

**cert-fi**

**INFORMATION SECURITY REVIEW  
3/2009**

21.10.2009

# CERT-FI Information Security Review 3/2009

## Introduction

Between the start of 2008 and the end of August 2009, CERT-FI handled some 1,800 cases in which data-stealing malware conveyed user information to outsiders. Finnish users have also been targeted by this kind of malware.

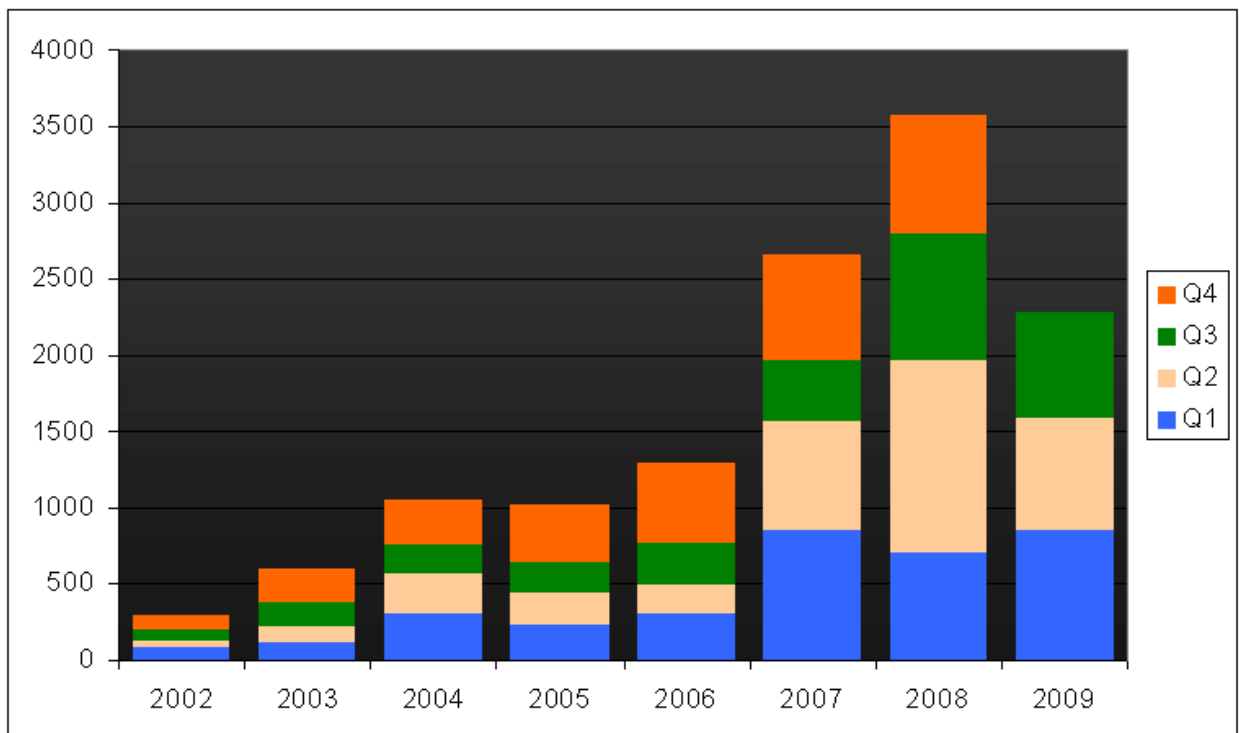
The results of two larger-than-average vulnerability coordination projects have been published. August saw the publication of a coordination project related to XML libraries. XML libraries are used for processing data and documents in various types of information systems.

The results of a long-term vulnerability coordination project related to TCP protocol server implementation were released in September. TCP is a network communication protocol that is used for data transfer in most Internet

applications, making this issue relevant to many software manufacturers.

The goal of vulnerability coordination is to have manufacturers test their products and rectify any vulnerabilities that are found. Thanks to smooth cooperation between CERT-FI and software manufacturers, the coordination projects turned out well.

Besides numerous foreign services, a Finnish website has also been the target of a Denial-of-Service attack. CERT-FI is coordinating the investigation of this case. The investigation has progressed well, owing to international cooperation.



