# Information security in

# 2018

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

# CONTENTS

## KEY INFORMATION SECURITY THREATS AND PROTECTION AGAINST THEM

## MOST SIGNIFICANT CYBER SECURITY PHENOMENA

## NATIONAL CYBER SECURITY CENTRE FINLAND PROVIDES SERVICES

## CYBER WEATHER 2018 AND A LOOK AT CYBER YEAR 2019

# Cyber security is everyone's business

The year 2018 was a time of change. In the summer we moved to new premises in Kumpula, and at the end of the year we became part of the new Finnish Transport and Communications Agency Traficom. After extremely positive but also highly labour-intensive experiences, we can fully focus on developing our operation in 2019.

The strong cooperation between the private and public sectors is the foundation of the Finnish security culture. I have not come across anything similar anywhere else in the world.

There are undoubtedly many reasons for this tradition in cooperation. Firstly, people involved in information security in Finland know one another well; names quickly become familiar faces. It is also easier to trust people you know. Solid trust between partners is another factor that supports cooperation. Thirdly, partners feel that they genuinely benefit from this cooperation, which is an enormous resource for us. We receive extremely confidential information from our partners in an agile and flexible manner, without coercion based on law. One of our priorities is the responsible processing of confidential information. According to feedback received from our stakeholders, efficient and reliable cooperation is our key strength, without forgetting our professional skills. We will uphold these in the future also.

However, there is still room for improvement in this cooperation. We must ensure that we do not operate merely in a bubble of information security professionals and that also the public benefits from the results of our cooperation.

Several cyber security threats may gradually erode our trust in digital environments, if our senses of security and control disappear. The most significant information security threat in 2018 was gradually spreading Office 365 scams used for phishing information from users. The importance of human information security should not be forgotten or underestimated. Cyber security cannot become a civic skill in everyday life if we do communicate about it in a relatable and understandable manner. I hope that the 'Teijo ja turvalistit' campaign and the Longer the Better password generator have reached as many people as possible. We wanted to bring information security to every home with these 2018 citizen campaigns.

Our goal is to develop Finnish cyber cooperation so that it works even more closely than before. The intention is to build the whole package around our HAVARO service, enabling us to efficiently distribute and refine information about threats. Critical services offered to the public through closer cooperation can be protected better than before, because protection against information security threats and recovery from them would be faster than at present. I believe that, by means of a "cyber ecosystem", both the private and public sectors can provide electronic services that children, young people, adults and the elderly can use without feeling unsafe.

*We welcome you to join us, because this joint project needs all of us!*

Helsinki, 31 January 2019,
**Jarkko Saarimäki**
Director
National Cyber Security
Centre Finland (NCSC-FI)
Finnish Transport and
Communications Agency
Traficom

# KEY INFORMATION SECURITY THREATS AND PROTECTION AGAINST THEM

## TOP 5 threats and solutions for private individuals and organisations

# PRIVATE INDIVIDUALS

## THREATS

**Criminals attempt to steal your user credentials**
The criminal uses the stolen credentials to try and access the victim's email account, for instance. Email is used as the password recovery address in several online services, so it is the key to many places.

**Scams are part of daily life on the internet**
Fake online stores and subscription traps steal money from consumers. Emails that extort people with sensitive material as well as tech support scams have also been on the rise.

**Poorly protected devices**
Consumers are offered smartphones, computers and home IoT devices with non-existent information security: the use of default passwords, with hardly any product support or updates available. Such devices should not be online, disrupting the operation of communication services.

**Fake applications in official application stores**
Applications installed on a phone can forward more information to other parties than you have accepted, and even spy on and steal your data.

**Valuable information leaks from online services**
User and payment detail leaks are continuously found from genuine online stores and social media services – criminals can use these in their scams, for example.

## SOLUTIONS

**Do not give unnecessary access rights to applications**
The rights of applications can usually be edited even after installation. A flashlight app works without access to your contact list or photos.

**Verify that a message you have received and its attachments are genuine**
A scam message can come via email, as a text message, phone call or private message on a social media service. If you are in doubt, verify the accuracy of the message contents by phone, for instance.

**Password managers and two-factor authentication**
Passwords that are long and secure enough are difficult to remember. Enable two-factor authentication (2FA/MFA) especially in email accounts, social media services and the most common cloud services whenever possible.

**Protect yourself with information security software**
Malware protection and a firewall often come in the same package. Use them. Remember to heed the warnings and instructions they give.

**Check your credit card invoice regularly**
Be careful especially after shopping online, because data breaches at genuine online stores have become more common. You can cancel your card if necessary. Please note that a web criminal will not be caught if the offence is not reported to the police.

# ORGANISATIONS

## THREATS

**Criminals try to get rich with your information**
Scammers and phishers want access to an organisation's information systems and benefit from the data they steal. Some scams are highly credible and well targeted, and they can cause serious financial losses.

**Outsourced services as additional avenues for attackers**
An attacker may gain access to a company through the systems of its partners and subcontractors, especially if the company outsources its key services and also provides them to its partners. Attacks or incidents in systems can spread widely and to surprising places, if a company is unable to control its own technical environments.

**Lack of visibility**
Organizations do not necessary know their own environment well enough. Detecting and locating attacks is extremely difficult if a sufficient amount of logs is not collected. For example, software vulnerabilities are used in attacks almost immediately once information about a vulnerability has become public.

**Valuable information activates spies**
In Finland, valuable information includes political decisions, high technology and innovations. Foreign powers can also be interested in Finnish elections. During the Finnish Presidency of the Council of the EU, Finland is a potential target for cyber espionage and influencing. In addition to the media, hacktivists and political groups also become active.

**Denial-of-service attacks are frequent phenomena**
Every organisation must prepare for denial-of-service (DoS) attacks.

## SOLUTIONS

**Include responsibilities for information security in all agreements and contracts**
Outsourcing can provide you with the information security skills that are outside your own core operations. You cannot outsource responsibility without including it in a contract.

**Basic hygiene for devices and software**
Maintain and update all devices that are connected to the network. Create a routine operating model for regular, frequent updates and backups.

**Arrange training, exercises and tests**
Exercises are used to test regular operations and find development priorities. Learning from your own cases is an essential part of preparedness.

**Embed information security as an operating method in the work community**
Information security must be taken into account in all operations. It must be part of comprehensive risk management and preparedness.

**Know your systems and services**
This enables efficient maintenance and preparedness, and logging is an essential part of it. Consider automation if it makes the work more efficient and improves the operation of the processes.

# MOST SIGNIFICANT CYBER SECURITY PHENOMENA

## Scammers did not rest

## From email accounts to invoicing fraud

The 2018 scam year was characterised by extortion scams, Office 365 phishing, and CEO scams. Subscription traps and phishing of banking credentials that became familiar in previous years showed no signs of abatement. Different scams have only increased.

The year 2018 will certainly be remembered for Microsoft Office 365 email service related phishing for credentials. This is not a new phenomenon, because attackers have always tried to gain access to different organisations' accounts. Thus far, phishing has required time-consuming background work when a criminal has had to study every organisation's remote use interface separately. Now the Office cloud service platform that is widely in use has harmonised the email services of various organisations. This has also made phishing easier: the same scam message can be sent to several organisations that use the same service.

We published a critical alert on phishing in June 2018 when hundreds of email accounts from dozens of organisations fell into the wrong hands. Thousands of new scam messages were forwarded from accounts in the criminals' possession, and the worst phishing wave of the year steamrolled like an avalanche from one organisation to the next.

Hijacked email accounts were used for other offences too. Criminals were able to monitor message traffic on the accounts and gain access to internal information from organisations. The phishers used this information to carry out invoicing fraud, falsify invoices and swindle money from the organisations themselves and from their customers.

## Fraud and diversion

Online scammers have endless resourcefulness. All kinds of information can be misused, such as for extortion scams. Web users have become familiar with different password leaks when ancient password lists surface, for services forgotten years ago. If enough expired passwords are available, they can easily be used to scare people into believing that now all of their other details have also been stolen.

Extortion emails spread around the world proved to be scams combining old, leaked passwords and shaming people for watching porn. These messages proved to be scams. Even if a scammer did not have sensitive material on their victim, a random old password leak added credibility to the scam message: Pay the ransom or I will reveal everything about you!

> *“Criminals were able to monitor transactions on the accounts and obtained internal information from organisations.*

## Scam text messages to mobile devices

More and more people use mobile devices to browse the web. This has also shifted the focus of scammers who approach their victims with text messages. Scam messages flood both email inboxes and smartphones. A web link included in a text message may lead to a subscription trap or phishing, in the same way as an email message.

Consumers are lured into subscription traps with false marketing and promises of lottery prizes. Products by famous brands, TV sets and phones for a couple of euros are typical baits. A consumer is tricked into providing a credit card number under the guise of a raffle or delivery fee. The prize is never delivered, but the consumer will realise having committed themselves to a nominal service for a high monthly fee charged to the credit card.

## Can anything be done about such scams?

We inform the public of current online dangers by publishing information security alerts. Our alerts have been noticed widely, and they have effectively crossed the media threshold. Some potential victims have probably averted danger, but still too many have fallen into the trap. Organisations, in particular, must take responsibility for educating their employees and keeping them aware of the dangers of scams, for instance. As an information security authority, we help them in any way we can.

## Crimes are planned more carefully than before

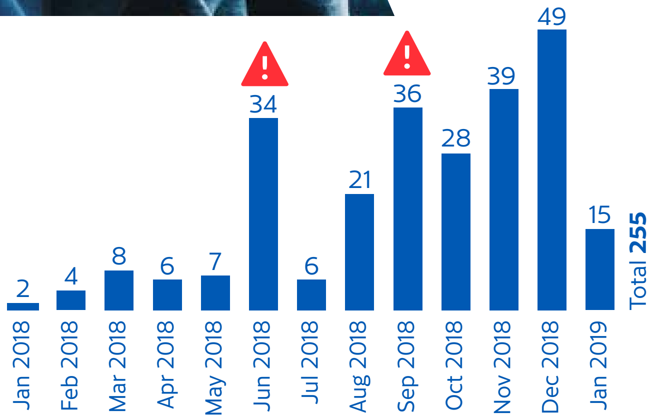
In many ways, the past year opened eyes from the perspective of the police also. Traditionally online fraud targeting Finland has occurred on domestic trading places, as email scams and as “Nigerian letters”. However, we experienced a new phenomenon in the past year: Microsoft Office 365 phishing.

The modus operandi vary slightly, but the common observation is that crimes are planned more carefully and with greater detail than before. In practice, this is a data breach after which the actual fraud scheme is planned based on information obtained from email or other services on the platform.

Phishing related to cloud services is actually an extension of CEO fraud that has been with us for a while, where hundreds of millions of euros have been lost globally. Some perpetrators have been caught through international cooperation. A fraudster who was caught through collaboration between the police in Israel, France and Belgium and the FBI had amassed approximately EUR 1.2 million as proceeds of crime.

Dozens of criminal cases are under investigation in Finland. The losses amount to hundreds of thousands of euros.

**Tomi Liesimaa**
National Bureau
of Investigation



*Number of tickets related to the Office 365 scam in January 2018 – January 2019. Clear peaks in June, September, November and December.*

### 2017

Aug 2017 We received a report of Office 365 phishing and communicated it.

### 2018

Feb 2018 In February–March 2018, Office 365 detections began to attract attention again.

11 Jun A critical alert was published. ⚠

8 Aug The alert was reduced from critical to severe. ⚠

21 Sep The alert was increased back from severe to critical. ⚠

26 Sep Two-factor authentication was bypassed.

4 Oct Scam messages were falsified as a secure mail notification.

26 Oct The alert was reduced from critical back to severe. ⚠

27 Nov More victims: 100 credentials were stolen with a phishing link to a PDF file.

11 Dec Regional restrictions on log-in were bypassed by means of VPN connections.

20 Dec Scam messages were falsified as a voicemail notification.

28 Dec Scam messages were distributed on the SharePoint pages.

### 2019

Jan 2019 The situation remains severe in January 2019. ⚠

# Phases of the Office 365 scam

June 2017 saw a high number of phishing emails in Finland. The campaign was mostly targeted at corporate executives and employees in IT maintenance. After the successful phishing of email credentials, unauthorised email forwarding rules were added in the organisations' Office 365 Exchange Online cloud email service which were difficult to detect with common administrative tools.

