

**CERT-Fi**

**ANNUAL REVIEW 2009**

20.1.2010

# CERT-FI annual review 2009

## Introduction

### Conficker spread widely

Computer worm Conficker spread to millions of computers in 2009. Conficker is a mysterious worm, since it has not been reported to do anything more than spread from one computer to another through network or portable memory devices.

Malware can be used for remotely controlling a computer or for 'phishing' for user information. It has been reported also in Finland that a trojan has been used to interfere with online banking sessions and to make bank transfers without the user knowing of them.

### Efficient international cooperation

International information security communities and authorities have tightened their cooperation over the course of the year. In addition to dealing with the Conficker worm, this cooperation ensured that certain companies offering malicious content have been shut off from the Internet. Domain names used by malware have also been blocked.

### Comparative research on European CERT organisations was conducted

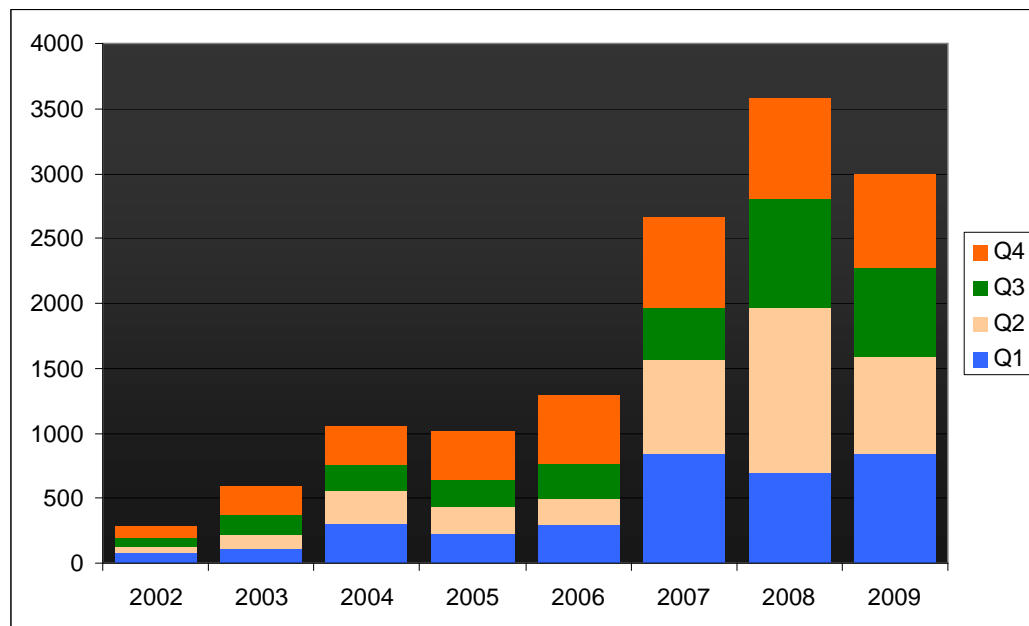
CERT-FI completed research on European CERT organisations in 2009. The operation of 11 CERT units was compared in the research. This research was the first of its kind in Europe, and its results have met with international interest.

### The Act on the Protection of Privacy in Electronic Communications was amended

The changes in the Act on the Protection of Privacy in Electronic Communications went into effect in June. After the act entered into effect, FICORA recommended that telecom operators protect Finnish online banking users as specified therein.

### Swedish intelligence operations may have an effect on Finnish telecommunications

A new act concerning signals intelligence in Sweden came into force on 1.12.2009. FICORA has issued regulations for the telecom operators concerning informing their customers of international information security threats targeted to services offered to Finnish customers.



The number of cases handled by CERT-FI appears to be stabilising.

## **Conficker is the most widespread malware**

Aggressively spreading malware Conficker has infected millions of computers. An estimate presented at the end of 2009 concerning the number of computers infected by Conficker was approximately seven million, around the world. Thousands of computers have been affected by Conficker in Finland.

In 2009, CERT-FI's Autoreporter system sent out nearly 100,000 notifications related to the Conficker worm. This number does not directly indicate the number of infections, since many IP addresses are repeated among the notifications. More detailed research shows that more than 25,000 computers have been infected by the worm in Finnish networks.

One reason for the efficient spreading of the Conficker worm is its ability to propagate via mobile memory devices, such as USB memory sticks. Additionally, the worm uses the network for spreading, which is typical for computer worms.