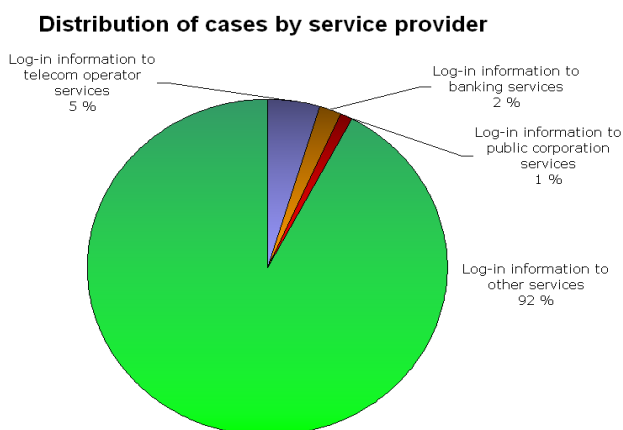
The number of contacts handled by CERT-FI is somewhat lower compared to last year.

## Malware stealing Finnish users' identification data

CERT-FI occasionally receives reports of cases in which users of Finnish e-services have fallen victim to data-stealing malware. These reports may also include information compiled by the malware. The information gathered by malware usually comprises log-in information, such as user IDs and passwords, for e-services. However, malware also gathers information from web browser forms, such as e-mails, online purchases and online banking forms.

Between the start of 2008 and the end of August 2009, CERT-FI handled some 1,800 cases related to data-stealing malware. Most of the targeted services were social networking sites of various kinds on the Internet. In a significant share of the cases handled by CERT-FI, the target has been the international service provided by a Finnish company. The majority of cases thus involve foreign users of the service in question.

When reviewing cases, it should be noted that stolen sign-in information for online banking services constitutes only a small proportion of all stolen information. Credit card information is not included in the data received by CERT-FI, since there are other established reporting channels for such information.



## Websites infected with malware are common

Malware is increasingly often contracted by visiting a cracked website that distributes it. FTP codes hijacked by the malware are used to embed a JavaScript code in the website's code. This JavaScript code may, for example, download malware or a link to a concealed iframe tag that downloads malware. Malware contraction may occur if a random site visitor's browser add-ons or software used for viewing content, such as Adobe Acrobat or Flash Player, are vulnerable and the antivirus software is not up-to-date.

Once a computer is infected, the malware may monitor the workstation's network traffic in order to steal the user's FTP codes and passwords. It can also use the workstation to send spam email, install malware resembling antivirus software, or doctor Internet search engine results in order to direct the user to fraud websites. The operational mechanisms of malware vary in accordance with the software in question.

Software in the Zeus family of malware can also gather codes and passwords by storing key strokes and sending them to a command server for later exploitation.

Stolen codes can be used for adding content that has been created for attack purposes to new websites.

## Search engine result optimisation is used for the distribution of malware

For a number of years now, search results provided by search engines have been used for malware distribution. This year, this phenomenon has become more common and taken on new forms. Malware is distributed through cracked websites or ones established on servers expressly created for the purpose. Malware distributors strive to raise these websites to the top in the search result standings, by means of search engine optimisation.

Search engine optimisation involves adding search words related to topical events to malware sites. As a result, while following some search engine results,

users searching for further information on a topical subject end up on a website that tries to exploit browser vulnerabilities to contaminate the user's workstation or dupe the user into installing the malware.

### **Browsers and search engines recognise some fraud websites**

Websites infected with malware may be difficult to spot. Such websites may in no way differ in appearance from normal, uninfected websites. This phenomenon is known as drive-by-download.

It should be noted, however, that during the last year, search engine companies have made significant investments in ensuring that websites provided in search results are inspected for malware and exploitative processes transmitting malware. The most widely used search engines now alert the user if a website containing malicious content is included in the search results. Browsers can also alert users to malicious content.

Some websites try to circumvent the security check mechanisms of search engines. This is done by having the links shown in the search engine results direct the user to a website that is merely used for redirecting the user to a new site containing malware. The server responsible for the last website in the chain checks the Referrer field value of the HTTP request. Based on this, only visitors redirected from certain websites are offered a website that distributes malware.

### **Clean-up of site is not enough, recontamination must also be prevented**

Cleaning the content of a site that has been infected by a malware does not always suffice. The webmaster of the site should be notified that the usernames and passwords used for updating the site have fallen into wrong hands and that the computer is infected. This may prevent the site from recontamination. The ftp password used for site maintenance must be changed.