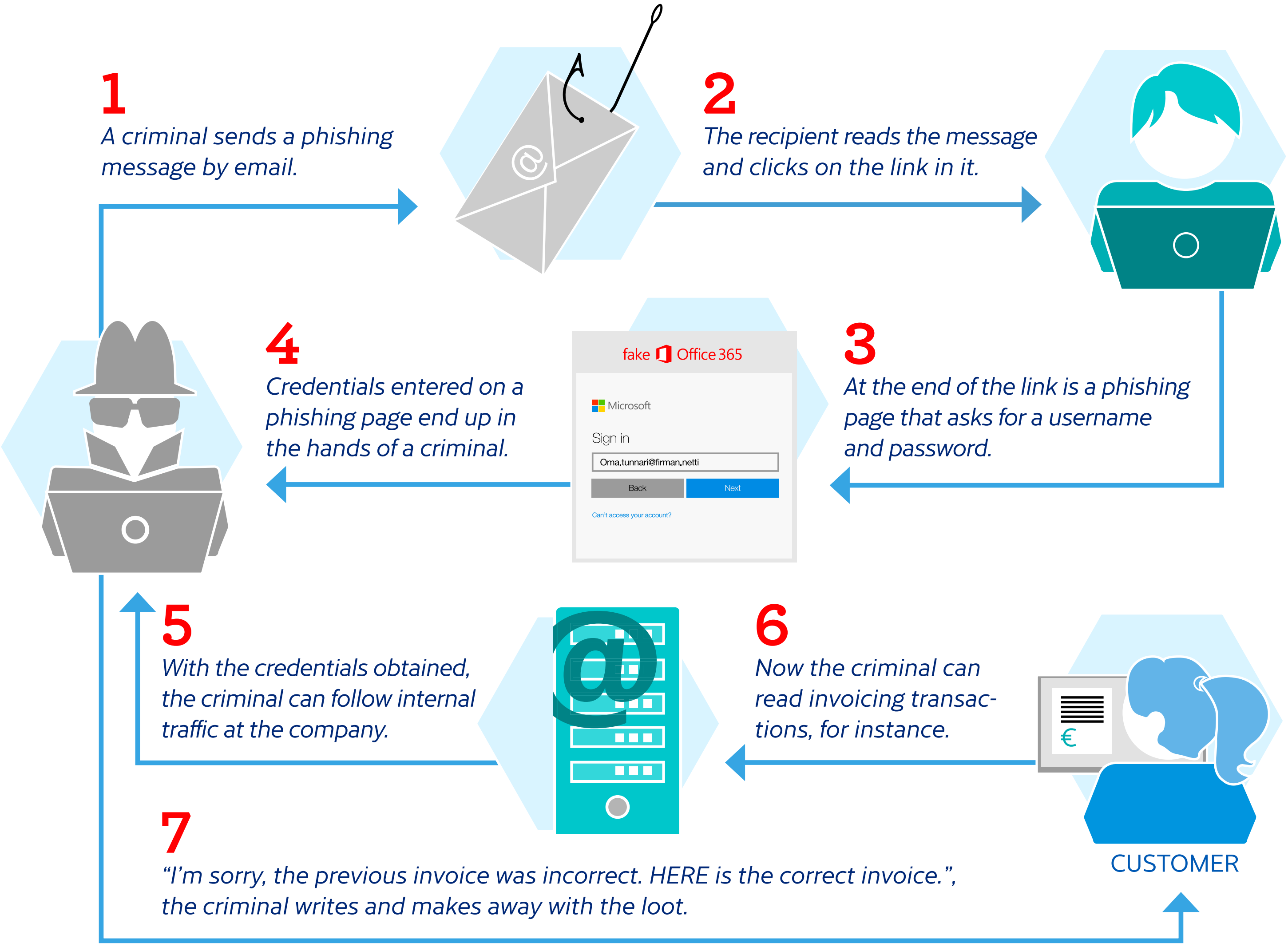
In August 2017 we advised people to pay attention to the security of authentication, and in our Information Security Now! article we recommended adopting two-factor authentication, due to the rampant phishing of passwords. In September we issued an alert on targeted phishing. We communicated the problem again in November, because the phenomenon did not seem to be fading away.

In February 2018 we again gave organisations a wake-up call of the gravity of the situation. We published an Information Security Now article which included example pictures of a phishing site with the Office 365 and OneDrive theme. We also warned of a PDF document in circulation that included a link to a phishing page.

Despite our active communication, the number of cases brought to our attention doubled. In June we decided to publish a critical alert on the topic, because organisations that were using Office 365 had to take action to rein in the problem! The alert received a great deal of public attention and visibility but the phenomenon did not go away, instead it became increasingly worse.

In September 2018 we discovered that two-factor authentication was not enough if the system allowed it to be bypassed with older client devices. In October scam messages began to spread, disguised as secured mail notifications. O365 scammers only seemed to increase in numbers, and new victims were tricked into giving their credentials on criminals' phishing sites.

The number of reported phishing cases did not significantly decrease even late in the year, so we have been unable to end the alert.



1 *A criminal sends a phishing message by email.*

2 *The recipient reads the message and clicks on the link in it.*

3 *At the end of the link is a phishing page that asks for a username and password.*

4 *Credentials entered on a phishing page end up in the hands of a criminal.*

5 *With the credentials obtained, the criminal can follow internal traffic at the company.*

6 *Now the criminal can read invoicing transactions, for instance.*

7 *"I'm sorry, the previous invoice was incorrect. HERE is the correct invoice.", the criminal writes and makes away with the loot.*

# Vulnerabilities and malware

> *“Detections of malware in home routers and IoT devices account for almost 60% of all malware detections made by the NCSC-FI.*

## Vulnerabilities were kept in line, and epidemics were avoided

The most significant vulnerability phenomenon in 2018 related to vulnerabilities found in the processors of different manufacturers.

The web began to untangle in January, when the Spectre and Meltdown vulnerabilities showed that an attacker could gain access to data of another program or operating system running on the same processor. Due to Spectre and Meltdown, more processor vulnerabilities were investigated around the world than before, and several new cases were discovered. Processor vulnerabilities have especially affected cloud platforms and other multi-user environments, but some of them also pertain to ordinary home users.

In the past year numerous critical vulnerabilities were found in the network implementation of operating systems, as well. These vulnerabilities impacted Windows, Unix, MacOS and FreeRTOS, practically all the operating systems. A denial-of-service status, for instance, could be caused by utilising different vulnerability types. At its most severe, a vulnerability allowed attackers to run their own program code in the target system. However, epidemics spreading like worms were avoided, because an effective exploitation method was not immediately available for such vulnerabilities.

## Malware mined virtual currency, clicked on ads, and penetrated online banks

The years 2017 and 2016 saw a rampage by not-Petya, WannaCry and Mirai, but 2018 was easier in this respect. Ransomware that encrypts a computer's hard disk and demands ransom for decryption, which became more common in earlier years, decreased despite our forecasts.

Instead of using ransomware, cyber criminals earned revenue by mining virtual currency with the resources of their victims' computers. We detected malware mining virtual currency in Finland too. The most visible case in the first half of the year was the WannaMine malware, which affected City of Lahti's information systems, mined virtual currency and spread by itself. A miner can also be hidden in the source code of a website, so currency can be mined in the browser of users visiting the site, almost unnoticed. This does not require an infection of malware on the victim's computer.

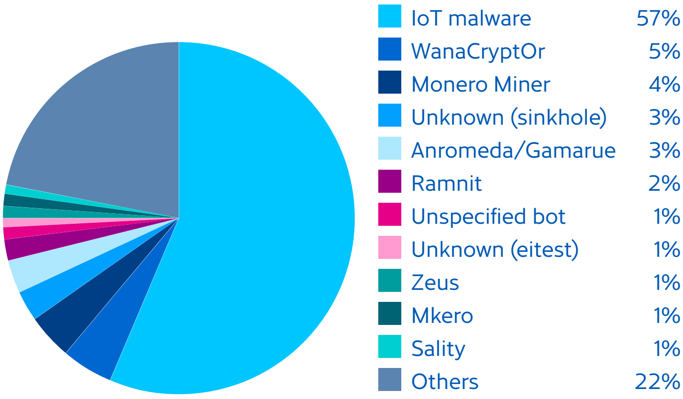
We made observations in Finland of the Kovter and Emotet malware that spread around the world. Kovter is malware that "clicks" on online ads, allowing a website to artificially increase its own advertising revenue. Emotet is multipurpose malware that can be used for stealing credentials or downloading other malware, for instance.

*"If regular updating of a device is impossible, it must be disconnected from the internet.*

## Spreading through email attachments, routers and unpatched computers

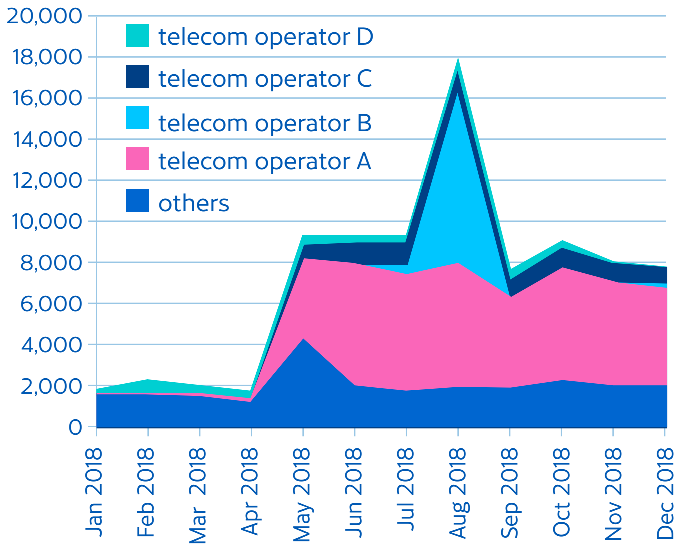
Email attachments were the most common way to distribute malware in 2018. Often the attachment is a document that contains macros and infects a computer with malware.

Our detections of malware in home routers increased significantly in the summer of 2018. These detections concerned especially certain home router models of a few telecommunications companies. At present, different malware in home routers and other IoT devices account for a large share, almost 60%, of all malware detections reported to us.



