+wegens+phishingmails+Belastingdienst, consulted on 5 July 2016.
351 http://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/, consulted on 5 July 2016.
352 https://googleonlinesecurity.blogspot.nl/2016/01/google-security-rewards, consulted on 5 July 2016.
353 http://standards.iso.org/ittf/PubliclyAvailableStandards/c045170_ISO_IEC_29147_2014.zip
354 http://www.thegfce.com/news/news/2016/05/12/launch-manifesto-on-responsible-disclosure, consulted on 5 July 2016.

*SMEs are important for the economy, but are fragile in the digital domain*

# 6 Interests

**Cybersecurity means taking steps to prevent damage being caused by IT being disrupted, interrupted or exploited and, if such damage occurs, repairing it. The prevention of damage, including through digital means, is in the interests of the Netherlands. The government's position on encryption shows that the government is making the interests of citizens, businesses and government a priority. It sees no possibility to weaken encryption without affecting those interests. The data breach reporting obligation can ensure that organisations pay more attention to measures to protect personal data. The importance of small and medium-sized enterprises for the Netherlands is great: many chains contain SMEs. However, in the area of cybersecurity measures, this group is lagging behind.**

Disruption of IT systems and leaks in their security harm the interests of individuals, organisations or society. This is reflected in interests in the area of freedom, security and societal growth.[355]

## Societal interests

### Freedom

IT plays a central role in society. Fundamental values and rights are no longer separate from the technical environment in which they occur. These values and rights must, therefore, be guaranteed in the digital domain.

### Security

The security of society, in general, and citizens, in particular, is partly dependent on IT. Failure of IT-based services and processes can have major social consequences in terms of security. Also, it can affect the safety of citizens. Confidence in the digital domain is essential for ensuring safety.

### Societal growth

The development of IT and the innovative power of technological development are key drivers for growth. Aside from economic growth, it also concerns social growth. Digitisation offers society new opportunities, for example in the form of applications for educational purposes, possibilities to maintain social contacts and improved government facilities.

## The development of interests

Interests often remain stable over a longer period of time. However, there have been developments: the use of digital resources is changing. These developments mostly focus on the effect that growth in the use of digital resources has on existing interests.

### Government's position on encryption: no measures to weaken encryption

In January 2016, the government sent its position[356] on encryption to the House of Representatives. The position of the government is that the importance of encryption for government, businesses and citizens is great. Cryptography plays a key role in technical security in the digital domain and many cybersecurity measures in organisations rely heavily on the use of encryption, according to

the government. The government believes that there is, currently, no insight into possibilities to weaken encryption products without thereby affecting the interests of government, industry and citizens. Introducing a technical entryway into encryption products to enable law enforcement agencies to be able to view encrypted files, for example, might make digital systems vulnerable to, for example, criminals, terrorists and state actors.

Communication by the government is increasingly digital. One of the agreements from the coalition agreement is that, by 2017, all communication between citizens and businesses and the government must be digitally available. Also, information within the government is increasingly digital. For these cases, the possibilities of encryption are essential. Encryption can ensure that the data is protected against perusal by third parties.

Encryption enables businesses to securely store and send corporate information. If they can use encryption, that strengthens the international competitive position of the Netherlands. Confidence in secure communication and data storage is essential for the (future) growth potential of the Dutch economy. This is primarily in the digital economy. The interests of businesses in the field of social growth is thus protected.

Finally, encryption supports citizens in protecting themselves against infringements of privacy and against restricting freedom of expression. This allows citizens to protect their interests in the area of freedom and security.

Encryption provides benefits to government, the business community and citizens. At the same time, it also offers malicious persons the ability to conceal their conduct in the digital domain. This can keep them out of sight of investigative, intelligence and security services. This touches upon the security interest. The government considers the adoption of restrictive legal measures against the development, availability and use of encryption within the Netherlands not to be desirable at this time.

## Data breach reporting obligation

The data breach reporting obligation[357] which took effect on 1 January 2016, will contribute to the respect for and the protection of privacy. Anyone who processes personal data must protect it against loss or unlawful processing. If this protection fails, and there is a security breach of personal data, this will constitute a data breach. Serious data breaches must be reported to the Dutch Data Protection Authority. In some cases, the person concerned must also be notified of the data breach.

The introduction of the data breach reporting obligation had impact on many companies. They had to think about how and when the organisation would proceed in reporting a data breach and, in many cases, organisations had to adapt their internal processes in order to prevent data breaches, their notification and the fines and potential reputational damage. This could encourage companies to take better measures to protect personal data.

## Cybersecurity in SMEs of importance for society

SMEs constitute a large group of companies and account for 61 percent of gross domestic product.[358] In addition, many vital processes are part of a chain and SMEs are often also part of this. SMEs are, therefore, important not only for the economy, but also for society. Although this is the case, SMEs have low digital resilience. Along with the growing threat of professional criminals, this represents a growing risk to the economic interests of the Netherlands.

To a greater or lesser extent over the past few years, large companies and organisations have nearly all been investing in cybersecurity measures. This is not the case for SMEs. Research by Interpolis shows that entrepreneurs underestimate the risk of digital threats.[359] A third of the businesses surveyed did not pay regular attention to digital threats. Many SMEs have no idea about cybercrime. The protective measures they take are basic, such as using virus scanners, firewalls and encrypting WiFi connections. This is striking, because research shows that 74 percent of SMEs say that they are largely or entirely dependent on IT.[360] The same study reports that more than 28 percent of SMEs have been victims of cybercrime.

In recent years, however, attention has been paid to digital security of SMEs. In order to reach SMEs better, the theme of the annual 'Alert Online' campaign was digital responsibility in business.[361] This, however, seems insufficient to protect SMEs, which are an essential party in society and in critical processes, well enough.

## Quality requirements as implicit expectation

IT systems and the internet are an integral part of many processes within society. The government has set up its communication with the public through the internet and lays out its services in digital portals. For the business community, the analogue world has, for some items, long been an idea from the past. This is not new, but the trend is continuing. What is striking, is that users implicitly set quality demands, in the broadest sense, on IT. They expect IT processes to withstand disturbances in the area of availability and infringement of integrity and confidentiality. These expectations are often not expressed. The expectation and the actual outcome of measures taken do not, therefore, correspond with each other.

From a traditional information security point of view, requirements are set on availability, integrity and confidentiality of information and information systems. Service providers, in turn, feel the need to take 'due care' of the information of their clients.[363] Even if contractually agreed availability requirements are met, but a malfunction occurs anyway, the expectation of clients that their unspoken demands are not being taken into account, is felt. The requirement for 99.9% availability can be agreed upon while, during the Christmas season, there is the implicit expectation that this should be 100 percent.

This can also been seen in other areas. Consumers know that their mobile provider will give them a certain quality. They also expect this in their business practices. Special subscriptions for high availability and specific services are skipped because of cost considerations.[363] The business community prefers cheaper standard subscriptions for, for example, business data traffic. Through cost savings and implicit expectations, the business community runs unnecessary risks.

## Conclusion and looking ahead

Cybersecurity affects the interests of individuals, organisations and society. These are interests in the area of freedom, security and societal growth. These interests often remain stable for long periods of time. The past year, a number of developments have been observed in this area.