Conficker is mysterious malware: its original purpose is still unknown. One version of the worm is known to spread the Waledac malware and Spyware Guard, which is known for being scareware. Waledac has previously been used for sending junk mail and for stealing network service domain name addresses.

### **Spam campaigns spreading malware targeted also Finland**

Scam junk-mail campaigns have primarily targeted foreign banks and US organisations, such as the Internal Revenue Service.

However, spam messages spreading malicious content also spread to Finland. CERT-FI received several reports of junk mail containing links to malware being sent to Finnish addresses.

In most cases, the links in the junk-mail messages led to variations of the Zeus malware family. This malware is also known as Zbot and WSNPOEM. A Zeus spamming campaign reported in Finland

sent messages containing a link ostensibly to an application for specifying Outlook e-mail settings. In reality, the link led to malware.

The Zbot malware has previously been used for stealing network service and credit card information. Some variations of this malware family have mechanisms for identifying online banking applications. Zeus malware tailored for Finnish online banks has not been encountered yet.

Computers infected by Conficker or Zbot are an example of how computers are hijacked and used for many types of malicious activity. Large remotely controlled botnets can consist of hundreds of thousands of hijacked computers.

### **Malware is distributed through cracked websites**

CERT-FI continuously receives reports of cracked or vulnerable Finnish websites. Site content has been edited through addition of a hidden iframe or obfuscated JavaScript code. When the user visits a cracked website, the browser downloads a page containing malware.

This malware distribution method is known as drive-by download. The user may not notice the infection at all, and infection may occur even when the user visits otherwise reliable, trusted websites.

Malicious content can be added to the website by utilising either server vulnerabilities or stolen administrator credentials.

### **Gumblar steals FTP codes and passwords**

Malware that steals website administrator usernames and passwords, such as Gumblar, enables unauthorised editing of websites' content. The software searches for FTP administrator usernames and passwords in the password files of website administration software, such as FileZilla and Dreamweaver, on the infected computer.

Gumblar is also able to monitor the traffic between the computer and the FTP server and to separate unencrypted passwords

and usernames from other traffic. The malware uses the information to edit website content and to spread further. The information is used to add a hidden iframe containing links to malicious sites.

### **Search engines are used to attract users to harmful websites**

Search engine result optimisation is used in malware distribution. The goal is to raise a website offering harmful content higher in search engine result lists. Some search engines make use of lists of harmful websites, filtering them out from the search results.

Current events, such as natural disasters and scandals related to celebrities, are popular search topics. Search results can be affected by adding suitable keywords to the pages and by linking masses of pages to the desired target via SQL injection and malware. Following New Year's, the Haiti disaster has been a popular target among criminals.

### **Name service is vulnerable to misuse attempts**

Domain name service is an essential part of the Internet, and it too attracts misuse attempts. Malware can direct name service queries to a nameserver controlled by the attacker and the user can be directed to a fraudulent website.

The DNSSEC mechanism is available to verify name service replies, but currently it is not widely used.

### **Vulnerabilities of auxiliary applications can be utilised longer**

Malware often makes use of operating system or application vulnerabilities. Operating systems and Web browsers are often automatically updated, so their vulnerabilities can be fixed relatively quickly.

For this reason, malware often targets other applications or browser add-ons. Malware using, for example, PDF reader, Flash Player, or Java environment vulnerabilities has been detected recently.

### **Users can be lured into installing harmful software**

Cracked websites can lure users into installing malware themselves, which makes it easier to bypass operating system protection mechanisms.

Visiting a website can trigger a pop-up window warning of a malware infection. The user is instructed to install and run an application to search the computer for malware and remove harmful applications. In reality, the application itself is harmful.

Scareware can look very reliable, and it can be very hard to distinguish malware from real information security applications. During installation, the application may ask for credit card information for licence fee payment and install a keylogger or other spyware on the computer.

Malware masquerading as an information security application has been around for several years, and the number of infections is expected to only increase.

### **Widespread and targeted attacks are being seen**

Malware can be distributed widely, and this way the number of affected computers and users can be maximised. The goal can be to strengthen the attacker's botnet or to acquire personal information.

CERT-FI received reports of attacks also on specific organisations. Malware distributors forge a well-known entity as the sender of a message, the message's subject looking trustworthy and being related to the organisation's ordinary activities. The message may be an invitation to a meeting or a conference, and the recipients may be key persons of the organisation. Often the version of malware distributed is not recognised by information security software.

### **Ghostnet was unveiled**

In March 2009 a report was published in Canada on a series of extensive data system break-ins conducted via targeted malware distribution. A remote control connection established with the Ghost

malware was used to spy on information from various organisations' computers.