*IoT malware accounted for almost 60% of all the malware we detected in 2018.*

> *“Detections of malware in home routers and IoT devices account for almost 60% of all malware detections made by the NCSC-FI.*



*Detections of IoT malware became more commonplace in 2018. Most detections pertained to a few telecommunications operators. A peak was seen in August 2018.*

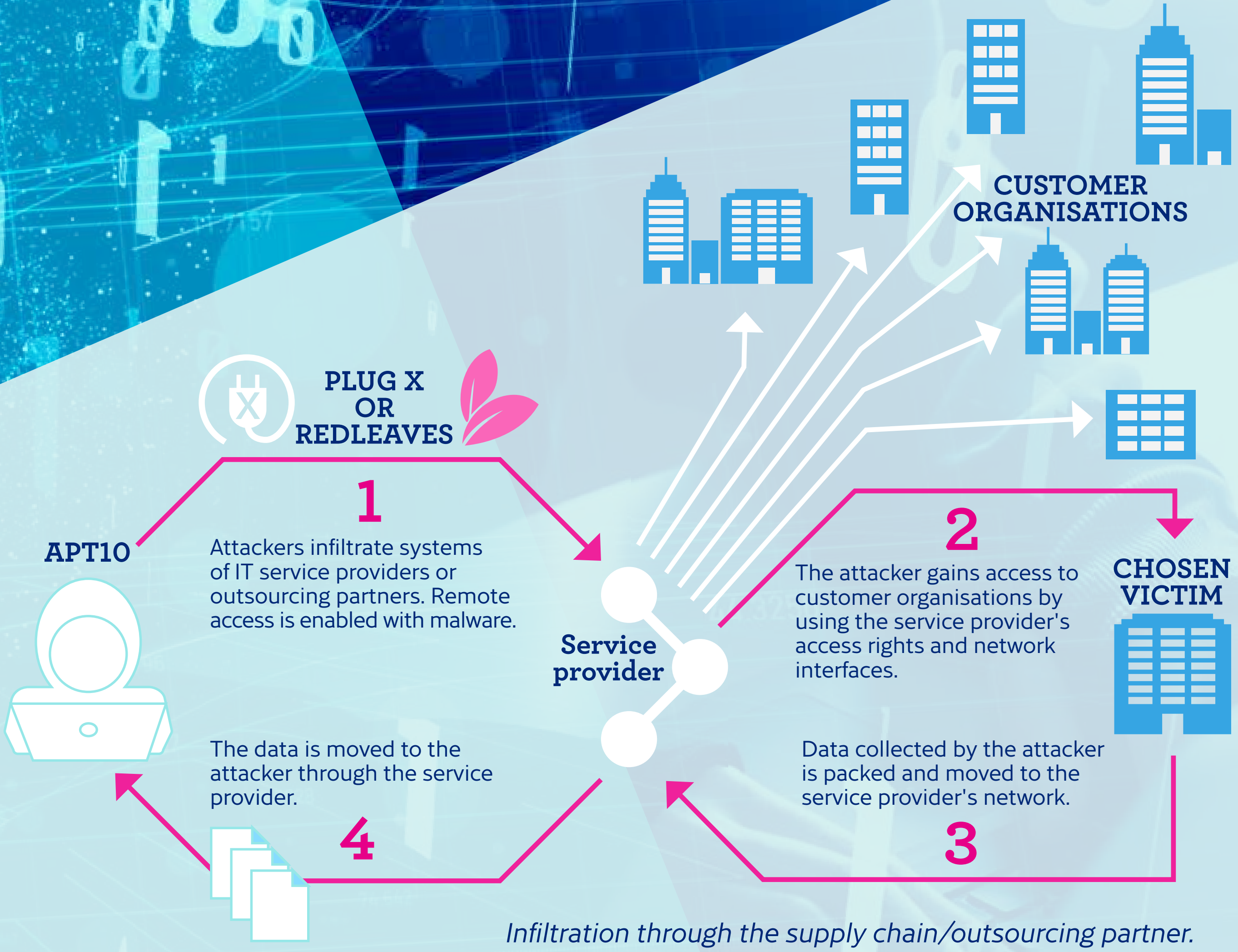
We still see very old malware, as well. For example, the Zeus malware, found in 2007, is still around. This is a typical phenomenon, probably because some computers are never updated or restarted. Users have forgotten to maintain such devices after installation, so they have become fertile ground for different malware infections.

Whether it is a network server of a large corporation or a webcam used at home, all devices connected to the internet should be maintained and their updates applied. If regular updating of a device is impossible, it must be disconnected from the internet.

Criminals are constantly scouring the internet for vulnerable devices. A device that is online and has a vulnerability, with a public method for exploiting that vulnerability, is quickly hacked. Devices that have been hacked take part in DoS attacks, mine virtual currency or send spam.

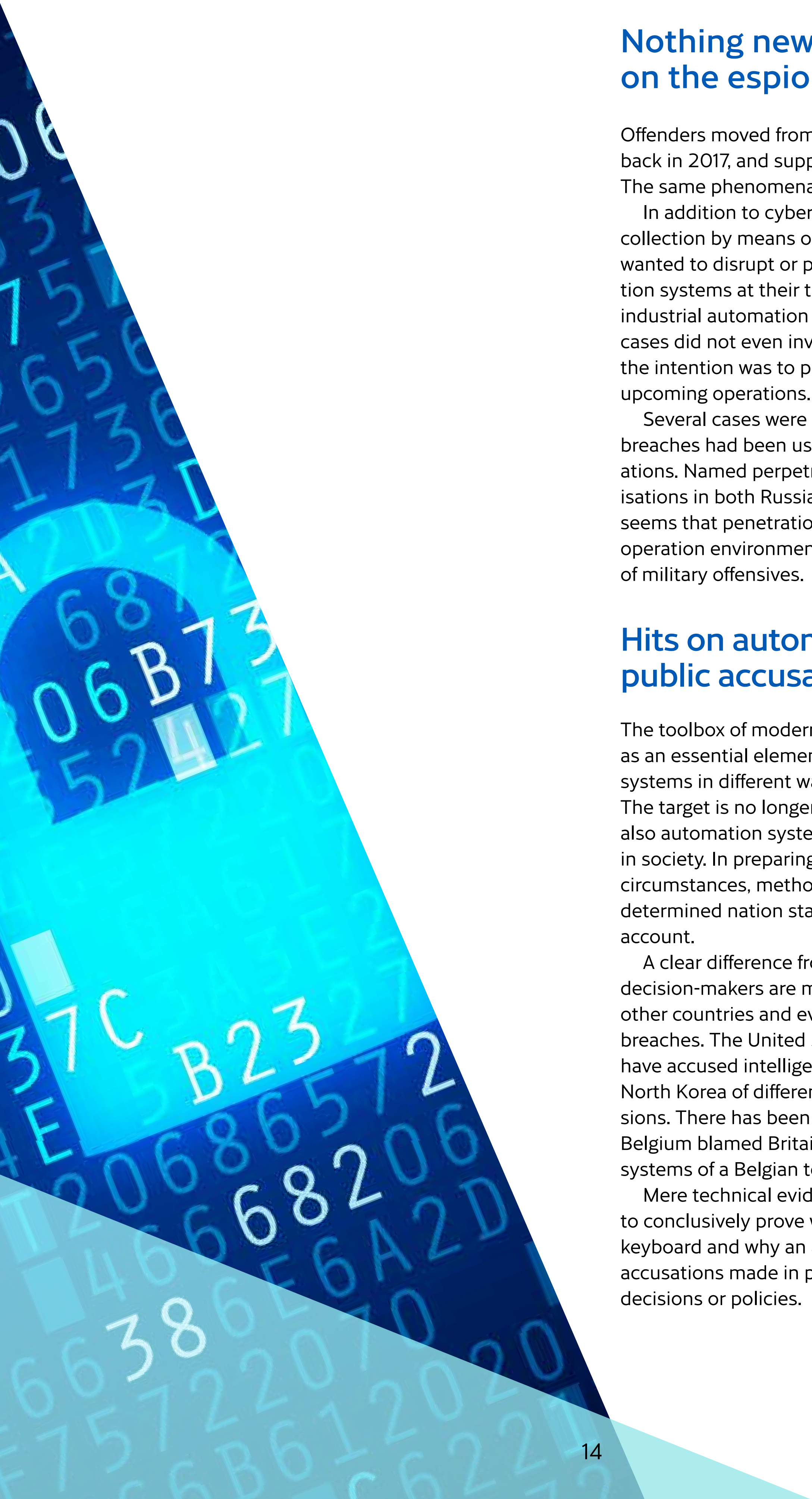
# Spying and influencing

> *“The target is no longer ordinary ‘office technology’ but also automation systems used to run vital operations in society.*


CUSTOMER ORGANISATIONS
PLUG X
OR
REDLEAVES
1
APT10
Attackers infiltrate systems of IT service providers or outsourcing partners. Remote access is enabled with malware.
Service provider
2
The attacker gains access to customer organisations by using the service provider's access rights and network interfaces.
CHOSEN VICTIM
The data is moved to the attacker through the service provider.
Data collected by the attacker is packed and moved to the service provider's network.
4
3

*Infiltration through the supply chain/outsourcing partner.*

*Source: BAE Systems Threat Research Blog
https://baesystemsai.blogspot.com/2017/04/apt10-operation-cloud-hopper_3.html
https://2.bp.blogspot.com/--sBNjr4znWk/WN573Vvsfml/AAAAAAAAAno/OKLwDezpCF-gLwQt8k-EfvG7Ptn6nETefACLcB/s640/infographic.png



## Nothing new on the espionage front

Offenders moved from pure espionage to influencing back in 2017, and supply chains attacks were obvious. The same phenomena stayed on the surface in 2018.

In addition to cyber espionage, i.e., illegal data collection by means of information networks, attackers wanted to disrupt or paralyze the operation of information systems at their targets. These targets varied from industrial automation to the Olympic Games. Some cases did not even involve actual sabotage, instead the intention was to prepare a foothold for possible upcoming operations.

Several cases were publicized in 2018 where data breaches had been used in support of military operations. Named perpetrators included military organisations in both Russia and the United States. It now seems that penetration methods related to the cyber operation environment have become an integral part of military offensives.

## Hits on automation systems and public accusation of attackers

The toolbox of modern hybrid influencing includes, as an essential element, infiltration of information systems in different ways and for different purposes. The target is no longer ordinary "office technology" but also automation systems used to run vital operations in society. In preparing for incidents and exceptional circumstances, methods for preventing action by a determined nation state actor must also be taken into account.

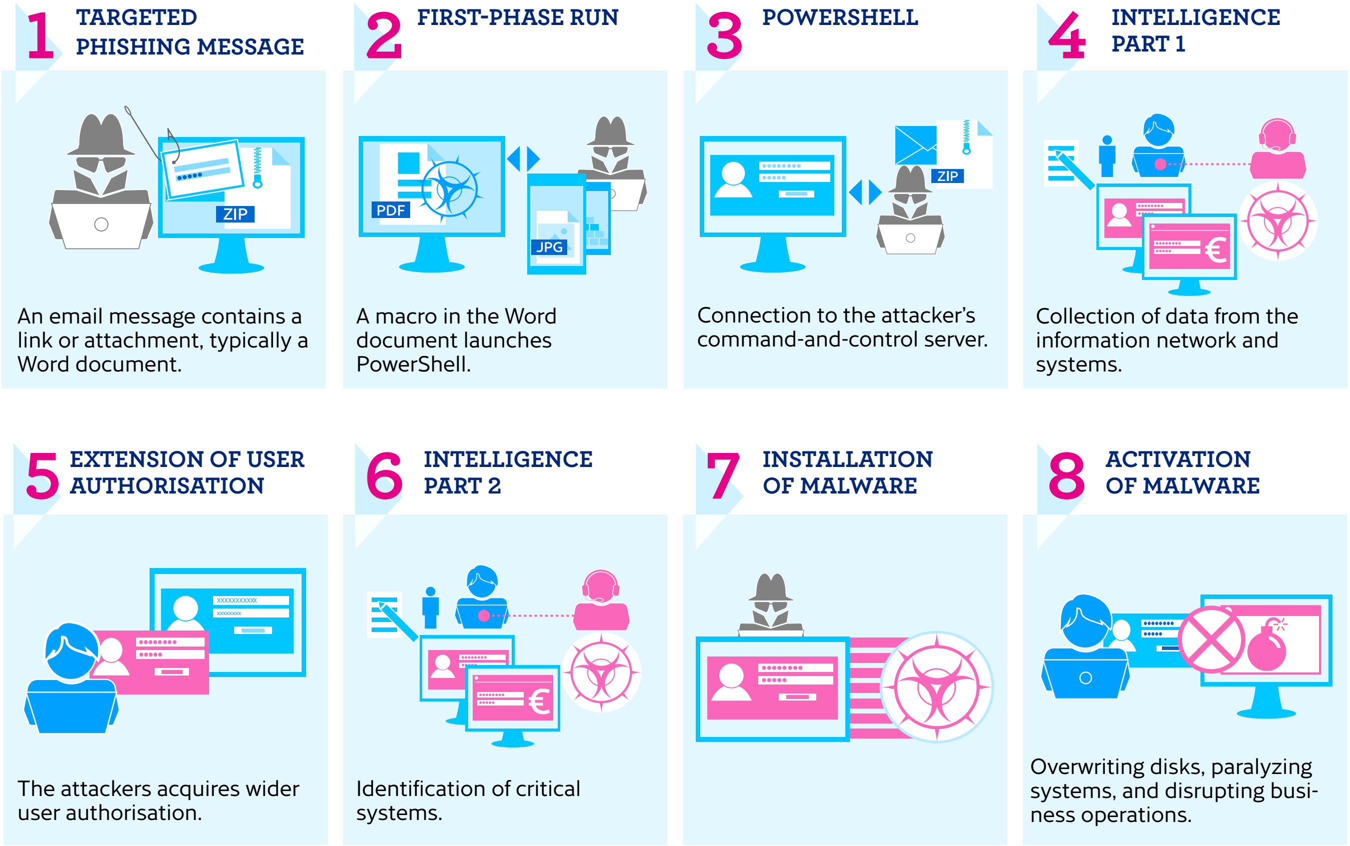
A clear difference from the past is that political decision-makers are more willing to publicly blame other countries and even individual officials for data breaches. The United States and Britain, in particular, have accused intelligence services of both Russia and North Korea of different data breaches on several occasions. There has been turmoil in Europe too, like when Belgium blamed Britain for infiltrating the information systems of a Belgian telecommunications operator.