The government's position on encryption shows that the government is making the interests of citizens, businesses and government a priority. It sees no possibility to weaken encryption without affecting those interests. The data breach reporting obligation goes hand in hand with the ability to impose sanctions on organisations with data breaches. This can encourage these organisations to make sure that the security of this data is in order and to keep it that way.

SMEs are important for the Netherlands. Many chains contain SMEs, and the same goes for chains within the critical processes. This group is lagging behind in terms of cybersecurity measures. That means a risk to critical processes and thus for the Dutch society.

Users implicitly set high quality requirements on digital services. Without expressly verbalising this, they assume that availability, integrity and confidentiality are high. Service providers feel the necessity of 'due care,' but cannot meet all the implied expectations.

### Notes

355 National Cyber Security Strategy 2, https://www.rijksoverheid.nl/documenten/rapporten/2013/10/28/nationale-cyber-security-strategie-2.

356 https://www.rijksoverheid.nl/documenten/kamerstukken/2016/01/04/tk-kabinetsstandpunt-encryptie, consulted on 5 July 2016.

357 https://autoriteitpersoonsgegevens.nl/nl/melden/meldplicht-datalekken

358 http://www.staatvanhetmkb.nl/nieuws/kernpublicatie-de-staat-van-het-mkb-2015, consulted on 5 July 2016.

359 https://www.interpolis.nl/DocumentenLijst/rapport-mkb-cybersecurity.pdf

360 Cybercrime among companies. An investigation into cybercrime victimisation among SMEs and self-employed workers without employees in the Netherlands. https://www.nhl.nl/sites/default/files/files/Bedrijf-en-Onderzoek/Lectoraten-Documenten/Cybercrime%20onder%20bedrijven%20definitief%20rapport.pdf

361 https://ecp.nl/actueel///4492/alert-online-maakt-vliegende-start-met-eerste-netwerkbijeenkomst.html, consulted on 5 July 2016.

362 Source: input to the NCSC from the MSP ISAC.

363 Source: input to the NCSC from the Telecom ISAC.

# Appendices

# Appendix 1 NCSC statistics

**This appendix offers a summary of the responsible disclosure reports, security advisories and incidents that have been handled by the NCSC. The NCSC keeps a record of incidents using a registration system. This system is the source for all of the graphs in this appendix. This year, too, the number of incidents handled and security advisories published is larger than the year before. This year, the NCSC has dealt with about 5 percent more incidents and has written 25 percent more new security advisories than the year before.**

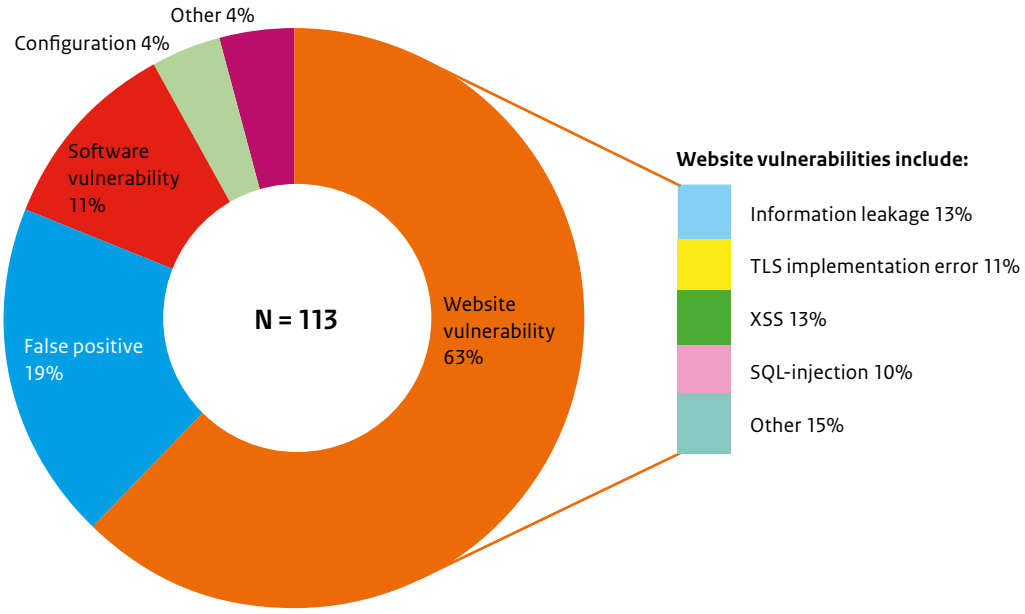
The NCSC facilitates the making and processing of responsible disclosure reports for both its own infrastructure and that of the Central Government and several private parties. It issues security advisories for its participants and deals with cybersecurity incidents. For this reporting period (May 2015 to April 2016) statistics have been calculated that are presented below. By comparing these statistics to previous reporting periods, trends and developments become visible.

## Responsible disclosure

During the reporting period, the NCSC received 113 responsible disclosure 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 are filed if, for example, two or more researchers report the same vulnerability. As a result, the total number of reports is not representative of the total number of vulnerabilities. In 19 percent of all reports, further research showed that there was no vulnerability or that it concerned an accepted risk. An example of this is the login page on a website that has no specific measures against brute-force attacks. These cases were classified as false positives. In the past year, this concerned 20 percent of all notifications.

Figure 12 shows the different types of notifications. The majority (63 percent) of all reports have to do with a vulnerability in a website, a web application or infrastructure on which web applications run. Examples of such notifications are weak TLS parameters, cross-site scripting (XSS), SQL injection and information leakage. An example of the latter is a vulnerability through which it is possible to see a version number of a web application or a configuration file. Eleven percent of all reports concern vulnerabilities in software (excluding web servers and applications). Relatively few reports (4 percent) have to do with configuration errors in hardware and software.