According to CERT-FI's information, no Finnish parties were among the distributors of this malware. CERT-FI received information on two foreign computers in the Finnish network.

### **Unjustified malware intimidation also occurred**

In 2009, CERT-FI received reports of a circulatory e-mail letter warning of malware attached to certain messages, which was described as deleting all files from one's hard disk. Previously the same e-mail message spread on the Internet in Swedish and English. In December 2009, a person working in the National Bureau of Investigation was forged as the sender.

According to CERT-FI's information, copies people sent to each other as a warning contained no malware or links to harmful websites. In addition to this circulatory letter, other letters – promising either money or mobile phones – have spread on the Internet. More traditional letters have also promised fortune or misfortune, depending on how many people the letter is forwarded to.

Traditional scam attempts sent by e-mail are reported continuously. These can offer legacies, lottery prizes, or work as a money broker.

### **Security deficiencies and malware are found in mobile devices too**

Information security problems related to smartphones' installation messages and WAP Push messages emerged in the first half of 2009.

Experts have long been aware of problems related to processing of mobile phone network setting messages. Not all mobile phones provide the user with information on the true sender of setting messages. The phone might also accept settings without the user knowing of this or not display the settings to be changed.

A WAP Push message is a message sent to the phone that contains a link to a WAP

address. Problems related to WAP Push message processing have emerged in some older phone models uncommon in Finland. A problematic mobile phone may download or even install the WAP content when a WAP Push message is received without the user knowing of this.

### **A worm spread over iPhone mobile phones**

A network worm, Ikee.B, was found on Apple's iPhone mobile phones. This worm spread from one phone to another via the sshd service and unchanged default passwords. The worm spread only to phones with locking removed, enabling installation of applications not officially approved by Apple. The sshd application cannot be installed with locking enabled.

### **Smartphones are a tempting target**

Smartphones' properties and functions approach those of personal computers. They often have a continuous Internet connection and can be reached from the Internet. The applications used are at least partially the same as or resemble applications used on ordinary computers.

Operating system and application information security is in many ways worse in smartphones than in ordinary computers. Normally, the phones have no information security applications installed and have no centralised management or automatic software updates. Phones also are lost or stolen more often. Also, phones use several networks, providing the worms with possibilities to spread easily.

### **Malware was encountered also on other devices**

ADSL terminal devices hijacked to form botnets were found in Finland at the start of the year. It may be difficult to detect an infection in a network's active devices, and protecting a device and updating software may prove more complicated than simply ensuring that workstation software is updated regularly.

## **Internal cooperation to stop misuse is proceeding well**

Parties designing and spreading malware and operating botnets are well networked, with the operation resembling models used in the software and ICT service industry.

Servers used to spread malware and used as botnet command servers are often hired from large service providers, who may have subcontracting relationships in place where they hire out physical server equipment to those who hire out the actual service capacity. The hosting service provider may not necessarily have knowledge of the criminal end customer. At the other extreme are parties focusing on criminal activity who have the appearance of legitimate hosting service providers.

## **There are no signs of a slowdown of growth in the number of misuse cases**

Investigation of botnet operations based on distributed activity requires comprehensive international cooperation. CERT organisations, Internet service providers' data security units, researchers in universities and companies, and police authorities are networking to form more efficient cooperation networks. The activity of these networks increased significantly in 2009.

## **International cooperation of information security communities is succeeding**

An example of the successful information security cooperation is the investigation of a denial of service attack targeted partly at a Finnish company in autumn 2009.

International cooperation provided CERT-FI with the botnet command and control server address used in the attack an hour after the information security breach notification was received. Efficient procedures limiting the effects of the breach were initiated rapidly. CERT-FI also warned several foreign parties targeted by the same botnet attack. Command servers were cleaned from several countries around the world.

## **Operators providing harmful content were blocked from the Internet**

Several operators shown by information security community research to be concentrating on harmful activity lost their network connection in 2009. Perhaps the best-known case was that of American service provider 3FN. Several junk-mail network command servers were maintained in this provider's network.

CERT-FI assisted Icelandic colleagues in investigating a case of malware stealing online banking usernames and passwords. A Latvian service provider clearly focused on harmful activity was found in the investigation. Latvia is the closest EU country to the Nordic region where increased activity degrading information security can be observed.

## **Conficker brought information security parties together**

One of the largest common international information security community efforts was targeted at the Conficker malware family. A special team, the 'Conficker Working Group', developed defence against the malware. For the first time, also ICANN, responsible for managing domain names, participated in the effort. Fighting Conficker required preventing registration of a large number of domain names.