Mere technical evidence makes it almost impossible to conclusively prove who was behind an attacker's keyboard and why an attack was made. Especially accusations made in public are often based on political decisions or policies.

## Modern corporate espionage is more difficult to detect than before

In espionage against businesses, data breaches made through supply chains were emphasised in 2018 also. Software update servers and maintenance services of information systems can be used to infiltrate several targets at the same time. Detecting attacks made through supply chains is significantly more difficult than with targeted, harmful emails, for instance.

For the EU Commission, for example, to intervene in corporate espionage by nation state actors, businesses would need to submit an estimate of the financial losses arising from cyber attacks. Such an estimate should include indirect costs in addition to direct expenses, which include costs related to the investigation of data breaches and reconstruction of information systems. Indirect costs, on the other hand, include losses caused by the theft of intellectual property and loss of business opportunities.



1 TARGETED PHISHING MESSAGE

An email message contains a link or attachment, typically a Word document.

2 FIRST-PHASE RUN

A macro in the Word document launches PowerShell.

3 POWERSHELL

Connection to the attacker's command-and-control server.

4 INTELLIGENCE PART 1

Collection of data from the information network and systems.

5 EXTENSION OF USER AUTHORISATION

The attackers acquires wider user authorisation.

6 INTELLIGENCE PART 2

Identification of critical systems.

7 INSTALLATION OF MALWARE

8 ACTIVATION OF MALWARE

Overwriting disks, paralyzing systems, and disrupting business operations.

*Progress of infiltration. The last phase is a successful data breach.*

* Source: IBM X-Force IRIS Team
https://securityintelligence.com/the-full-shamoon-how-the-devastating-malware-was-inserted-into-networks/

# Denial-of-service attacks

> *“The average size of DoS attacks continues its steady growth. In late 2018 it was completely normal that even attacks against individual consumers were over 10 Gbps. Attacks that use Memcached are here to stay but, fortunately, they have not generated major problems since the flood at the start. There is no end in sight for the growth of the attacks, so we should prepare ourselves for problems caused by denial-of-service attacks.*

**Osmo Soinio**
Telia

## Anyone can buy a DoS attack against the target of their choice

“Stresser services”, which provide DoS attacks, also offer free, short-term sample attacks. Statistics show that the majority, or approximately 75%, of all DoS attacks seen in Finland last for less than 15 minutes. The short duration but also the high number of these attacks suggest that they are probably free sample attacks by stresser services.

In April webstresser.org, the service for ordering DoS attacks, was shut down as the result of an international police operation. It was the world’s largest DoS service, and the shutdown reduced the number of attacks around the world. Still there are numerous services on the web where you can order a DoS attack against any online target.

DoS attacks typically last as long as they have an impact on the operation of the target. Usually the attacker stops when a DoS attack is mitigated and the operation of the service is restored. However, the attacker often simply changes the target and the attack continues against another service in the targeted organisation.

The typical volume of DoS attacks seen in Finland is approximately 1–10 Gbit/s. These volumes usually can have an effect on the operation of the service, unless specific preparations have made against DoS attacks. There are several attacks of more than 10 Gbit/s in Finland every week. The largest attack reported to us in 2018, which was directed at Finland, had a volume of approximately 90 Gbit/s, and it lasted several hours.

*“Approximately 75% of all DoS attacks seen in Finland last less than 15 minutes.*

## Highly visible attacks against the suomi.fi identification service

During the summer and autumn several denial-of-service attacks were made against the suomi.fi identification service, which undermined the operation of numerous government services. The identification service is a key component in the operation of many other services, so it is an attractive target for attackers.

The attacks against suomi.fi were perhaps the most visible example of denial-of-service attacks, but they were not the only ones. In all, several thousand DoS attacks were carried out in Finland in 2018. Indeed, it can be said that DoS attacks have become commonplace and they are being made on a continuous basis. However, not all attacks have visible effects on the operation of various services, thanks to efficient preparedness by organisations.

*“In all, several thousand DoS attacks were carried out in Finland in 2018.*

## Attack techniques have remained almost unchanged

Attackers use different techniques in the implementation of denial-of-service attacks, the most common of these being reflection attacks and online traffic sent from hacked terminal devices. Often these techniques are also combined. Reflection attacks utilise servers on the internet, such as domain servers of CLDAP directory services, to strengthen the attacking traffic. 2018 saw a rise in reflection attacks against incorrectly installed memcached servers.

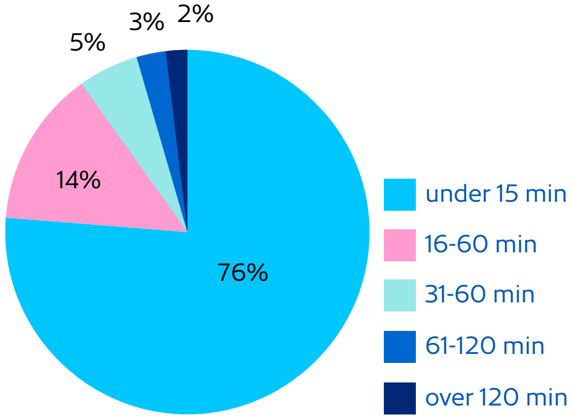
## No protection against attacks without preparation and planning

Denial-of-service attacks must be taken into account in the risk assessment of every organisation. For instance, if the availability of a company's online services is important, protection against DoS attacks must be planned and they must be prepared for in good time.

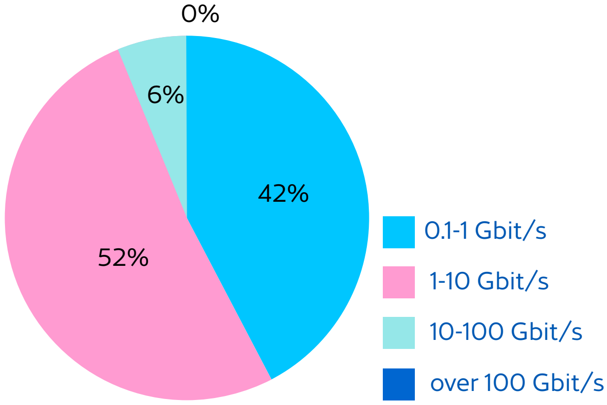
Protection methods vary for different types of attacks. In protection against application-level attacks, the online service must be designed so that it cannot be easily overloaded with individual requests, such as complicated database queries. When preparing against attacks that create multiple TCP connections, the network architecture, load balancing and content distribution must be designed so that the service is not jammed by the creation of simultaneous sessions. Services purchased from telecommunications operators, such as a client firewall and DoS protection, mitigate attacks based on traffic volume.

There is no individual "silver bullet" for protecting online services. The design of an online service, as a whole, must be aimed at high resilience against different attacks and the rapid recovery afterwards.

> *"A DoS attack is the most impressive threat to information security in terms of price-to-quality ratio but usually not the most severe one." It can be compared to an organised demonstration outside an office building: it attracts attention and prevents entry to customers. In the worst case an attack can jeopardise people's lives if it blocks critical services.*
>
> **Jarna Hartikainen**
> Head of Unit
> Traficom/National Cyber Security Centre Finland



*Duration of DoS attacks against Finland in 2018 (source: Telia).*



*Volume of DoS attacks against Finland in 2018 (source: Telia).*

# Reliability of Finnish communications networks

*“In recent years, cooperation between the NCSC-FI and telecommunications operators has improved significantly and become more open than before.” Operators meet regularly in various working groups of the Transport and Communications Agency, dealing with the management and prevention of incidents. The cases and situations where cooperation is beneficial in terms of the functioning of society emerge naturally. The perspective is wider than that of an individual operator.*

*Rapid recovery from incidents, the functioning of critical national services, and preparedness for incidents is in everyone’s interests. Working services benefit all of us, so – despite a competitive situation – operators benefit from cooperation during extensive, technical incidents and exceptional circumstances.*

*These days even electricity companies and rescue departments take part in this collaboration. Now we are better able to ensure that the general public has access to data communication services that function as well as possible.*

**Tomas Lång**
DNA Oyj

## The situation has improved further

The number of significant incidents in Finnish communications networks has clearly decreased in recent years, and the same trend continued in 2018. Weather conditions caused the longest network incidents, but due to joint efforts by telecommunications and electricity companies, their effects remained moderate compared to previous years and the repair work proceeded efficiently.

In total we received almost 70 reports of significant incidents from telecommunications operators. Of these, 14 were severe, large-scale disruptions. The number of incidents decreased by approximately one third in comparison with the preceding year. However, there were more incidents in the “A” severity category than in the previous year. The number of incidents in the “B” severity category more than halved from the year before.

Approximately 50% of the “A” incidents involved the terrestrial television network, and most of them were caused by equipment malfunctions. Maintenance work of the networks, hardware and software used by telecommunications operators and software modifications caused communications network interruptions.

## Phones and the internet worked, reliability of critical systems must be improved

At the beginning of 2018, there were extensive power failures in Kainuu that lasted from a few days to more than a week. The Kainuu Rescue Department assumed general responsibility for managing the situation, which indicates the scope and severity of the incidents. The power failures also affected the operation of communications services, but major incidents were avoided. Emergency calls could be made, and those participating in rescue operations were able to use the mobile phone network for sharing information.

The reliability of Finnish communications networks has improved in recent years. One reason is network structures modernised by telecommunications operators, whereby a break in an individual link no longer causes extensive interruptions. The positive effects of changes made to the network can be seen in the 2018 statistics as a significant reduction in the number of incidents. The issue in 2018 was incidents in individual networks that caused interruptions in important national services. For instance, incidents in networks of hospitals and traffic control system prevented the use of services related to them. Organisations should prepare for incidents and interruptions in critical systems well in advance, during the tendering and contract phases.

## Telecommunications operators report security breaches more actively than before

The number of security breaches or threats varies from one year to the next, but we receive an average of one or two reports of significant cases each month. This was also the case in 2018. Most cases involve data breaches into information systems or unauthorised use of these, vulnerabilities in the systems of telecommunications operators, or large-scale DoS attacks made through telecom networks.

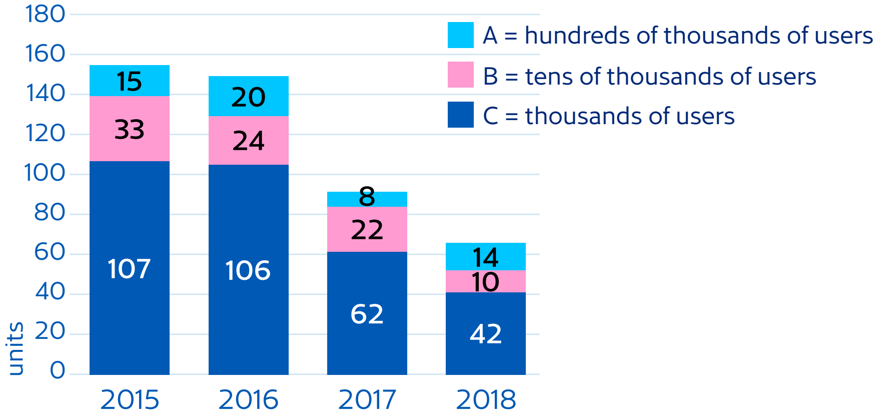
The number of reports involving personally identifiable information (PII) has increased in recent years. It is unlikely that the number of personal data breaches, as such, is growing. Instead, telecommunications operators are now better aware of the situations where personal data security can be breached and that all such situations must be reported.