Figure 12 **Types of responsible disclosure reports**

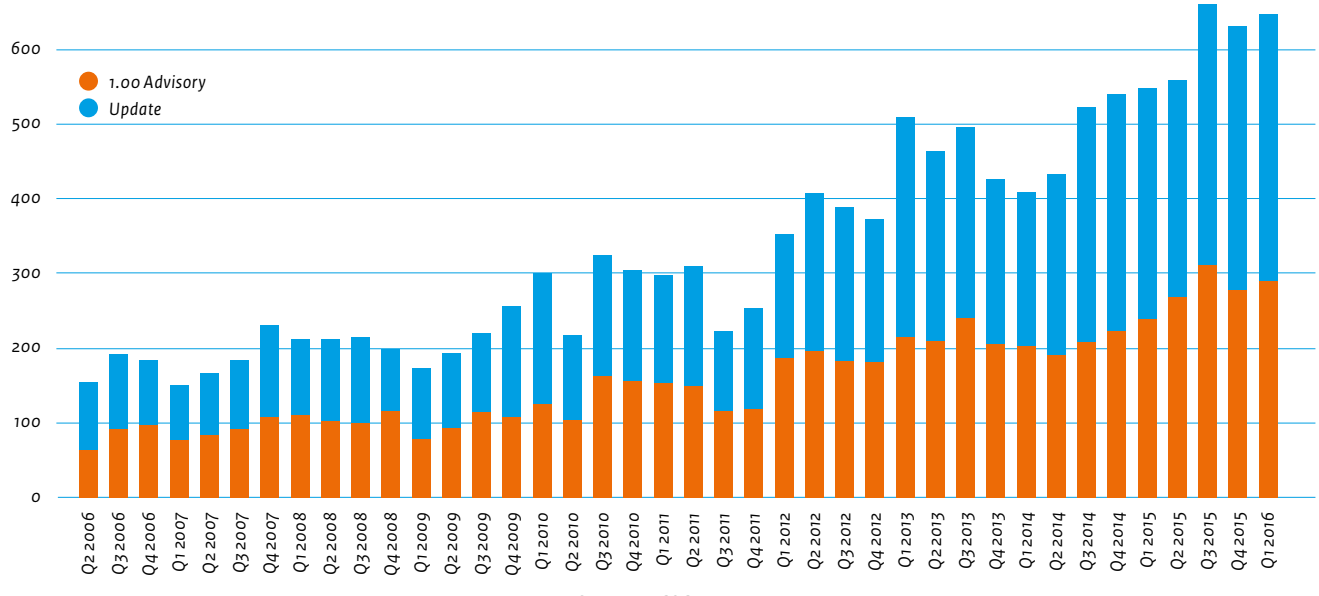



**Source: NCSC-NL.**

# Security advisories

The NCSC publishes security advisories for software vulnerabilities or perceived threats. A security advisory describes what is going on, what systems may have been affected and what should be done to prevent an organisation from becoming a victim. Figure 13 shows the number of advisories that the NCSC published per quarter between the second quarter of 2006 and the first quarter of 2016. Here, a distinction is made between new advisories (with version number 1.00) and updates of existing advisories. In total, the NCSC published 1133 security advisories over the reporting period. This is about 25 percent more than the year before. This increase can be partly explained by the growing number of participants that the NCSC serves. The growth of the number of participants leads to a growth in the list of software and systems for which the NCSC writes security advisories.

Figure 13 **Number of advisories per quarter (Q2 2006 - Q1 2016)**



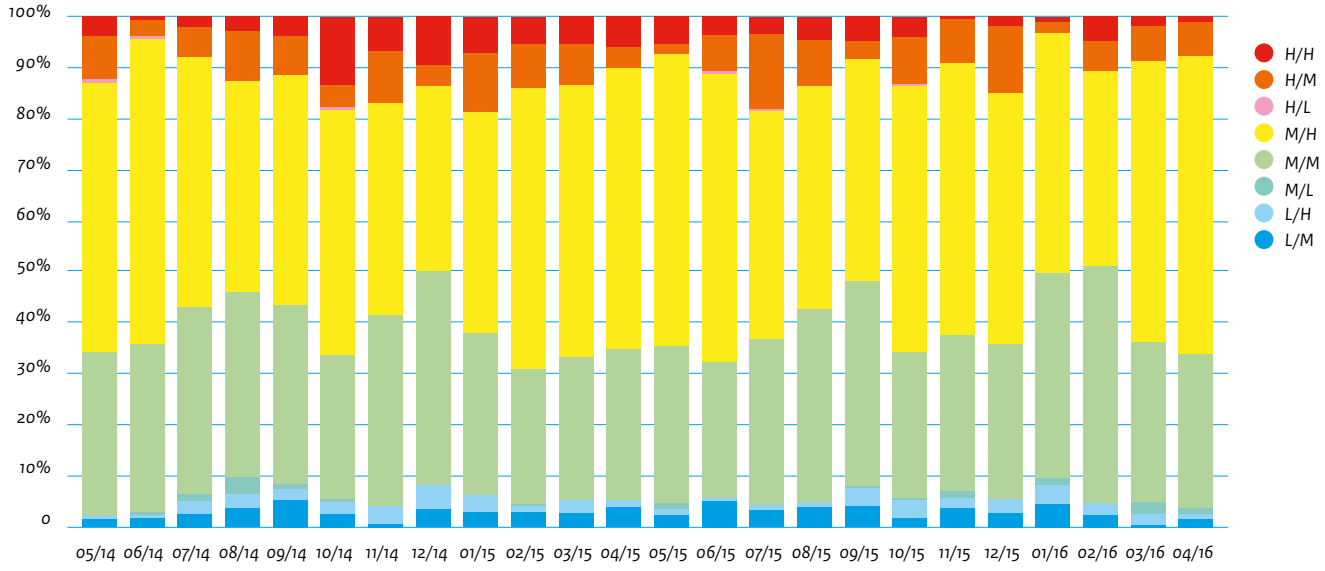

**Source: NCSC-NL.**

The NCSC security advisories are classified according to two elements. Firstly, it determines the likelihood that the vulnerability will be abused. Secondly, the NCSC determines the damage that occurs when the vulnerability is abused. Thus, the classification has two criteria: likelihood 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 14 shows the relationships between these levels for all published advisories (including updates) per month for the past two reporting periods.

## Damage from vulnerabilities

Every security advisory comes with a description of the possible damage that malicious parties could cause if the advisory is not followed-up on. Table 3 shows the percentage of advisories per damage description for the past 3 reporting periods. Security advisories related to denial-of-service (DoS) still appear to have the largest proportion (56 percent), followed by remote code execution with user rights (37 percent), access to sensitive data (32 percent) and bypassing a security measure (25 percent). These were also the most common security advisories in the previous reporting period. An advisory often comes with several damage descriptions.

Figure 14 **Classification of advisories per month (May 2014 - April 2016)**




**Source: NCSC-NL.**

Table 3 **Percentage of security advisories per damage description CSAN-4 to CSAN 2016**

| Damage description | 2014 | 2015 | 2016 |
|---|---|---|---|
| Denial-of-service (DoS) | 46% | 51% | 56% |
| Remote code execution (user rights) | 31% | 29% | 37% |
| Access to sensitive data | 24% | 26% | 32% |
| Security bypass | 13% | 19% | 25% |
| Privilege escalation | 21% | 14% | 21% |
| Access to system data | 8% | 9% | 13% |
| Cross-site scripting (XSS) | 11% | 6% | 9% |
| Manipulation of data | 6% | 5% | 8% |
| Authentication bypass | 6% | 4% | 5% |
| Remote code execution (administrator/root rights) | 4% | 4% | 6% |
| Spoofing | 4% | 2% | 5% |
| Cross-site request forgery (XSRF) | 3% | 1% | 2% |
| SQL injection | 2% | 1% | 2% |