### **Authorities go on the offensive against malicious content**

At the beginning of June, the US hosting services provider 3FN was blocked from using the Internet by official decree, upon the request of the Federal Trade Commission (FTC). According to the FTC, the service provider had actively protected criminals by failing to react to so-called takedown requests. In its complaint, the FTC accused the service provider of distributing malicious content, including malware, child pornography and spam email. The company was further accused of consciously maintaining a network of hijacked computers, or botnet, and maintaining the botnet's command servers.

The operator was disconnected by means of a court order, with an immediate impact on the amount of spam email sent by the Cutwail botnet. This impact was not, however, equal in magnitude to the case of service provider McColo, disconnected in November 2008. Its network comprised several botnets that were sending out spam email and, following its elimination, the amount of spam temporarily dropped to a third of previous levels.

The exceptional aspect of the disconnection of 3FN lies in the service provider being disconnected from the Internet by official decree. Previously, in the cases of McColo and another US service provider, Intercage, the key factor in their disconnection was continual reports of malicious traffic and criminal activity sent to telecom operators by the international data security community.

### **CERT-FI published the results of extensive vulnerability coordination projects**

In August, CERT-FI published the results of a vulnerability coordination project concerning XML libraries, with a greater scope than average. This project was so extensive due to the fact that the XML language is used for processing information and documents in various types of information system. Moreover, the vulnerabilities of software libraries generally have extensive implications, since vulnerable libraries are often used in

dozens or hundreds of application software programs.

The results of a long-term vulnerability coordination project related to TCP protocol server implementation were released in September. TCP is a network communication protocol that is used for data transfer in most Internet applications, making this issue relevant to many software manufacturers.

The goal of vulnerability coordination is to make manufacturers test their products and rectify any vulnerabilities that may be found. CERT-FI has been in contact with a hundred software manufacturers during TCP vulnerability coordination. So far, 13 software companies have released a statement or software fixes on the basis of the information provided to them.

In extensive vulnerability coordination projects, the risk of failure grows as well. Failure usually refers to the partially or completely premature disclosure of detailed information concerning a vulnerability. Premature disclosure of details may lead to exploitation of the vulnerability in attacks.

Both of the published projects achieved their goals. The vulnerability details have not been published in full in either case. The coordination project related to TCP protocol-related vulnerabilities and work to identify vulnerable manufacturers will continue. A vulnerability bulletin related to the project can be found at [www.cert.fi](http://www.cert.fi)

### **Denial-of-Service attack against a Finnish website**

CERT CERT-FI has taken an active role in solving a case in which a Finnish company was subjected to a DoS attack. The Finnish website was not the only target of this attack; several foreign websites were also targeted.

Coordination related to this case is still underway. The work got off to a good

start: the botnet attacking the service was identified very quickly by means of international cooperation.

In the case of DoS attacks, the impact of the attack can be limited through rapid cooperation with the attacked party's ISP and CERT-FI.

If the organisation's operations are heavily dependent on Internet services that work in all circumstances, the required preparatory measures should be discussed with the service provider in advance.

DoS attacks are rather rare in Finland.

### **FICORA participated in the Tieto 2009 preparedness exercise**

FICORA participated in the Tieto exercise, held in early October.

The objective of this exercise was to enhance the authorities' and administration's ability to cooperate in solving problems related to information systems.

In addition to the Defence Forces, the government's information administration and some ministries, IT companies, including telecom operators and ICT service providers, also participated in the event.

### **Future prospects**

Data-stealing malware and campaigns to distribute it through spam email and websites will in all likelihood play a prominent role during the rest the year. Messages disguised as holiday greetings or Christmas offers are a typical method of distributing malicious content.

Malware can also be disseminated through links included in messages.

<b>CERT-FI contacts by subject type</b>	<b>1-9/2009</b>	<b>1-9/2008</b>	<b>Muutos</b>
Interview	78	67	+16%
Vulnerability or threat	107	323	-67%
Malware	1451	1719	-16%
Guidance	250	243	+3%
Preparation for attack	29	71	-59%
Information break-in	101	147	-31%
Denial-of-service attack	63	72	-13%
Other information security problem	82	33	+148%
Social engineering	118	127	-7%
<b>Yhteensä</b>	<b>2279</b>	<b>2802</b>	<b>-19%</b>

Malware reports form a majority of contacts handled by CERT-FI.