The most common type of personal data security violation is the mismanagement of customer information. In such cases, a telecommunications operator processes its customers’ personal data erroneously, such that one customer’s personal data is revealed to another customer. For example, a customer who is ordering a new subscription accidentally receives a copy of the subscription order of the customer served before them. There may also be cases where a customer wants to postpone the due date of an invoice and contacts their operator by phone or chat channel, but a wrong phone number is saved in their contact details, so a confirmation text message of the postponement is sent to another customer.

We have collected information from telecommunications operators about significant security breaches or threats against communication networks and services since 2002. A breach or threat is deemed significant especially based on the protection of subscriber and user rights, the availability of the service, and geographical impact.

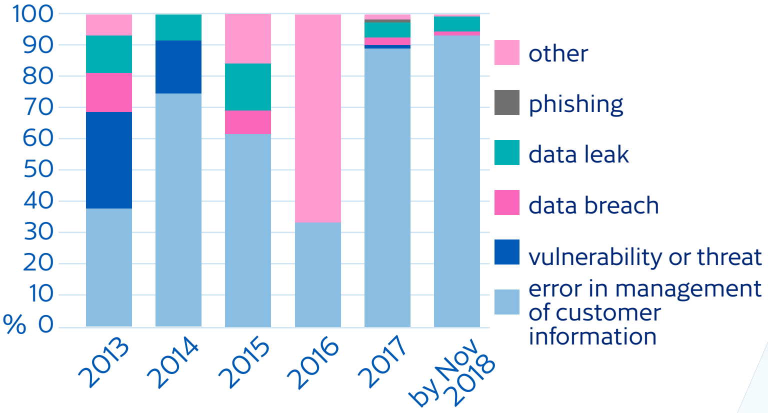
Since 2013 telecommunications companies have also reported privacy violations to the current Finnish Transport and Communications Agency. Most reports involve cases in which personal data is destroyed, lost, altered or disclosed to other parties accidentally or without authorisation.

## Number of significant incidents in different severity categories



*The annual number of significant incidents (A-C), in total, has decreased since 2015. In 2018 there were fewer C disruptions but more A disruptions than in 2017.*

## Case types of personal data breaches



> *“The positive effects of changes made to the network can be seen in the 2018 statistics as a significant reduction in the number of incidents.*

# Internet of Things

> *“An individual problem becomes a shared one when unsafe and poorly controlled devices are hijacked and used for denial-of-service attacks, for instance.*

## Data leaks, illicit viewing and DoS attacks

The Internet of Things (IoT) became an increasingly significant part of consumers' daily lives in 2018. Devices that monitor their environment and transmit data on it facilitate the lives of consumers by, e.g., controlling lighting in the home or reporting on the quality of sleep and heart rate. Unfortunately, information security problems related to the devices spread along with the new IoT innovations.

Defects in the information security of consumer equipment manifested as data leaks and privacy breaches. The cases show that few people can assess and control the information security of devices that are used at home, connected online, and which record or store data. An individual problem becomes a shared one when unsafe and poorly controlled devices are hijacked to be used for denial-of-service attacks, for instance. As critical and public services become digitalised, attacks on IoT devices can undermine the functioning of the whole society.

Currently there are no generally recognised or mandatory requirements for the information security of IoT devices, so preventing security defects is not easy. Rapid advances in technology have made a profound understanding of risks in devices and services difficult. Drafting of legislation has also been slow, but the situation appears to be improving gradually.

## Resolving defects through regulation, information security logo for secure devices

In September 2018, the State of California ratified the apparently first every law regarding information security of the Internet of Things. Furthermore, international standards concerning the Internet of Things and its information security are being drafted. Lighter principle-level policies were drafted during the past year in Germany and Britain, for instance.

In Finland, the Transport and Communications Agency Traficom has monitored the development of international regulation. Information security problems with IoT devices seem to be increasing more quickly than requirements concerning the equipment. This is why Traficom has begun developing an information security logo that would help consumers identify secure devices and thus make safer choices. Since adding information security features to equipment afterwards is expensive and often difficult, the logo is intended to encourage manufacturers to design devices that are secure throughout their life cycle. This is called "secure by design" thinking. In consumer devices, it has already been applied by Ikea in its Trådfri smart lights.

# Risk assessments on information security phenomena

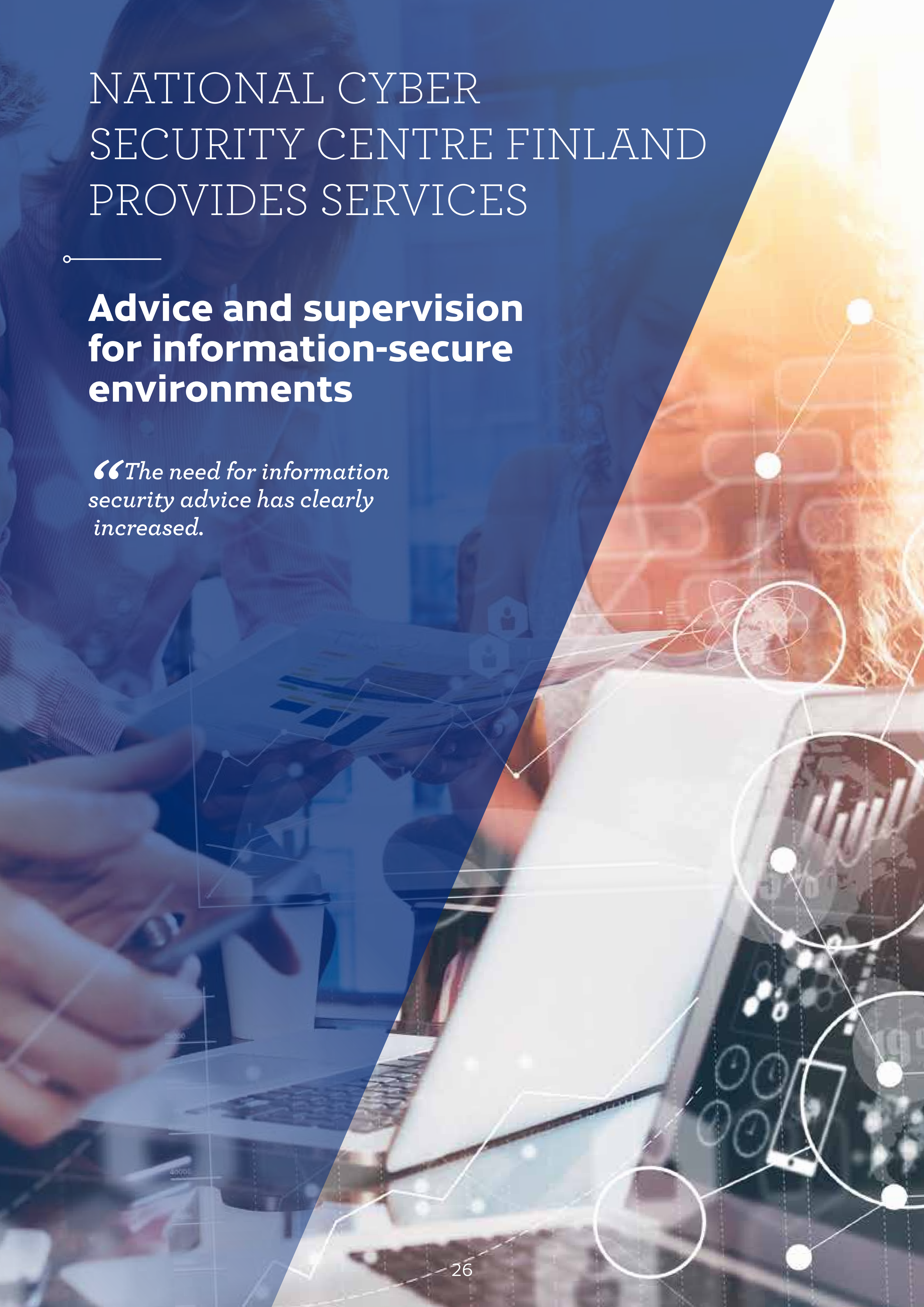
# Key information security risks for private individuals, organisations and central government

This is our evaluation of the most significant risks related to key cyber security phenomena in 2018. We have highlighted examples of cases how risks can be seen by private individuals, businesses, municipal organisations or central government. The direction of the arrow describes the trend of the situation compared with 2017. In our view, the general cyber security risk level in Finland in 2018 remained almost unchanged from 2017. Risks have grown in certain phenomena.

▶ The risk has remained unchanged

▲ The risk has grown

| | PRIVATE INDIVIDUALS | ORGANISATIONS | GOVERNMENT |
|---|---|---|---|
| SCAMS AND PHISHING | ▲<br>There is a great deal of phishing of banking credentials and credit card details. Scams and extortion are very common. | ▲<br>User accounts at cloud services have been targeted by numerous phishing campaigns. | ▶<br>CEO and invoicing scams hit central government as well. |
| DENIAL-OF-SERVICE ATTACKS | ▶<br>Hacked home routers and other IoT devices are used for making DoS attacks, for instance. | ▶<br>Denial-of-service attacks are frequent phenomena. Prevention of attacks must be planned so an organisation's online services remain operational. | ▶<br>Denial-of-service attacks are frequent phenomena. Organisations must protect both their own online services and those purchased from a service provider. |
| MALWARE AND VULNERABILITIES | ▲<br>Malware quickly infects IoT devices that are unsafely connected to the internet. | ▲<br>Offenders look for and hack into servers that are unsafely connected to the internet. Malware is distributed as email attachments. | ▶<br>Malware is distributed as email attachments. |
| SPYING | ▶<br>Social media activists who deal with politically sensitive subjects may be targeted by cyber espionage. | ▲<br>Spying on critical infrastructure companies seems to have increased. | ▶<br>Central government is still a significant target of cyber espionage. |
| INTERNET OF THINGS, IOT | ▶<br>Private data is revealed through devices that have been connected to the internet unprotected. Such devices are also utilised in bot networks. | ▲<br>Network resources can be accessed by utilising security defects in IoT devices. Details on equipment and users may end up in the hands of attackers from public sources also. | ▲<br>IoT devices involve a risk to reputation, in particular. For instance, movements and positions of soldiers can be monitored through smartwatches. |
| COMMUNICATION NETWORKS | ▶<br>Use of digital services is growing, but people are not fully dependent on their operation. Resilience for short incidents is at a good level. | ▲<br>There are fewer incidents, but dependence on digital services is increasing. Since preparedness for incidents is inadequate, the effects are reflected on consumers too. | ▲<br>Dependence on digital services is growing. Preparedness for incidents varies. |



# NATIONAL CYBER SECURITY CENTRE FINLAND PROVIDES SERVICES

## Advice and supervision for information-secure environments

> *“The need for information security advice has clearly increased.*

## Lessons from information security assessments in 2018

The assessment subjects varied wildly during the year. There was also an evident need for security counsel. As in previous years, we noticed that the protection level in the information system assessments had significant variation. The scale of assessment subjects was also extensive.

Our smallest subject was a computer that had been physically isolated from other environments. In such cases we focus on assessing administrative and physical security as well as protection methods related to diffuse radiation and the production process, in particular. When the case involved an information system, as a whole, used in several countries and by numerous different organisations, we specifically evaluated the management of security and protection related to the security of supply chains.

In our work, it became clear that the need for information security counsel has clearly increased. Counsel was needed for both efficient protection of information systems and ensuring cyber security in society at large. Specifically, support was required for the design of information systems and the identification of risks targeted at organisations.

## Towards better corporate security

Our goal is to improve corporate security in cooperation with information security evaluation bodies. This collaboration has already taken its first steps, and tried and true methods are gradually being created.

The cooperation is being developed methodically by means of an annual schedule, among other things. Its purpose is to make operations between organisations regular, increase meetings, provide training, harmonise practices and – perhaps most importantly – create connections for discussion.