# Cybersecurity incidents registered with the NCSC

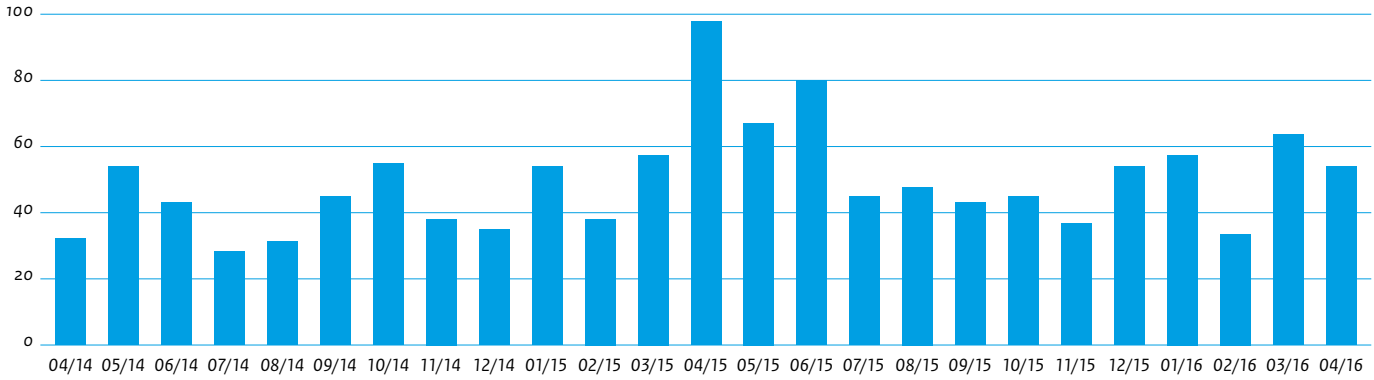
The NCSC assists governmental departments and organisations in critical infrastructure in the handling of incidents in the area of IT security. In this role, the NCSC receives reports of incidents and vulnerabilities and also identifies incidents and vulnerabilities itself, for example on the basis of various different detection mechanisms. At the request of national and international parties, the NCSC supports Dutch internet service providers in the fight against cyber incidents that originate from a malicious web server in the Netherlands, for example, or from infected PCs in the Netherlands.

## Number of incidents handled

Figure 15 shows the number of incidents handled per month (excluding automated checks) for the last two reporting periods. In the previous reporting period, a total of 598 incidents were reported: an average of 46 per month. In this reporting period, 629 incidents were reported: 52 per month. This difference can be partly explained by the growing number of participants that the NCSC serves.

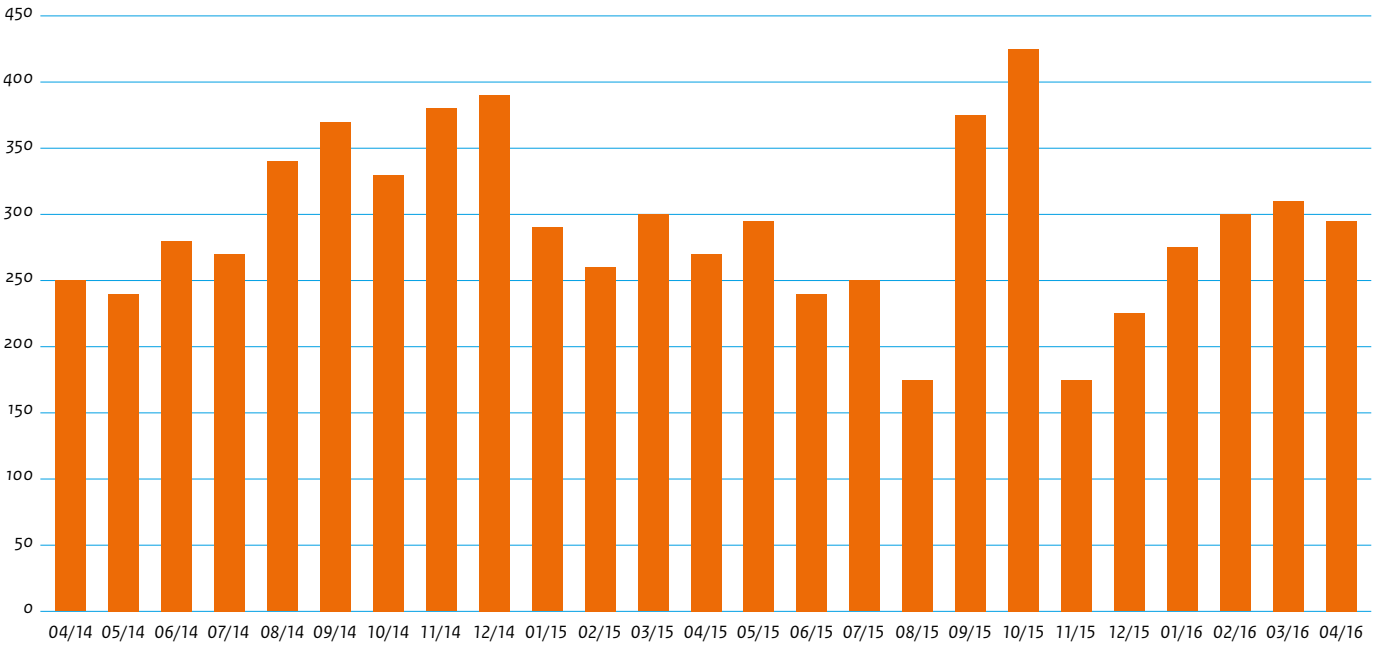
Figure 16 shows the results of automated checks for the last two reporting period. This shows that, in the past reporting period there were, on average, 280 incident reports per month on the basis of this automation. In the previous reporting period, there were an average of 300 reports per month. A report may concern several infected systems within an organisation.

Figure 15 **Incidents handled (excluding automated checks)**




**Source: NCSC-NL.**

Figure 16 **Automated checks**




**Source: NCSC-NL.**

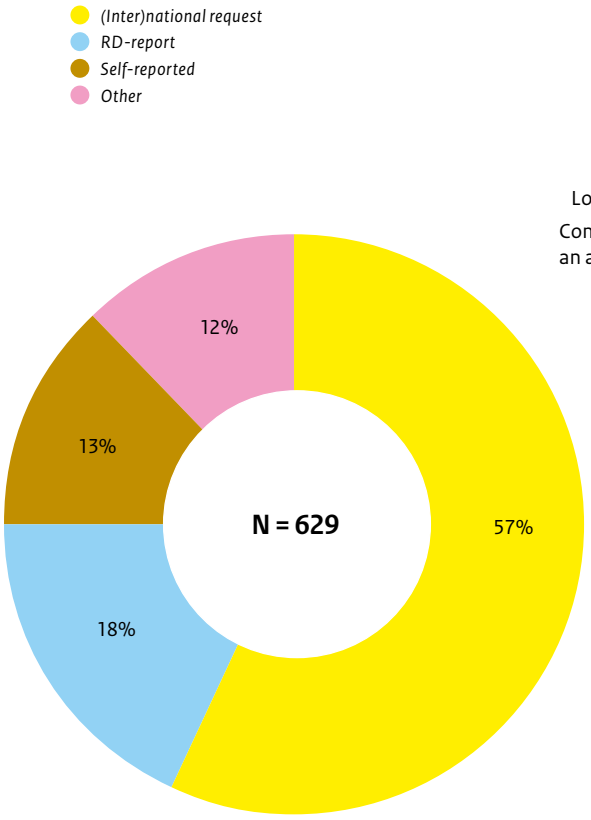
## Distribution of incidents per report, category and handling

For the following analyses, the NCSC made use of an incident taxonomy other than the taxonomy used in previous reports. These analyses are therefore difficult to compare with analyses from previous editions of this report. This taxonomy was proposed by CERT.PT [364] and recommended by ENISA [365] as a common taxonomy for the international network of Computer Security Incident Response Teams (CSIRTs). By using this taxonomy, it becomes easier to compare the analyses with other CSIRTs. A common taxonomy also makes it possible to share incident information with partner organisations for incident response.