## **CERT-FI has completed comparative research on European CERT organisations**

CERT-FI completed a study of European CERT organisations in 2009. The purpose of this research was to compare the operation of 11 CERT organisations and to identify good practices that could be utilised in CERT-FI and FICORA. This research was the first of its kind in Europe, and its results have been met with international interest.

Similarities and differences among CERT organisations participating in the research were discovered. From the results it can be stated that all organisations are unique. Each has adapted its operations to meet the requirements of the operating environment and the customers.

Nonetheless, there are many similarities. All organisations are a national contact point for processing of information security breaches. Being a contact point requires broad, well-functioning domestic and international contact networks, which all organisations considered important.

In addition, all organisations offer customers basic services, including analysis and co-ordination in information security breaches targeting their country, monitoring of the national information security situation, and creation of status reports.

The research also showed that preparedness for efficient CERT activity varies significantly among European countries. The European Commission has also paid attention to this.

### **FICORA is participating in developing CERT activities in African countries**

In 2009, FICORA provided international expert assistance in establishment of national CERT activities. South Africa is being aided in creating and implementing CERT functions in a project funded by the Ministry for Foreign Affairs.

A project worker has been employed in CERT-FI to support the South African partner organisation in planning the CERT activities. Additionally, this worker's responsibility has included initiating and co-ordinating international cooperation and to organise events and training.

Kenyan and Tanzanian communications authorities have also been provided with ideas on how to design and start CERT activities.

### **Autoreporter has been honoured**

CERT-FI's Autoreporter-palvelu was rewarded in a contest organised by FIRST (the Forum of Incident Response and Security Teams) and CERT/CC (CERT Coordination Center)<sup>1</sup>. The contest was held in order to determine best practices

for detecting and preventing information security violations.

Autoreporter is a service produced by CERT-FI that automatically collects malware and information security breach information related to Finnish networks. In 2009, the system sent out nearly 215,000 notifications to Finnish network administrators. The number of notices has increased by 250% from that of the previous year. To some extent, the reason for the increasing numbers is the number of notifications concerning the Conficker worm.

CERT-FI will publish detailed statistics on malware detected in 2009 in its next information security report, in April 2010.

### **Several extensive software vulnerabilities were published**

CERT-FI published the results of two extensive vulnerability-related co-ordination projects in 2009. They concerned vulnerabilities of libraries related to TCP implementations and XML file processing. Vulnerabilities related to Microsoft's ATL development library and SSL protocol were also published.

### **Vulnerability with TCP was revealed**

Problems related to TCP implementations enabled denial of service attacks even with very low amounts of traffic. Sixteen manufacturers issued statements for the vulnerability notification published in September. CPNI<sup>2</sup>, JP-CERT<sup>3</sup>, and US-CERT<sup>4</sup>, who participated in the co-ordination work, published their own reports.

### **Vulnerabilities were found in XML file processing**

The Finnish Codenomicon Oy provided CERT-FI with results of XML file processing application tests for co-ordination. Three XML file processing libraries had vulnerabilities.

1 <http://www.cert.fi/tietoturvanyt/2009/06/ttn200906301435.html>

2 <https://www.cpni.gov.uk/Products/technicalnotes/Feb-09-security-assessment-TCP.aspx>

3 <http://www.jpCERT.or.jp/english/at/2009/at090019.txt>

4 <http://www.kb.cert.org/vuls/id/723308>

Patches for relevant applications have been published by 12 manufacturers. Some vulnerabilities were fixed in code distribution of the library, but the fixes had not spread to all products using the library. This indicates that fixing vulnerabilities is not limited to removing their cause. It is important to inform all parties whose products the vulnerability affects of fixes and their details.

### **Errors in Microsoft's software development libraries emerged**

A vulnerability was discovered in Microsoft's ATL software development library version, which enabled running the attacker's code on the target system. The source code has not been published as a product, but it is used in many applications. Microsoft has published a patch for the vulnerability, and prevention lists blocking the vulnerable components have been distributed as part of the monthly updates.

Since this vulnerability concerns not only Microsoft's products but also many third-party products, Microsoft announced that it has begun cooperation with other manufacturers to correct the errors.

### **A vulnerability of the SSL/TLS protocol also was uncovered**

An SSL/TLS protocol vulnerability published in November in some cases enables addition of one's own content when an encrypted connection is opened. The vulnerability does not enable theft of confidential information, but it is still considered serious, because SSL encryption is an essential part of security in sectors such as e-trade.