1 **Allocate resources and ensure skills**
Organisations do not allocate enough resources to information security. Without expertise, it is almost impossible to ensure that operations are secure, let alone maintain such security. Planning of information security for systems that support the operation, in particular, should be in expert hands in order to avoid deficiencies or excesses.

2 **Identify targets to be protected and critical information**
If information that needs to be protected is not identified or specified, risks and costs related to the implementation of the services will increase. In the worst case, organisations end up making uncontrollable decisions on architecture. Such a situation is possible when a target to be protected has not been sufficiently isolated from other systems, for example.

3 **Services cannot be implemented in an information-secure manner without the necessary competence**
In the outsourcing of services, organisations must ensure that obligations and responsibilities agreed on with a service provider are carefully specified and sufficient. In exceptional circumstances, a service provider may not supply the information needed to rectify the situations, updates may be neglected and management connections without proper information security may be used.

4 **Events, exceptions and logs in one's own network must be monitored**
Even if systems logs are kept, the logs may not be comprehensive enough. An organisation may not monitor them, or they may be so contradictory in terms of time stamps that the information required cannot be determined.

5 **Verify the level of information security in the systems**
An assessment may not have been made at all, or it may be the responsibility of a company that sells evaluation services on commercial grounds. The independence of such an evaluation can be questionable. Assessments made by the National Cyber Security Centre Finland or an approved evaluation body give an independent picture of the security of the system.

## Galileo activated Finnish satellite experts

The past year was a busy period for NCSC-FI, especially with coordination work on cyber security at various EU cooperation bodies. As the president, Finland hosted a joint meeting of PRS authorities of EU countries in Helsinki last September.

European Galileo satellites now have global coverage. This has increased Finnish experts' willingness to contribute to the construction of the national section of the PRS. We discussed the subject during a workshop in November that was attended by a total of 80 representatives from various authorities and critical infrastructure companies.

In 2018 Finnish PRS cooperation was built with the Finnish Geospatial Research Institute FGI and the Defence Forces, among others. Our Spectrum Management division helped make this collaboration closer than before.

In Finland the European Union's own Galileo satellite navigation system will probably be taken into use at the beginning of the 2020s. It provides better protection against interference of GPS navigation, for instance. Such interference became evident in Lapland in November, and it was linked to the major military exercise of NATO.

## Agile control and vigorous supervision

When used correctly, regulation is a great tool for improving cyber security and resilience for incidents in society.

In 2018 information security and preparedness were more visible than before in the drafting of legislation. There has been a perceptible change especially in regulation concerning the security of electronic services or the processing of important data in network and information systems. This trend has delighted us at NCSC-FI but it has also meant more work as requests for consultancy and statements.

In the latter half of the year we handled 50 statement requests. Every one of them involved some perspective concerning cyber security, information security or preparedness. Our experts have been familiar visitors to both working groups and Parliament committees.

> *“In 2018 information security and preparedness were more visible than before in the drafting of legislation; in the latter half of the year we processed 50 statement requests.*

*Picture of a Galileo satellite. The Public Regulated Service, or PRS, is a positioning and timing service in satellite navigation intended for the authorities. Service users are managed and the distribution of keys is handled, in each EU country, by the PRS authority, which in Finland is the Transport and Communications Agency.*

## We must be familiar with phases of EU regulation projects

Amendments to legislation do not occur quickly. A key aspect of the work is monitoring of amendments to EU provisions and preparedness for these. Over the past year, we watched closely the overall reform of the Directive on privacy and electronic communications last amended in 2009, the drafting of the European Union's General Data Protection Regulation (ePrivacy), and the progress of the EU's Cybersecurity Act. Not to mention changes to regulation on the Finnish Trust Network in strong electronic identification, whose urgent drafting the Ministry of Transport and Communications initiated last autumn.

An important EU project was brought to conclusion in the spring when the requirements of the Directive on security of network and information systems, known as the NIS Directive, entered into force. This Directive imposes minimum obligations on the monitoring and reporting of information security for critical sectors in society and, in the future, provides us with more information on the status of information security in various sectors. Such information can be used in the future development of cyber security.

Obligations on reports on information security and incidents now also apply to digital services, i.e., cloud services, search engines, and online marketplaces. Information security obligations included in the NIS must also be observed in the energy, transport, financial and health care sectors, and in the supply and distribution of drinking water. We invited supervisory authorities in these sectors to join a working group where control, competence and supervision can be coordinated. The application of the Directive will be reviewed with supervisory authorities in other Member States.

## Aiming for reliable electronic services

Regulation was not as rapid as software development, for instance, even in 2018, but still we aim to act in the most agile manner possible in our regulations and other control measures. We anticipate and evaluate what stipulated requirements mean, in practice, for the enterprises and other organisations we supervise. This all takes time. Open cooperation has been valuable but also necessary for us, because the information we gained has helped us take account of practical requirements in the development and interpretation of regulation.

We listen, we take into consideration, but we are also demanding. Everyone must abide by the stipulated requirements, but we prepare regulations and advise on the interpretation of provisions, so all operators know what is demanded from them and what they could do better. Thus we can help develop the reliability of services provided by actors we supervise.

We apply control measures whenever necessary. Late in the year we pushed the last providers of strong electronic authentication to stop using TLS 1.0. In 2018 our experts also met with several regional network operators when inspecting the compliance of backups in communication networks.

# Cooperation and sharing of information

## Information Sharing and Analysis Centres provide the best lessons

Cooperation and exchange of information between the central government and critical infrastructure providers is a central part of the operation of the National Cyber Security Centre Finland. This collaboration is at its closest in Information Sharing and Analysis Centres (ISACs) that share information and whose operations we coordinate.

Sectors significant for the functioning of society have their own ISAC groups that search for information security solutions related to the sector and share information on topical cyber threats and phenomena. Such cooperation is beneficial for organisations included in the groups, the authorities and, first and foremost, the general public. We support organisations that provide services critical for society and important for the public, in ensuring the maintenance and development of information security in their business decisions.

At present, there are 13 groups from various sectors, from central government to the media. The latest group is the WATER ISAC founded last autumn. The information sharing group in the energy sector, E-ISAC, which used to be called E-CIP, has the longest history of operation. Significant investments were made in developing the operation of the groups in 2018. We have received additional resources for this work from the Cyber 2020 programme.

Sector-specific groups can focus on challenges and threats characteristic for the sector in question. In 2018 the various groups discussed, e.g., preparedness for elections, protection against denial-of-service attacks, information security in routers, ensuring data security in remote connections of automation environment, and practised sharing information during incidents.

Although the groups have differences, most subjects are common to every one of them. Topics that cause concern include ensuring information security in cloud solutions and questions related to training of personnel. More and more organisations must outsource their information security solutions, in the name of a rapidly changing technology environment and cost efficiency. Successful outsourcing projects, including contracts, require special competence.

## Energy sector ISAC was rewarded for praiseworthy cooperation

The energy sector has enormous responsibility for securing the functioning of society. This has been well understood among specialists in the sector who work in active cooperation to improve cyber security in their field. We granted E-ISAC the Information Security Trailblazer award for merits in exemplary cooperation in the spring of 2018.

The importance of preparedness for problems, development of collaboration and own operations and practising these were emphasised in the energy sector in 2018.

An exercise called TURVA18 was arranged at the Olkiluoto nuclear power plant in September. In October, energy sector operators joined other businesses and the authorities in TIETO18, an exercise for large-scale cyber security incidents. An exercise called Black Screen II in November focused on the management of cyber threats together with Nordic main grid companies and authorities in the sector. The Kyber-ENE2 project involved improving cyber security among operators who provide critical energy products and services. Different workshops and exercises related to cyber security will also be arranged in 2019.

⚠ The year 2018 was characterised by the Microsoft Office 365 scam campaign. In the summer we learned of several successful and near-miss scams through our ISAC groups. On the basis of the information, we evaluated the situation in Finland as severe and published a critical alert on the scam campaign. The alert helped Finnish organisations protect themselves against the scam and damage caused by it. ISACs have also provided significant assistance and guidance for protection from Office 365 scams.

## Current affairs in the ISAC sectors

| SECTOR | SPECIAL CHARACTERISTICS | NEWS |
|---|---|---|
| CENTRAL GOVERNMENT | A high number of information security requirements that are statutory and based on international obligations. The need to carefully consider questions related to geographical location for storing information, for example. | Finland will have several elections in the spring and assume the Presidency of the Council in the autumn. |
| FINANCE | Efficient preparations are in place for denial-of-service attacks that have become the “new normal”. Phishing messages are a challenge for banks. | Internationalisation of cooperation and Nordic collaboration, in particular. Monitoring of adoption of NIS obligations. |
| WATER SUPPLY | Strong dependence on automation systems, so protecting these is an important subject for cooperation. | Operation in ISAC cooperation began in 2018. Monitoring of adoption of NIS obligations. The Cyber Water project of the National Emergency Supply Agency brought tools for developing cyber security in water management. |
| TELECOMMUNICATIONS OPERATORS (ISP) | Solutions for efficient exchange of information on cyber threats during both preparedness for incidents and operational faults. | A joint exercise by telecommunications operators on preparedness for extensive incidents. |
| SOCIAL WELFARE AND HEALTH CARE | Methods for information-secure sharing of client data in health care. | The Cyber Health project of the National Emergency Supply Agency develops cyber security in the sector to a large extent. Guidelines for preparedness by social welfare and health care providers at the Ministry of Social Affairs and Health have been updated, with a view to cyber security. Monitoring of adoption of NIS obligations. |
| ENERGY | A high number of joint exercise activities. Advance preparedness is emphasised in operations. | The Cyber-ENE2 project is in progress. Exercises (such as the TURVA18 exercise at the Olkiluoto nuclear power plant, TIETO18 exercise, Black Screen II exercise). Monitoring of adoption of NIS obligations. |
| CHEMICAL AND FOREST INDUSTRY | Operations are dependent on automation systems, and there is production in several countries. Requires implementation of information security in different work cultures and legislative environments. | Strong increase in utilisation of IoT, and perspectives related to outsourcing. |
| FOOD INDUSTRY AND RETAIL DISTRIBUTION | Strong digitalisation of operations, a shift towards automation and robotisation. | Questions related to the security of email. |
| TRAFFIC | Automation of traffic and intense networking are challenges in the future. The sector is in a state of change. | ISAC will begin operation at the beginning of 2019. Monitoring of adoption of NIS obligations. |
| MEDIA | Networking of production systems in media organisations. Information security at editorial offices and among reporters. | Appropriate protection of cloud services. Information security questions involving the elections from the viewpoint of media organisations. |

# Supporting and planning for cyber exercises

“Joint efforts and networking produces successes that are greater than the sum of their parts.

## Learning opportunities and better cyber preparedness through exercises

The goal of exercises is to improve various organisations' operating and recovery capabilities in case of serious security breaches. Exercises simulate a crisis that the participants resolve and from which they obtain valuable lessons.

Our exercise services are part of the Cyber 2020 project of the National Emergency Supply Agency, and they are available for critical infrastructure providers. We help these organisations find a suitable partner, draw up an exercise scenario, and select the appropriate exercise method. Our services have also been used in the planning and organisation of joint exercises called TIETO, KYHA and TAISTO.

## Using exercises to bring forth benefits of cooperation

The TIETO18 exercise arranged by the National Emergency Supply Agency in the autumn brought together more than 120 representatives of businesses and authorities to practise handling challenging information security incidents with help from the cooperation networks. The exercise was organised in three parts, the last of which took three days, including the debriefing of results.

For the exercise, fictitious organisations were created that joined forces in combating numerous information security threats. The authorities joined in, helping solve problems and build operating models to cope with the threatening situations. The Finnish Broadcasting Company YLE added its own flavour to the exercise by holding its own preparedness exercise at the same time. Participants were able to give interview to real journalists, and news reports of the exercise were sent from the site during the second day.

## Regulatory activities also benefit from networking

Security authorities' own KYHA exercise in Jyväskylä put the authorities on the spot. Information systems had been created for the exercise environment that were attacked by the "red team" assembled by the exercise organisers.

During the KYHA exercise, we focused on created information exchange networks and establishing situational awareness that helped us make timely and justified decisions.