Figure 17 shows the distribution of incidents according to reporting type. Most of the incident reports (57 percent) come from outside: from national or international sources. In 18 percent of all incidents, the report comes from inside through responsible disclosure. In 13 percent of all cases, it concerns signalling by the organisation itself. Examples include a warning from one's own detection mechanism or a message from a public source. The remaining 12 percent of the reports concerns a PKI required notification, information that was accepted as a notification, automated reports for which additional manual actions were necessary or other various reports.

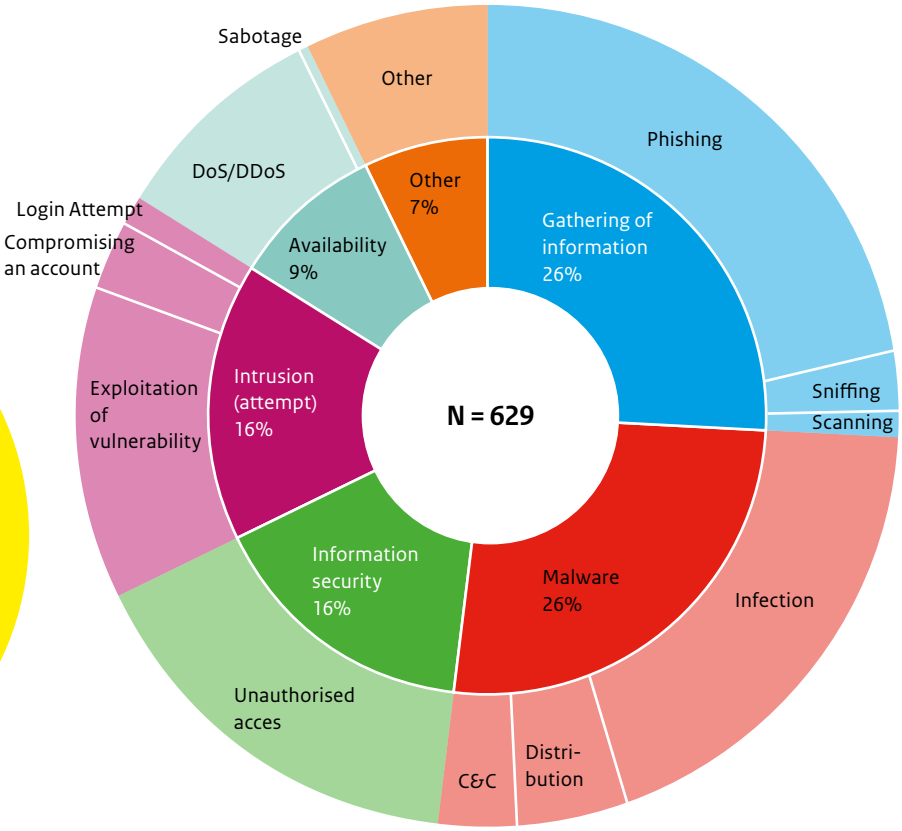
Figure 18 shows the distribution of incidents by category. In the inner ring, main categories are shown while the outer ring indicates the subcategories. This shows that incidents during which information was gathered made up more than a quarter (26 percent) of all incidents. The vast majority of these were phishing incidents. Malware incidents were responsible for 26 percent of all incidents. The majority had to do with malware infections. Sixteen percent of all incidents related to unauthorised access. (Attempted) intrusions made up 16 percent of all incidents. This mainly had to do with the exploitation of a vulnerability. Only 9 percent of all incidents had to do with availability. Almost all of these incidents were related to Denial-of-Service (DoS) attacks or threats. The remainder (7 percent) was due to various incidents, including fraud or sending spam.

Figure 17 **Incidents handled per reporting type**




Source: NCSC-NL.

Figure 18 **Incidents handled per category**




Source: NCSC-NL.

Figure 19 gives the distribution of incidents by handling. Incident handling is independent of how the report was received or in which category the incident falls, and the figure only looks at the actions that were carried out. In 61 percent of all incidents, the NCSC provided remote support. In 26 percent of all incidents, the NCSC issued a 'notice-and-take-down' (NTD) request. This is done, for example, if a rogue website must be taken off-line. If an incident turns out to be a false positive, or if information is accepted as a notification, the incident is registered as not having been processed.

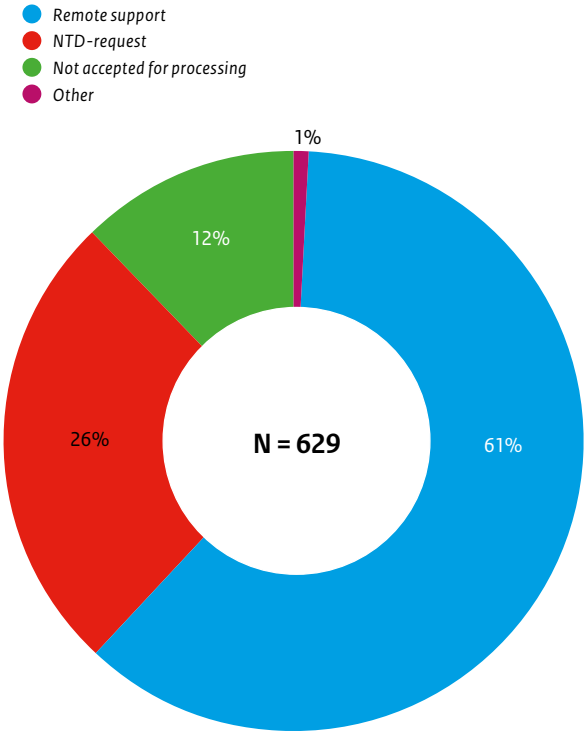
## Division of incidents between government and critical infrastructure

The NCSC supports both the Central Government and the critical infrastructure in security incidents. In addition, the NCSC acts as a point of contact for international requests for assistance concerning information security.

Figure 20 shows the distribution of the number of incidents handled, divided into public, private and international parties. A total of approximately 43 percent of the incidents concerns a public organisation. Thirty-five percent concerns a private organisation. The remaining 22 percent concerns an international party. Compared to the previous reporting period, the NCSC handled twice as many incidents from an international party. An example of this is the receipt of a malware report from the national CSIRT of another country. A foreign organisation can also ask the NCSC to take to a rogue website off-line which is hosted in Netherlands.

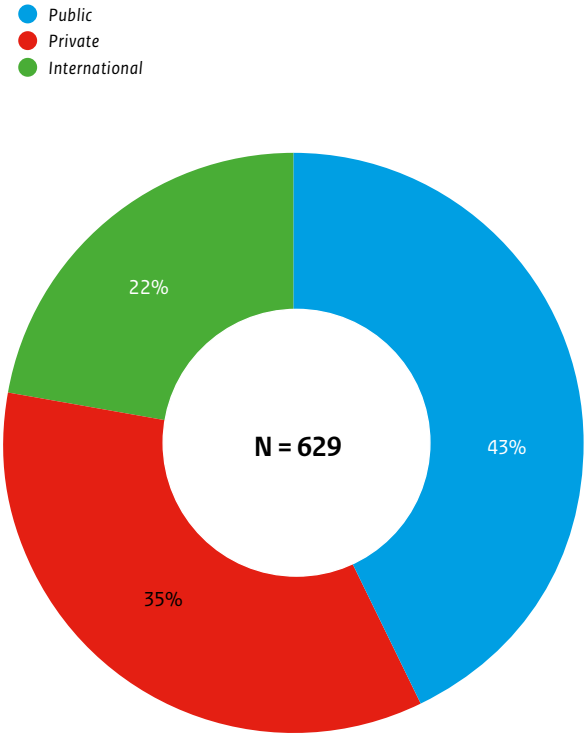
Figure 21 shows the distribution between incident categories per type of organisation. The bottom of each column shows the type of organisation the distribution concerns and the number of incidents it represents. Incidents involving malware are responsible for about a quarter of all incidents, regardless of the type of organisation. With incidents under the category 'gathering of

Figure 19 **Incidents handled, by handling**




Source: NCSC-NL.