The vulnerability is a rare case, in that its cause is an error in the protocol design and in practice it affects all SSL/TLS implementations. When an error is introduced early in the system development cycle, the extent of a vulnerability becomes wide and correcting the error becomes difficult.

This vulnerability is corrected by specifying an extension to the TLS protocol, which eliminates the vulnerability.

## **Changes have been made in the Act on the Protection of Privacy in Electronic Communications**

The amendments to the Act on the Protection of Privacy in Electronic Communications came into effect in June. In addition to authentication information processing rights, the change concerned paragraph 20 on information security actions. This paragraph was changed so that it better meets the requirements of telecom operators, added-value-service providers, and corporate subscribers.

In preparation of the change, the society's fixed and vital dependency on communications networks, services, and IT systems was taken into account. Ensuring the operation of electronic information and communication systems is an essential part of protecting critical infrastructure. Effects of information security threats must be minimised in Finland, since we only have limited control of foreign parties and systems.

The law states that telecom operators, added-value-service providers, corporate subscribers, and parties acting on their behalf have the right to act as specified in the law to ensure information security.

One situation in which action can be taken is detection, prevention, and investigation of disturbances affecting information security of communication networks and services related to them, and reporting of these disturbances to the authorities. Another way in which action can be taken is to ensure the communication abilities of a sender or recipient of a message. A third area of action of this type is prevention of preparation of large-scale financial frauds perpetrated via communication services.

### **Possibilities offered by the new law were utilised to protect online banking users**

After the act went into effect, FICORA recommended that telecom operators take actions to protect Finnish online banking users as specified in the act. In this classic case, an American network operator had repeatedly taken part in phishing and fraud targeted at online banking users.

Telecom operators do not require FICORA's recommendation before performing traffic filtering. Filtering can be used when the telecom operators evaluate the requirements as being met.

### **Swedish intelligence operation can have an effect on Finnish telecommunications**

A new act concerning signals intelligence in Sweden went into effect on 1.12.2009. This act gives Sweden's National Defence Radio Establishment (Försvarets Radioanstalt) the right to perform signals intelligence activities related to national defence also in fixed networks for electronic communications outside Sweden: communication traffic to Sweden and passing through Sweden is also affected by the signals intelligence act.

Intelligence activities targeted at communications traffic passing through Sweden are taken into account in FICORA's renewed regulation, which concerns telecom operators' responsibility to inform their customers and FICORA of security threats targeting their services. This regulation became effective at the beginning of 2010. The regulation emphasises telecom operators' responsibility to inform their customers of information security threats targeting services implemented abroad but offered to Finnish customers. This responsibility is detailed in the Act on the Protection of Privacy in Electronic Communications.

FICORA has reminded telecom operators of this since 2007. It has also been brought to attention that they must observe information security in the production of their services. If the telecom operator is not capable of providing the service without jeopardising information security, the telecom operator must notify its customers and FICORA of this. On the basis of the notifications, the customers can assess whether the service meets their information security requirements. Also FICORA has published information on protecting communications.<sup>5</sup>

### **Trends emerge**

CERT-FI sees that malware will be used for attempting to gain financial benefit also in the future. Credit card numbers and usernames are the most interesting and easily sold pieces of information.

Social networking sites are good targets for many types of scam attempts. Some sites offer payable services, which can be further sold within the service, but username and credit card information phishing are commonplace alongside this.

In addition to researching smartphone application vulnerabilities, it is expected that mobile network protocol and network operation investigation will become more interesting. Software for simulating mobile network operation was published in 2009.

In addition to researching smartphone application vulnerabilities, it is expected that mobile network protocol and network operation investigation will become more interesting. Software for simulating mobile network operation was published in 2009.

---

<sup>5</sup> <http://www.ficora.fi/viestinsuojaus/>

Most contacts processed by CERT-FI addressed harmful applications of various types and information security threats related to them.

CERT-FI contacts by subject type	2009	2008	Change
Interview	<b>97</b>	88	+10%
Vulnerability or threat	<b>148</b>	375	-61%
Malware	<b>1828</b>	2156	-15%
Guidance	<b>387</b>	359	+8%
Preparation against attack	<b>48</b>	87	-45%
Information break-in	<b>120</b>	187	-36%
Denial-of-service attack	<b>89</b>	96	-7%
Other information security problem	<b>118</b>	43	+174%
Social engineering	<b>164</b>	189	-13%
<b>Total</b>	<b>2999</b>	3580	-16%