The large-scale KYHA and TIETO18 exercises were good examples of cyber cooperation that produces successes through joint action and networking, which are greater than the sum of their parts.

Such joint exercises provide an excellent supplement to independent practice by businesses and other organisations whose game situations are often limited within their own premises.

| Exercises where we participated in planning and/or implementation. | |
|---|---|
| 2016: | 10 |
| 2017: | 9 |
| 2018: | 20 |

"The National Cyber Security Centre Finland operated at the core of the exercise, with a central and successful role. The contribution was extremely important for the exercise."
– Organiser of a joint exercise

"Especially during the planning phase we received excellent comments on authentic scenarios and which [security violations] the National Cyber Security Centre Finland has seen in real life."
– A critical infrastructure provider of its own exercise

# Work on the future and development of operations

## Preparing for the future with joint effort

Traficom has established a group of specialists who focus on the outlook and development of the communication sector. The group’s purpose is to identify new phenomena and technologies in communications and cyber security that will change our regulatory activities, society and everyday lives.

In 2018, the group concentrated on 5G networks and IoT products for consumers, and focused on better information security in cloud services. We also studied the operation of 5G and IoT ecosystems and the societal impact of satellite technology.

## Report on the cyber security of 5G networks

We investigated the kinds of cyber security risks that may be directed at consumers, enterprises and authorities when 5G technology and infrastructure critical for business activities merge and spread as a shared data processing platform of various functions in society.

The report provides tools for anticipatory and up-to-date regulatory work at Traficom. This way operators considering the adoption of 5G technology can make safe and secure decisions.

The work has proceeded well and on schedule, key risks have been identified, and we are even more familiar with the differences between 5G and previous mobile technologies.

The project identified the following subjects as new sections requiring special attention

**From data transmission to processing:**
We have moved from infrastructure that focused on the transmission of data to infrastructure that concentrates on comprehensive data processing, cloud services included. This is one of the key changes related to 5G networks. Data processing is moving ever closer to end users, so even the network will become more complex and inter-dependent. This change affects traditional risk management and security architecture models, and we want to join in developing these at a national and international level.

**Operators become providers of processing platforms:**
The architecture of 5G networks challenges the old model in which telecommunications operators are merely transmitters of data. 5G technology has edge computing functionalities due to which the role of the operator changes from a transmitter of data to a provider of a data processing platform. At the same time, the core and the edge of the network come closer to each other, and telecommunications operators have a bigger role than before in securing the data of end users.

**Virtualisation:**
Provision of edge computing capacity based on virtualisation to end users challenges telecommunications operators and network manufacturers in new ways. The network will change from being closed to being more open, and more attention than before must be paid to its information security updates. Virtualisation is a cost-efficient way to scale resources but, at the same time, the identification and management of risks related to it have an increasingly important role.

**Slicing:**
Network slicing and virtualisation of network functions offers end users service categories with even better performance, so 5G attracts operators providing critical functions to move their network traffic onto the mobile network. These migrations require a precise risk analysis that takes account of changes in threats to physical security.

In early 2019 we will organise a 5G hackathon to test the resilience for incidents and security of the 5G network and IoT devices essentially related to it during authentic operating situations. International researchers from our vulnerability researcher network will attend the hackathon.

## Information-secure concept

Effective cyber security principles for IoT devices and cloud services have been needed for quite a while now. It has been deemed important that consumers can identify information-secure devices and services upon acquiring them.

We respond to these needs with the Information-secure concept that includes security requirements and principles, which are based on voluntariness, and the Information-secure logo. Manufacturers who take information security into consideration during the design phase of their products or services can use the logo.

The overall concept and principles are being finalised. We have also started discussions with stakeholders to give us feedback and proposals for development on the concept before introduction. Cooperation with manufacturers of digital services and IoT devices and retailers has been constructive and provided excellent ideas for further development.

## Report on satellite technology

What is the actual role of satellite technology in society? How can we identify actors with business operations related to satellites and space? And how can we anticipate business activities in the future? With our report, we want to both answer these questions and find ways to support Finnish operators as well as possible. For instance, how can information security be turned into a competitive advantage?

We can already see ingredients of a technological revolution in the proliferation of satellite technology. This phenomenon can be compared to how the internet became part of our daily lives.

Next we will investigate how to create the most favourable conditions for innovations related to information security in satellite communications and the growth of business operations in the sector.

## Cyber security development programme CYBER 2020

CYBER 2020, the cyber security development programme of the National Emergency Supply Agency, has been a central element in the development of our operations since 2017. The key goal of the programme is to secure the continuity of critical infrastructure providers in all circumstances. Supported by the CYBER 2020 programme, several development projects have been and will be launched in 2017–2020.

At present, we develop our operation in three different projects that are HAVARO 2.0, ISAC groups, and exercise activities. With these projects we want to, among other things, improve our national detection capabilities, develop our exercise operations, and improve the exchange of information and cooperation in our networks. We also take part in development projects that focus on cyber security questions in the energy and social welfare and health care sectors, for instance.

## HAVARO 2.0 service provides better protection against serious information security threats

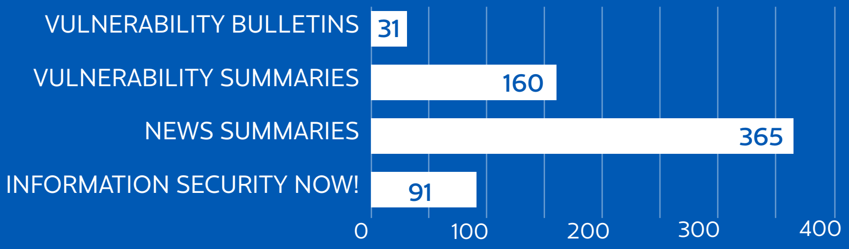
We have created our HAVARO to help organisations observe serious information security threats. Now the service is in a development phase to version Havaro 2.0 where we are moving from service by an authority to a service jointly provided by commercial operators and the NCSC-FI.

The purpose of the HAVARO 2.0 project is to create a trust network where members can exchange information among themselves better than before. Through rapid and reliable exchange of information, the HAVARO service can be maintained and developed to match the quantitative and qualitative trend in cyber threats, but with reasonable resources. The basis of the operation will be the Havaro 2.0 system, and we signed an agreement on software development on the system with Reaktor Oy in September.

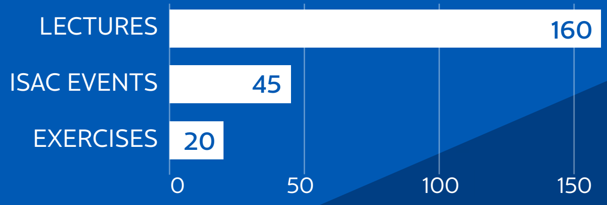
# Our KPIs

There was an increase in especially our communication, exercise activities and cooperation with the various sectors in 2018. There is plenty of work left in promoting cyber security because the Autoreporter system, for instance, detected much more traffic originating in Finland than in the previous year.

## Communication and bulletins



## Events and exercises



| | |
|---|---|
| UNINTERRUPTED ON-CALL DUTY | 24/7/365 |
| ALERTS | 2 |
| PROCESSED CASES ("TICKETS") | 6100 |
| NUMBER OF INCIDENTS: SEVERE | 41 |
| SIGNIFICANT IN TOTAL | 67 |
| CASES PROCESSED THROUGH VULNERABILITY COORDINATION | 35 |
| SHUTDOWN OF HARMFUL SITES | 500 |
| FACEBOOK FOLLOWERS | 5135 |
| TWITTER FOLLOWERS | 8356 |
| CONTACTS BY MEDIA | 187 |
| AUTOREPORTER | 154000 |

### PEOPLE ARE SATISFIED WITH OUR SITUATIONAL AWARENESS PRODUCTS

In 2018 we conducted three customer surveys to determine the satisfaction of our customer organisations with our situational awareness products. The grading scale in our surveys was from poor (1) to excellent (5).

TIMELINESS:
**4.1**

CONTENTS:
**4.1**

SIGNIFICANCE:
**4.1**

### SURVEY FOR INFORMATION SHARING GROUPS IN THE VARIOUS SECTORS

Sector-specific information sharing groups were regarded as useful. Items deemed especially important included networking and the enabling of exchange of information.

GRADE:
**4.1**

### INTERVIEW SURVEY FOR STAKEHOLDERS

Success at coordination and assistance related to information security threats.

GRADE:
**4.2**

Of all the respondents in the survey, the percentage who use our services regularly, i.e., on a daily/weekly basis.

**66%**

# Cyber security to every home through public campaigns

*“These days cyber security is a civic skill.*

## Are you familiar with the Longer the Better (pidempi parempi) password generator and security expert Teijo?

We wanted to bring information security close to as many people as possible and campaigned for basic skills in cyber security in late 2018. The Longer the Better password generator and security expert Teijo gave practical tips on information security.

Besides such hints, Teijo gave his followers information security aphorisms, or 'securisms', on the Turvallisuustit social media channels and on the website turvalistit.fi. Teijo's amazing information security interventions are also available in video format.

Our daily lives go smoothly when phones and computer work and when we can use services at online banks, for example, without any fear. The authorities, electricity companies and telecommunications operators do their part, but responsibility lies in every home also. These days cyber security is a civic skill.

*The Longer the Better password generator at pidempiparempi.fi gives an example you can use to create your own passwords. A good password is one that is long and only known by you.*

## Remember these basic matters

1. Create a long and unique password for every service you use.
2. Update your devices and their software on a regular basis.
3. Make backup copies of your important information and photos.

# CYBER WEATHER 2018
# AND A LOOK AT CYBER YEAR 2019

# 10 + 1 information security forecasts for 2019

## 1 Significance of human information security will grow

As information security protection evolves, abuse of human weaknesses will rise ever more strongly alongside technical information security threats. Technology is still required, but we also need protection solutions based on human competence and behaviour.

## 2 Significance of information security in consumer devices connected to the internet will be emphasised

Poor information security causes inconvenience for both users of IoT devices and others using online services. Efforts are being made to improve the situation through regulation, international cooperation and standardisation. Fortunately, consumers are more and more interested in the information security and protection of their devices. A logo describing information security in devices will make consumers' decision-making easier.

## 3 Dependency on digital services creates surprising situations

The digitalisation of services, products and processes brings significant efficiency benefits. At the same time it also creates new, chain-type dependencies, and the visibility of overall risks may decrease. However, the pressure for making changes and experiments in business operations is great. Risk management has a tough job in keeping up with these changes.

## 4 Familiar threats that were deemed minor are gradually become more severe

Without widespread attention, familiar threats that have been deemed minor are growing to become massive. Phishing, in particular, is a more difficult scourge than before, and snooping of information becomes increasingly targeted. Exploitation attempts vary from small-scale crime on the web to governmental activities. Cyber criminals seek especially financial benefit and information vital to their victims.

## 5 New technologies determine the information security challenges in the 2020s

Machine learning, robotics, 5G and artificial intelligence are examples of new technology that will be adopted in the near future. A great deal of investments are made in their development. The way such development and deployment take account of information security show the kinds of information security challenges we will wrestle with in the 2020s.

## 6 The cloud comes with force, and the change is cause for both joy and concern

Information security requires the ability to adapt information security which leans on traditional protection solutions and the cloud world into one whole. Demand for new thinking and innovative solutions will increase.

## 7 Outsourcing of information security will increase

There will be an increase in different information security control rooms and SOC services, in particular. Even other external information security services will be acquired in support of one's own competence.

## 8 Cyber attacks by governmental actors and news reports on them will continue

Attacks carried out in the cyber operation environment are effective, and the direct risk of getting caught is small. Different countries will bring estimations of the perpetrators to the forefront more and more strongly.

## 9 Still room for improvement in the basic matters involving information security at organisations

Many organisations still do not take sufficient care of updates, backup copies and passwords. In terms of information security, there is plenty of room for improvement especially in contracts signed with service providers and partners.

## 10 Information security will become part of business-oriented risk management

Information security will rise better than before from the depths of the IT department to the agenda of comprehensive risk management at organisations. Ownership of risks must be given to those who make decisions related to risks. This is the only effective way to fight against increasing information security threats.