Figure 20 **Incidents handled per type of organisation**



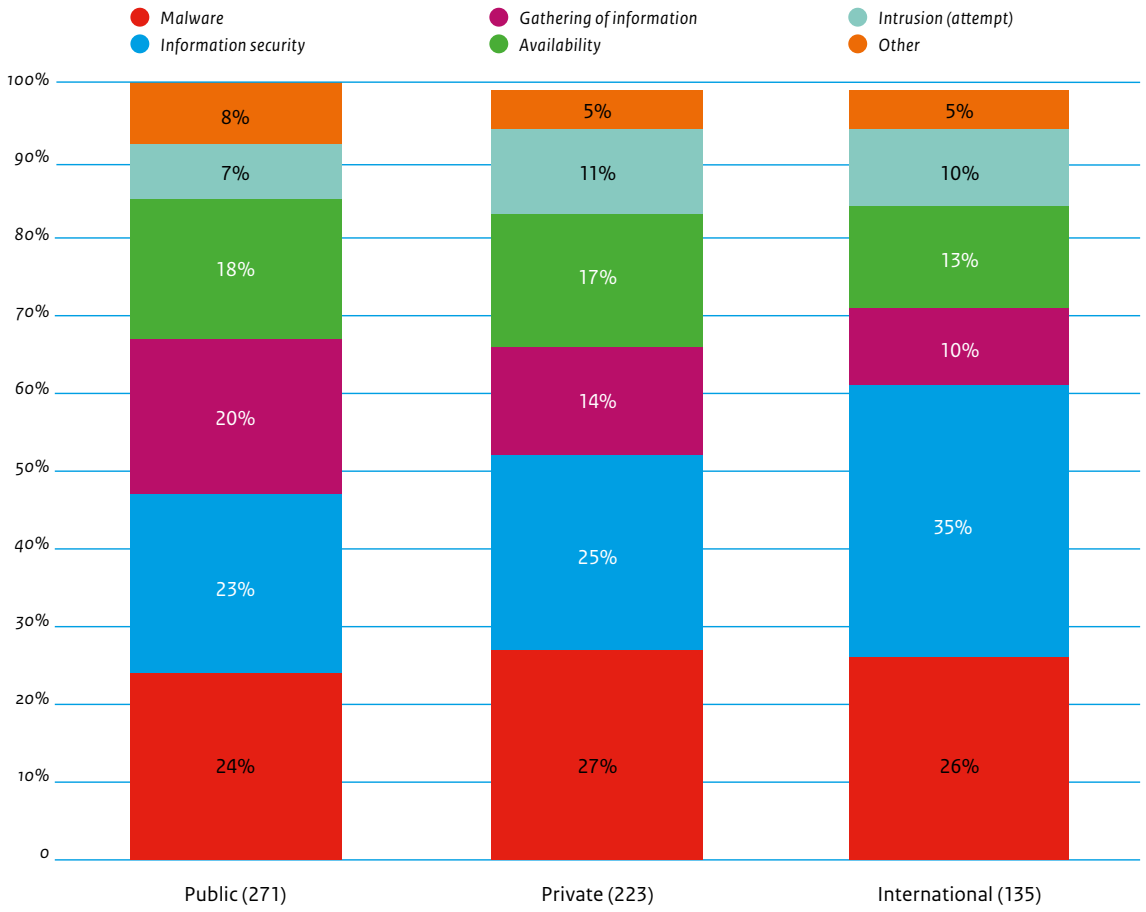

Source: NCSC-NL.

information', the difference is even greater. Thirty-five percent of all cases involving an international party fall into this category. In practice, most of these incidents have to do with phishing campaigns.

This figure also shows that (attempted) intrusion occurs more frequently in incidents in the public sector (20 percent) than with a private party (14 percent) or an international party (10 percent).

Such a distribution can also be seen with incidents dealing with 'information security'. Such incidents are often related to unauthorised access to sensitive information or systems. An example of this is the reporting of a website vulnerability that allows an attacker to view a customer base. With incidents involving an attack on the availability of an organisation, there is a clearer difference between public organisations (6 percent) and the rest (11.5 percent on average).

## Figure 21 Incident categories per type of organisation




**Source: NCSC-NL.**

## Notes

364 http://www.cncs.gov.pt/home/index.html

365 https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement

# Appendix 2 Sectoral assessment of cybersecurity

In the drafting of the CSAN, discussion sessions were held with representatives of Dutch organisations within the critical infrastructure and other sectors. These meetings have helped in shaping 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 | Manifestations of ransomware, phishing and DDoS attacks have been observed in particular. | The sector has no picture of specific actors that pose a threat. However, internal actors have been named as important actors. | Malware, phishing and DDoS attacks on office automation; malware on process automation. |
| Energy | Manifestations of ransomware, phishing and DDoS attacks have been observed in particular. | The greatest threat to this sector comes from state actors and internal actors. | Many (spear)phishing attacks take place. DDoS-as-a-service, including through booter services, is seen as a tool that is used. |
| Financial institutions | Limited ransomware infections have been observed. These seem to be focused on staff as private persons and not specifically on the financial sector. Attacks on clients have shifted from massive attacks on large groups of (private) clients to targeted attacks on (often business) clients. | The greatest threats seem to come from criminals and (to a lesser extent) internal actors. | A limited amount of (spear)phishing has been observed. In addition, malware is being reused by various parties. Criminals are focusing more on bank employees, in addition to their customers. |

| Resilience: vulnerabilities | Resilience: measures | Interests |
|---|---|---|
| Human beings remain a weak link. In addition, dependence on third parties is seen as a vulnerability. | Security frameworks are being worked on, as well as the segmenting of networks and shielding of the segments. Renewal of process automation systems has been planned. In addition to prevention, more effort is being put into detection and response. | The drinking water supply is essential for public health and for the functioning of society. Any failure will result in social disruption. These interests are stable. |
| The biggest vulnerabilities are seen in chain dependencies. | Steps are being taken to ensure further segmentation of networks. Network monitoring, also of ICS networks, is on the rise. Pen testing is more commonly applied. | There are various developments in the interests. Because of the implementation of just-in-time processes, the impact of major disruptions is increasing.<br><br>Chain dependencies are increasing. The dependence on foreign parties is increasing, also through acquisitions in the cybersecurity sector. There is an increasing need for information exchange between various environments. These links can lead to risks through various security measures. |
| Observed vulnerabilities are the possible reason why common DDoS mitigation providers themselves are attacked and there are implementation errors in encryption libraries (Heartbleed, DROWN) that have been used for years. | Through current back-ups, organisations suffer less from the consequences of ransomware infections than individuals. Protection against DDoS attacks is expensive, but has now become business as usual. Banks are now improving their monitoring; also, the solutions for authentication are ever more frequently what-you-see-is-what-you-sign solutions. In addition, the cooperation with the Electronic Crimes Task Force helps with detection. | Extensive automatic data exchange and combinations increase the impact of inaccurate information for the client.<br><br>The importance of good protection is growing through increasing use of digital resources and the elimination of analogue resources (such as counters and phones).<br><br>Security is not always the basis for a (political) decision and sometimes loses out to costs and ease of use. |

