

# **CERT-FI INFORMATION SECURITY REVIEW**

11 April 2008

# CERT-FI information security review 1/2008:

CERT-FI was reported about a case where a third party succeeded in making bank transfers during an internet banking session without the user knowing about it. So far, the attacks made against Finnish banks have been isolated incidents.

CERT-FI published a group of vulnerabilities related to the handling of packing and archive formats. Information is compressed or archived in almost all applications. Therefore, vulnerabilities affect many different operating systems and software. As a whole, these vulnerabilities can be characterised as significant.

Numerous cross site scripting vulnerabilities of Finnish websites came to publicity. These vulnerabilities do not enable server break-ins, but they can be used for scam attempts or hurting the website owner's reputation.

## ***Finnish internet banking connections hijacked by malware***

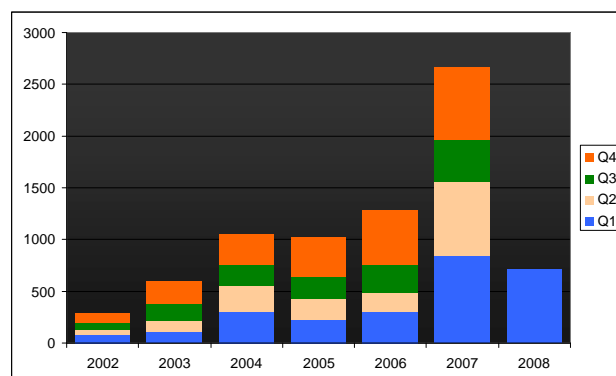
CERT-FI was informed of the first malware spying internet banking connections and successfully targeting its activities against Finnish internet banking customers. The malware characterised as a **banking trojan** was spread to Finnish addresses, in particular, via a targeted spam campaign. The subject of the scam messages was about either an alleged nuclear power accident in the central Finland city Mikkeli or a contact request from "Tatjana" looking for company. The links in the messages directed users to a website having the potential to infect one's computer with a malware.

The malware diverted the user's internet banking connection to pass through the computer controlled by the attacker who could thus, during the connection, monitor and change the information shown to the user and transferred to the bank's internet service. This

helped the attacker to make unauthorized bank transfers from the users' accounts.

Malware targeted at internet banking services develop so that the same malware is able to lure as many bank's customers as possible. The malware are made to be easily customized, which allows them to be directed at new internet banks by changing the configuration files of the software only. The program that has infected the user computer regularly seeks a new configuration file online, so it is possible to change and steer its behaviour after the infection, too. The malware found in Finland has formerly been used at least against German, Swiss and Dutch internet banks. The software version used was first unknown to anti-virus software, so they did not immediately protect from infection.

In the future, it can be expected that malware meant for hijacking internet banking connections are able to independently change the contents of the website exposed to the user already during the connection, steer the users' sessions into the web server controlled by the attacker and change the contents of the http messages sent by the user. The hijacking may be successful even though the connection is SSL-protected. Insofar, CERT-FI has not, however, been notified of malware with a fully-automatic function directed at Finnish internet banking customers.



*During the first quarter, 709 handled contacts were registered with CERT-FI's incident control management system.*

## ***Vulnerabilities in the handling of packing and archive formats***

Together with the British CPNI and the Japanese JPCERT, CERT-FI published several software vulnerabilities related to the handling of packing and archive formats. Some of them may enable the execution of the attacker's program code in the computer.

Nearly all applications involve the handling of archive formats. Normally, the aim is to compress the data to be handled in order to speed up the transfer of data or reduce the storage space required by files. In context with their normal functions, many software have to deal with compressed data and archive files consisting of many different files.

In context with the vulnerabilities, test material compiled by the Oulu university information security research group, OUSPG, was published. The material was put together with the help of the test methods developed in the PROTOS-GENOME project. The handling of files included in the test material caused fault situations in several different software products. The material consisted of over million different test incidents which tested the black spots of the implementation of over ten different archive formats.

Software manufacturers were offered an opportunity to test their own products before the material was published. CERT-FI, CPNI and JPCERT contacted tens of software manufacturers. The goal was to pass the information about the test results to major software manufacturers and to those whose products have had problems before.

The aim of publishing the test material was to enhance the quality of the implementation of handling archive formats instead of looking for isolated errors. During the project, it was remarked that manufacturers used to correcting isolated, strictly-determined programming errors were sometimes unable to exploit the given information or test material. The coordination was faced by the challenge of a great number of manufacturers.

The parties of the project are of the view that the public test material regarding archive formats improves the reliability of software implementations. CERT-FI and OUSPG will continue their cooperation in order to compile and publish comparable test material.