## +1 We will not see malware epidemics targeted at mobile devices

We have forecast the onslaught of mobile malware for several years, but this has not happened thus far.

# Cyber weather 2018

## Most significant incidents of the year in January–December 2018

Jan

Invoicing scam in the name of Traficom's Director-General

Detection peak: Subscription traps via text messages

Meltdown and Spectre attacks came to the forefront

Packed snow disrupted operation of networks in Kainuu

Feb

Memcached, the most powerful attack in history (1.7 Tbit/s)

Exceptionally high number of DoS attacks in Finland

WannaMine infected many organisation's servers in Päijät-Häme

🌐 Attacks against the information systems of the Olympic Games

Mar

Case Cambridge Analytica

Apr

⚠ **Passwords of Finnish users in plain language revealed from the liiketoimintasuunnitelma.com website**

Hijacked O365 email accounts are actively used for scams

🌐 An international police operation shut down the webstresser.org service

May

Office 365 email accounts were stolen

Plenty of malware infections in home routers

VPNFilter malware spread to SME routers and network storage devices around the world

Hide and seek malware spread to IoT devices

🌐 VPNFilter bot network connected to the APT28 group

Jun

⚠ **Active phishing of Office 365 credentials**

Emergence of mining malware that infects IoT devices

Magecart attack against Ticketmaster online store

🌐 = Kansainvälinen uutisnosto

## Jul

⚠ **Active phishing of Office 365 credentials**

Porn extortion campaign: I know your password!

Data leaks from systems of sports watch manufacturers

## Aug

⚠ **Phishing of Office email credentials, and hijacked accounts still used for scams**

DoS attack against the suomi.fi online service

Magecart attack against the British Airways online store

Vulnerabilities in fax machine firmware, even unprotected 3D printers observed on the Web

Swedish Security Service: Attempted cyber influencing of parliamentary elections in Sweden

## Sep

⚠ **Active phishing of Office 365 credentials, now also with falsified secure mail notifications**

Payment card details phished in the name of the MyTax service

Suomi.fi again under attack

Largest DoS attack in 2018 in Finland, with a volume of 90 Gbit/s

Leak of approx. 50 million users' data from Facebook

Magecart attack against Newegg online store

Suspected Satori botnet perpetrator was arrested

## Oct

⚠ **Active phishing of Office 365 credentials**

Finnish version of the porn extortion scam

Increase in detections of Kovter and Emotet malware

Port Smash vulnerability published

Vulnerabilities discovered in solid state drives (SSD)

## Nov

⚠ **Active phishing of Office 365 credentials**

Marriot data breach

Yandex application leaks data

Information security criteria for home routers from German authorities (BSI)

## Dec

⚠ **Active phishing of Office 365 credentials**

EU's diplomatic communication was spied on for years

Prosecutor in the United States: espionage by the APT10 group extended to Finland also

# How accurate were the information security forecasts for 2018?

Our forecasts for information security phenomena in 2018 were fairly accurate. Half of our forecasts became reality, two were completely wrong, and we classified three as borderline cases.

## Correct! Yes

In 2018 the GDPR and NIS made organisations invest in information security. As most of the malware infections we observed in Finland were due to unprotected and unupdated IoT equipment, our forecast of IoT devices abandoned on the web was accurate. There was no oversupply of information security specialists; bug bounties and hackathons increased openness and awareness of information security. Also, outsourced supply chains were used for data breaches, as we had forecast.

## Wrong! No

Updating chains were not used for distributing malware as we had expected. And that's a good thing. Criminals also did not attack companies through social media, instead they used mostly email for distributing scams and malware. Private individuals suffered the most from social media attacks made by criminals.

## In a way yes, in a way no... –

A union between innovative information security products and artificial intelligence did not become a phenomenon in 2018, although advances were made in technical solutions and new ones are constantly developed. Automation and machine learning are being utilised on a large scale, unfortunately this also applies to cyber crime. Even criminals did not utilise AI in a visible manner. They traded more in denial-of-service attacks that gained their power from botnets comprised of IoT equipment. Hacked IoT devices were used for mining of crypto currency too. We did observe some IoT malware, but epidemics were avoided.

| | | |
|---|---|---|
| 1 | Yes | **GDPR and NIS will make organisations invest in information security** |
| 2 | Yes | **Dying IoT devices will be a nuisance** |
| 3 | Yes | **Demand for information security experts on the labour market will continue** |
| 4 | – | **Innovative information security products will use artificial intelligence** |
| 5 | – | **The IoT will attract criminals and ransomware** |
| 6 | Yes | **Openness will increase (bug bounties, hackathons)** |
| 7 | – | **Criminals will boost their attacks with AI** |
| 8 | No | **Security of updates will be undermined** |
| 9 | Yes | **Outsourced supply chains will be used in data breaches** |
| 10 | No | **Social media will become an access route to companies** |

# News summary of the most significant cases during the year

## Scams and phishing

- **Office 365 alert: Active phishing of Office 365 credentials:**
  https://www.kyberturvallisuuskeskus.fi/fi/office-365-sahkopostin-tietojenkalastelu-ja-tietomurrot-erittain-yleisia-havaitse-suojaudu-tiedota
- **Scammer with a poker face – invoice scammer poses as the Director-General of the Transport and Communications Agency:**
  https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/01/ttn201801231206.html
- **Porn extortion scam:**
  https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/07/ttn201807171603.html

  https://www.is.fi/digitoday/tietoturva/art-2000005848028.html
- **Scams via text messages:**
  https://www.mtvuutiset.fi/artikkeli/poliisi-varoittaa-huijausviesteista-ala-avaa-linkkia-ja-sulje-viesti/6747364#gs.bMJpkrtC
- **MyTax:**
  https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/09/ttn201809111520.html

## Vulnerabilities and malware

- **Meltdown & Spectre:**
  https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/01/ttn201801041615.html
- **WannaMine:**
  https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/02/ttn201802161123.html
- **VPNFilter:**
  https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/05/ttn201805241306.html

  https://www.thedailybeast.com/exclusive-fbi-seizes-control-of-russian-botnet
- **Hide and seek malware spreads to IoT devices:**
  https://www.bleepingcomputer.com/news/security/hide-and-seek-becomes-first-iot-botnet-capable-of-surviving-device-reboots/
- **Kovter, malware that clicks on advertisements:**
  https://www.proofpoint.com/us/threat-insight/post/kovter-group-malvertising-campaign-exposes-millions-potential-ad-fraud-malware
- **Emotet, bank malware:**
  https://blog.trendmicro.com/trendlabs-security-intelligence/new-malicious-macro-evasion-tactics-exposed-ursnif-spam-mail/
- **Port Smash vulnerability:**
  https://www.io-tech.fi/uutinen/intelin-prosessoreista-loytyi-uusi-portsmash-sivukanavahaavoittuvuus/
- **Vulnerabilities in solid state drives (SSD):**
  https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/11/ttn201811081513.html

## Data leaks and breaches

- **Cambridge Analytica & Facebook:**
  https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

  https://yle.fi/uutiset/3-10121765
- **Magecart attacks**
  - **Ticketmaster:**
  https://www.securityweek.com/ticketmaster-breach-tip-iceberg-major-ongoing-magecart-attacks
  - **British Airways:**
  https://www.bleepingcomputer.com/news/security/british-airways-fell-victim-to-card-scraping-attack/
  - **Newegg:**
  https://www.bleepingcomputer.com/news/security/newegg-credit-card-info-stolen-for-a-month-by-injected-magecart-script/
- **Leak of 50 million users' data from Facebook:**
  https://yle.fi/uutiset/3-10430506

  https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/10/ttn201810011357.html

- **Sports watches:**
  https://www.mtvuutiset.fi/artikkeli/viestintavirasto-sijaintitieto-ja-maailmalla-levittaneesta-sovelluksesta-voi-tulla-yllatyksena-etta-tiedot-menevat-kaikille/6987790#gs.kQinniCY
- **Data breach at the Marriott hotel chain:**
  https://yle.fi/uutiset/3-10534789
- **Yandex application leaks data:**
  https://www.mtvuutiset.fi/artikkeli/asiantuntija-yandex-kohusta-kyberturvallisuuskeskuksella-ei-ole-resursseja-tutkia-yksityisten-sovellusten-tietoturvaa/7162778#gs.PZV5cZwA

## Spying

- **Attempt at destruction of information systems at the Olympic Games:**
  https://blog.talosintelligence.com/2018/02/olympic-destroyer.html
- **Swedish parliamentary elections & cyber influencing:**
  https://yle.fi/uutiset/3-10366498
- **Espionage at Belgian operator Belgacom:**
  https://www.theguardian.com/uk-news/2018/oct/25/uk-refusal-cooperate-belgian-hacking-inquiry-condemned-gchq-belgacom

  https://www.theregister.co.uk/2018/10/26/belgium_finds_evidence_gchq_belgacom_hack_proximus/
- **Attacks through supply chains:**
  https://www.tekniikkatalous.fi/talous_uutiset/yritykset/sahkoposti-harrastuskerhon-vetajalta-kyberrosvot-valmistautuvat-jo-todella-hyvin-keikkoihinsa-pystyy-jopa-tappamaan-6746737

## DoS attacks

- **Shutdown of the webstresser.org service:**
  https://www.bleepingcomputer.com/news/security/europol-shuts-down-worlds-largest-ddos-for-hire-service/
- **Attack against the suomi.fi identification service:**
  https://valtori.fi/artikkeli/-/asset_publisher/sunnuntain-12-8-palvelunestohyokkayksen-yksityiskohtia-selvitetaan

  https://yle.fi/uutiset/3-10349357?origin=rss

  https://vrk.fi/artikkeli/-/asset_publisher/suomi-fi-tunnistuksessa-on-kohdistetusta-palvelunestohyokkayksesta-johtuva-hairio

  https://legacy.viestintavirasto.fi/viestintavirasto/blogit/2018/ddosinternetinraksyttavarakkikoiraeisaaaikaanhaavaa.html
- **Memcached, the most powerful attack in history (1.7 Tbit/s):**
  https://legacy.viestintavirasto.fi/kyberturvallisuus/tietoturvanyt/2018/02/ttn201802281537.html
- **Satori botnet:**
  https://portswigger.net/daily-swig/hacker-arrested-over-satori-botnet-malware

## Operation of communications networks

- **Power failures in Kainuu:**
  https://twitter.com/CERTFI/status/956127257755635712

  https://erveuutiset.erillisverkot.fi/blog/2018/01/24/sahkot-poikki-kainuussa/
- **Incidents in individual networks caused interruptions in services important for society:**
  https://yle.fi/uutiset/3-10207164
- **Interference of GPS navigation in Lapland:**
  https://yle.fi/uutiset/3-10498891

## IoT

- **Mining malware that infects IoT devices:**
  https://www.bleepingcomputer.com/news/security/prowli-malware-operation-infected-over-40-000-servers-modems-and-iot-devices/

  https://www.fortinet.com/blog/threat-research/pyromineiot--nsa-exploit--monero-xmr--miner----iot-device-scanne.html
- **Fax machines and 3D printers:**
  https://blog.checkpoint.com/2018/08/12/faxploit-hp-printer-fax-exploit/

  https://isc.sans.edu/diary/rss/24044
- **German authorities (BSI) and information security criteria for home routers:**
  https://www.zdnet.com/article/germany-proposes-router-security-guidelines/

TRAFICOM
Finnish Transport and Communications Agency
National Cyber Security Centre

Do you or your organisation need help with preventing information security breaches, or do you have questions about legislation related to cyber security? We also evaluate and approve information systems.

We develop and supervise the reliability and security of communication networks and services. You can reach us as follows:

via email: cert@traficom.fi
Customer service: 0295 345 630

**Follow us and our news**
www.kyberturvallisuuskeskus.fi
@CERTFI
www.facebook.com/NCSC_FI

**Report a security violation to us**
https://www.kyberturvallisuuskeskus.fi/fi/ilmoita

CONTACT INFORMATION
National Cyber Security Centre Finland (NCSC-FI)
Finnish Transport and Communications Agency
Traficom
PO Box 320
00059 TRAFICOM