| Sector | Manifestations | Threats: actors | Threats: tools |
|---|---|---|---|
| Managed Service Providers | MSPs have observed manifestations of cryptoware, DDoS attacks, social engineering, (digitally supported) invoice fraud and espionage. | Several times a year, the MSPs must deal with sophisticated attacks, which some organisations suspect are being carried out by state actors. | Cybercrime-as-a-service is seen as a threat. Reflection attacks are seen a lot. Social media used by organisations for legitimate goals are misused to collect information about goals. Booter services are used to perform DDoS attacks. |
| Nuclear | Manifestations of phishing, malware, telephone fraud, CEO/CFO fraud have been observed. These do not seem to be focused on the sector and manifest themselves in office automation systems. | State actors, criminals and internal actors (including suppliers) constitute a threat to the sector. | Generic malware, combined with the coupling with third-party systems, is a major threat. |
| Central government | The sector is coping with a growing number of DDoS attacks. Phishing is the order of the day, cryptoware infections are a weekly occurrence. In addition, there is also internal fraud. | State actors and criminals are major threats for the Central Government. Furthermore, internal actors form an (often unwitting) threat. | Malware that is available to a wide audience is actively used (cybercrime-as-a-service). Actors are becoming increasingly professional. The usual methods are seen, such as e-mail for (spear)phishing and Tor for communication through malware. Regularly, malware is spotted in or with portable apps, and is used, consciously or unconsciously, by internal actors. |
| Telecom | The sector was confronted with a vulnerability in an implementation of TN69, a protocol for managing modems remotely.<br><br>In addition, many ransomware infections have been observed. There are many DDoS attacks, but they are, for the most part, of short duration. In addition, the sector is hindered by criminals who impersonate telecom companies and steal via phishing and web shops | The main actors who form a threat to the telecom sector are state actors and criminals. | Actors seem to use many booter services for DDoS attacks. In addition, many phishing e-mails are sent to spread malware. |

| Resilience: vulnerabilities | Resilience: measures | Interests |
|---|---|---|
| Small parties are vulnerable to DDoS attacks around busy periods, such as the holiday season. Standard libraries, such as TLS implementations, often form a vulnerability without people realising this. Mixing private use and business use of mobile devices creates vulnerabilities. Not being able to update mobile devices makes a large group of users vulnerable in a short period of time. | Security awareness remains crucial. To improve this, various organisations carry out internal phishing tests. Measures that work are, for example, conservative ones, such as not linking management interfaces to the internet. | Users implicitly have the expectation that strong measures have been taken, whereas this is not always the case. At the same time, due to cost pressures, more single points of failure are introduced.<br><br>Chain dependencies are a growing challenge and are not 1-to-1 but many-to-many.<br>The Netherlands, as a digital hub, can provide economic growth but, at the same, that increases the threat. |
| There is a visible shift through the introduction of digital systems. | The Cyber Design Basis Threat is used to make the sector resilient against key threats.<br><br>The sector engages in peer testing in the field of security measures. | In view of the external security aspects within the sector, nuclear safety for the sector is of major importance. IT mainly has a role in, for example, access security measures. IT is supportive to the primary process. |
| The focus on internal (network) monitoring is too limited; the focus is still very much on traffic to and from the outside. In addition, logging is still not viewed proactively enough; responding to incidents is the norm.<br><br>The mixing of business and private communications causes vulnerabilities. There is a lack of cybersecurity knowledge among both administrators and politicians. It is not yet on their minds.<br><br>There are still single-points-of-failure in software. Organisations had been dealing with vulnerable servers that were accessible from outside. | Cybersecurity is more regularly included in contracts with suppliers.<br><br>The design of network security is continually improving. There is collaboration among various parties, including in the field of best practices and SOCs. This collaboration is seen as an important support for measures. | The dependence on digital resources is growing. One example is the use in transport systems. Also, the dependence on being able to work online is growing, through extensive use of teleworking.<br><br>There are a great many chain dependencies, for example, through the outsourcing or hosting by other organisations within or outside the central government.<br><br>Reducing the attack surface provides benefits of scale, but can also cause single points of failure. |
| Technical vulnerabilities: legacy devices for which no updates are available, leaks in Cisco routers, the disclosure of the algorithm used for calculating WiFi keys.<br><br>During overload in case of calamities, there is no straightforward scenario for assistance.<br>Suppliers do not practise secure software development. The size of suppliers ensures that small parties have little to say.<br><br>Finally, the sector is struggling with a misplaced sense of security through initiatives that do not always provide the implied solution. | The telecom sector considers the use of methods to follow actors as a good way to be able to achieve better protection, as is the use of strong cryptography for secure hardware and software. Public-private partnerships are encouraged, provided that they are channelled.<br><br>In the field of malware and DDoS attacks, various protection measures are being taken. | The sector notices that more is sent to recipients based on price. Customers implicitly expect perfect services. The growing use of mobile services allows for a greater dependence and thus the impact of disturbances on society increases.<br><br>Mobile operators are called to account for the malfunctioning of mobile devices that customers buy with a subscription. This increases the responsibility of the operators.<br><br>Parties that offer over-the-top services (such as calling and sending messages via the data network) are bound to other or more limited regulations than telecom providers. These parties have great freedom of movement and few obligations. |

| Sector | Manifestations | Threats: actors | Threats: tools |
|---|---|---|---|
| Transport (port, airport, rail) | In this year, the transport sector dealt with espionage attacks in which state actors were specifically looking for information on networks. There were a number of manifestations of a malware infection by an infected laptop from a supplier in the network.<br><br>General threats, such as ransomware, phishing and DDoS attacks have also manifested themselves. | Criminals are the most important threat for the transport sector. This group focuses on obtaining information for the smuggling of goods. Furthermore, state actors form an important threat. Internal actors are also an important actor, especially when they are the target of extortion by criminals. | The transport sector observes a shift from the physical to the digital domain when it comes to extortions. Blackmail, phishing and social engineering are increasingly digital. The aim here is often to get hold of access passes or login data.<br><br>Where WiFi networks are used for communication, for example in ports, drive-by attacks are carried out. Phishing e-mails are the order of the day, as is e-mail with malware attachments. The number of DDoS attacks has declined. |
| Insurers | The insurance sector has observed ransomware attacks in which users were infected via phishing e-mail. Also, they have had to deal with (disruptive) DDoS attacks. In addition, attackers use digital tools in support of insurance fraud. | The main actors for insurers are criminals, external actors in the chain and internal actors. | Phishing e-mails are the order of the day, as is e-mail with malware attachments. The number of DDoS attacks has declined. |
| Healthcare | The healthcare sector has observed manifestations of ransomware and phishing e-mails aimed at obtaining login data. In addition, many unauthorised login attempts have been detected on various systems. | Cybercriminals pose the biggest threat to the healthcare sector. Internal staff is seen as an important actor in the possibility of unknowingly leaking information. Hacktivists are sometimes also interested in attacking the healthcare sector. | Detected tools are, for example, self-inserted access points in the network and equipment remotely controlled by suppliers, which are used to gain access to the network. Phishing e-mails are becoming more and more sophisticated, thus increasing the chance of infection. |