CERT-FI will monitor the situation after the vulnerability publication. In all likelihood, not all vulnerabilities related to packing and archive formats have yet been found or patched. It is recommended that the updates provided by software manufacturers are installed without delay.

## ***Many websites have cross site scripting vulnerabilities***

Sampo Bank renewed its information system and internet banking at Easter. When the new web bank was introduced, a cross site scripting (XSS) vulnerability was found on the website enabling third parties to expose their content as part of the bank's website when the user moved to the website via a maliciously formed link.

<b>CERT-FI contacts</b>	<b>Q1/2008</b>	<b>2007</b>	<b>2006</b>	<b>2005</b>	<b>2004</b>	<b>2003</b>	<b>2002</b>
Interview	17	80	51	46	59	48	27
Vulnerability or threat	39	64	87	134	33	13	8
Malware	460	1678	536	212	216	115	34
Guidance	64	393	291	366	425	149	116
Preparation for attack	32	3	26	14	73	70	27
Data break-in	25	119	45	49	31	30	46
Denial-of-service attack	15	64	18	12	21	34	15
Other information security problem	10	48	67	129	141	98	3
Social Engineering	47	197	109	25	2	1	0
Spamming	-	18	58	31	46	36	12
<b>Total</b>	<b>709</b>	<b>2664</b>	<b>1288</b>	<b>1018</b>	<b>1047</b>	<b>594</b>	<b>228</b>

The vulnerability did not cause major threat to service users and it was corrected immediately. The wide publicity received by the incident nevertheless inspired network users to seek similar information security flaws from other websites. As a result, CERT-FI was reported of tens of different cases regarding Finnish websites.

Cross site scripting vulnerabilities make it possible that the contents created by a third party are exposed to the user as if they were part of the authentic site. In order to exploit the vulnerability, the website user is lured to enter the program code used in the attack into the web server which then returns the code to be run in the user's browser. The server does not validate the data entered by the user accurately enough, which opens the way for the vulnerability. Typically, JavaScript programming language is exploited in the vulnerabilities.

In addition to using XSS vulnerabilities for the purpose of making fun or defacements as we have now seen, they can be used for e.g. collecting passwords used in the service. A link with a short piece of code exploiting the vulnerability can be spread via spam messages. The password inquiry exposed to the user on the authentic website may thus originate from the attacker. CERT-FI has not, however, been reported about cases where the vulnerabilities of banks or other services would

have successfully been used for other purposes than making fun.

CERT-FI has informed service maintainers of the vulnerabilities. They have for the most part either corrected the vulnerabilities or removed the vulnerable service temporarily from use.

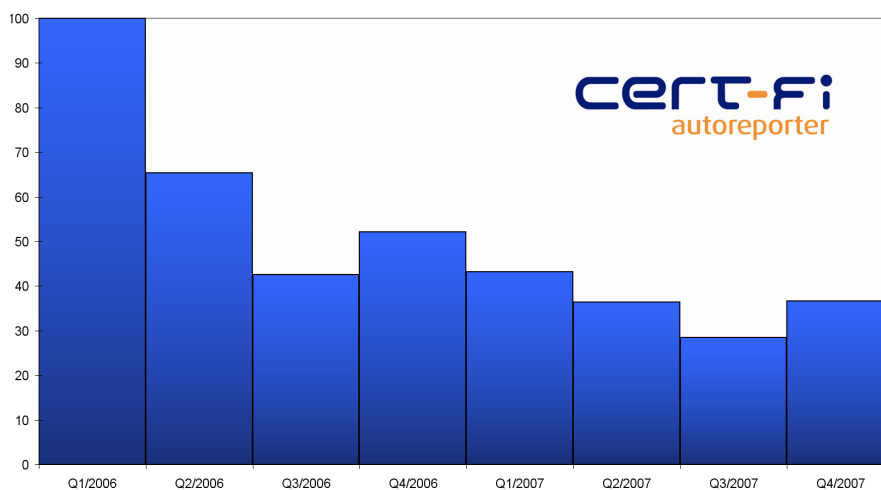
### **Future prospects**

According to CERT-FI, systematic spread of malware and using them for criminal purposes can in the future involve increasingly more often Finnish services, too. It is likely that the aim is to spread malware to specifically Finnish users, for example via websites or spam messages in Finnish sent to Finnish e-mail addresses. The scams are likely to become increasingly more credible and the characteristics of malware used in the attacks develop from what they are now.

Website vulnerabilities are continuously sought after and it is expected that more is likely to be found.

The now-published test material is expected to help find more vulnerabilities related to packing and archive formats, and software manufacturers release patched versions of their products. CERT-FI will soon also publish certain vulnerabilities in software widely used for protecting data transfer.

Malware incidents per broadband subscribers, Q1/2006 = 100



*The number of malware incidents has dropped during the past two years compared to the number of broadband customers.*