| Resilience: vulnerabilities | Resilience: measures | Interests |
|---|---|---|
| ICS are widely used in the transport sector. Often, no updates are published for these systems or updates are not installed by suppliers. With ICS and other systems, the increase in remote management is responsible for an increase in vulnerabilities.<br><br>Another specific vulnerability is the management of user accounts by chain partners. Collaborating parties are often themselves responsible for managing accounts on systems of chain partners.<br><br>Use of cloud solutions by employees forms a vulnerability. | Network segmentation is increasingly being applied, as well as vulnerability scanning and network monitoring.<br><br>Life-cycle management ensures that both office and process automation systems are replaced, so that the landscape is slowly stripped of non-supported systems. | The quality of digital services is more important because the competition from, in particular, ports, is growing. The transport sector is important for the economy, which makes good cybersecurity important. At the same time, this offers opportunities: excellence in cybersecurity can provide competitive advantages. |
| Use of cloud solutions, sometimes on the staff's own initiative, provides for vulnerabilities in the processes of insurers. When using agile software development, insurers notice that security does not always get the proper priority from scrum masters. | Measures against DDoS attacks have proven effective. The white-listing of permitted applications for employees is experienced as successful, as is blocking USB ports and using adblockers preventing malvertising. | Expansion of the Personal Data Protection Act increases the impact (in terms of finance and image) of not detecting and reporting data breaches to the supervising authority in time. Because of the data breach reporting obligation, clients have a higher expectation with respect to the safety of digital services. As a result, measures for protection of personal data have become more important. |
| Humans are seen as the greatest vulnerability. Mergers of organisations enhance the risk, because attention is then focused on other matters and the motivation to handle matters decreases.<br><br>Technical vulnerabilities include linking medical devices to networks, the use of software by employees that they themselves install and (medical) equipment with obsolete versions of operating systems.<br><br>Use of private devices with apps creates vulnerabilities. Data breaches occur if doctors use messaging apps to exchange patient data. | The healthcare sector is in the process of setting up a Healthcare-CERT. The implementation of NEN 7510, 7512 and 7513 allows for more monitoring in the field of information security. On the technical side, more IDS/IPS and SIEM systems will be deployed. Workstations sometimes use sophisticated protection measures that look at behaviours rather than patterns. | The healthcare sector works in chains and exchanges in these chains occur, to an increasing degree, digitally. This creates a dependency. Through central infrastructures, the growth of these chain dependencies also increases. |

# Appendix 3 Terms and abbreviations

| | |
|---|---|
| 0day | See Zero-day vulnerability. |
| AIVD | General Intelligence and Security Service |
| Authentication | Authentication means finding out whether the proof of identity of a user, computer or application complies with the authenticity characteristics agreed in advance. |
| Bad hosting | Bad hosting is the conscious or unconscious provision of hosting by a provider that can be used for cybercrime purposes. |
| Bitcoin | A currency, see crypto currency. |
| Booter service | Online service carrying out DDoS attacks for 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. |
| BYOD | Bring your own device (BYOD) is a policy in organisations whereby personnel are permitted to use their own consumer devices for carrying out their work. |
| C2 | A Command & Control (C2) server is a central system in a botnet from which the botnet is operated. |
| CEO fraud | A type of fraud wherein a criminal poses as a director (CEO or CFO) of an organisation, specifically focusing on a financial officer of that organisation, to carry out a rogue transaction outside the procedures. |
| 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-secured website. |
| Certificate authority | A certificate authority (CA) in a PKI system is an organisation that is trusted to generate, issue and withdraw certificates. |
| Cloud | A model for system architecture based on the internet which is mainly based on software-as-a-service (SaaS). |
| 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. |
| Cryptocurrency | An umbrella term for digital currencies whereby cryptographic calculations are used as authenticity feature and for transactions. The bitcoin is the most common cryptocurrency. |
| Cryptoware | Type of ransomware that encrypts files on a computer or in a network. The key is only issued upon payment. |
| Cybercrime | Form of crime aimed at an IT system or the information processed by this IT system. |
| Cybercrime-as-a-service | Cybercrime-as-a-service is a method used in the underground economy in which criminals without technical knowledge can use (paid) services of others to commit cybercrime. |

| | |
|---|---|
| Cybercriminal | Actors who commit cybercrime professionally, the main aim of which is monetary gain. The CSAN differentiates among the following groups of cybercriminals:<br>• in a strict sense, those who carry out attacks themselves (or threaten to do so) for monetary gain;<br>• criminal cyber service providers, those who offer services and tools through which or with which others can carry out cyber attacks;<br>• cyber dealers or service providers for stolen information;<br>• 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. |
| Cybersecurity | 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. |
| Dark web | Dark web is used as a designation for websites that are only accessible through Tor so that all actions carried out on these websites cannot be technically traced to the end user. |
| 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 renders the website inaccessible. |
| DigiD | The digital identity of Dutch 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 their 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 an extension to DNS with extra authenticity and integrity monitoring. |
| Doxing | Doxing is the collection of personal data from various sources, which data is then usually published online. |
| Dropper | Malware can be packaged in a dropper to bypass detection. The function of the dropper is to install malware on the system where it is to be run. |
| 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. |
| 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 and/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. |
| FIOD | Dutch Fiscal Intelligence and Investigation 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. |
| ICS | Industrial Control Systems (ICS), also called Supervisory Control And Data Acquisition (SCADA), are measurement and control systems used, for example, to control industrial processes or building management systems. Industrial control systems collect and process measurement and control signals from sensors in physical systems and steer the corresponding machines or devices. |
| Identity theft | The abuse of someone else's identity data to commit fraud. |
| Incident | An incident is an IT disruption that limits or eliminates the expected availability of services, and/or 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 (legitimacy), 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 cybersecurity 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. |
| 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 organisations in the critical infrastructure 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 | Contraction of malicious 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 |
| 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. |
| 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. |
| Ransomware | Type of malware that blocks systems and/or 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) 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 leaks found. Responsible disclosure is based on agreements that usually mean that a reporter will not share his discovery with third parties until the leak 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 cyberattacks motivated by mischief. |
| SIDN | 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 inducing the victim to perform a particular action. |
| Spear phishing | Spear phishing 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 as big an effect as possible without being noticed. |
| SPF | Sender Policy Framework is a protocol used by the owner of a domain name to indicate which servers are allowed to send legitimate 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. |
| SWIFT | The Society for Worldwide Interbank Financial Telecommunication is an organisation that facilitates international payment transactions. |
| 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. |
| THTC | National High Tech Crime Unit (Dutch National Police). |

| | |
|---|---|
| Threat | The Cyber Security Assessment Netherlands defines purpose and threat as follows:<br>• The higher purpose (intention) may be strengthening an organisation's competitive position; political/national gain, social disruption or threatening a person's life.<br>• In the Assessment, threats are categorised as follows: digital espionage, digital sabotage, publication of confidential data, digital disruption, cybercrime 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 technology 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. |
| 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

October 2016