

cert-fi

**INFORMATION SECURITY REVIEW
1/2010**

9.4.2010

CERT-FI Information Security Review 1 / 2010

Introduction

The publication of user credentials stolen in March from the online gaming service Älypää threatened the information security of the game site's registered users. More than 125,000 usernames, passwords, and e-mail addresses were published on the internet.

In February, it was discovered that credit card information of more than 100,000 card-owners were stolen from the computer server of a coffee shop in Helsinki.

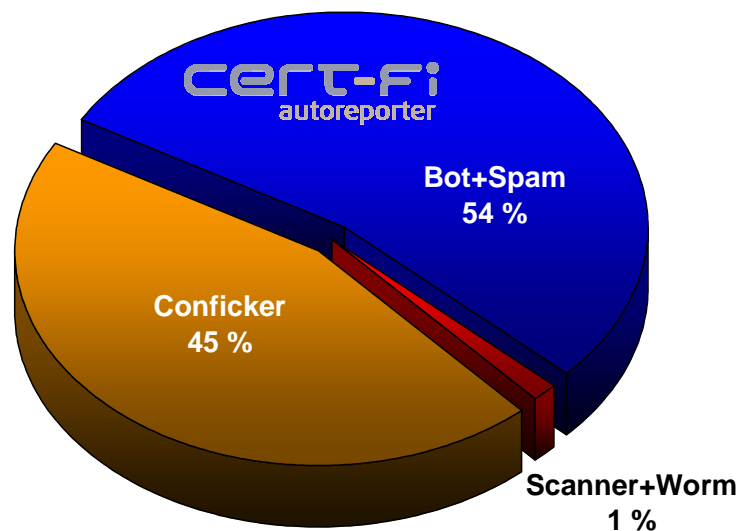
More focus needs to be put on secure implementation of online services. Poorly implemented information security enables password theft and unauthorised content. Also, the users' password practices often leave a great deal to be desired. Much too weak passwords used for a variety of

online services increase the risk of misuse.

Malware targeting online banking sessions already know Finnish online banking systems. The banks are adding security measures to prevent unauthorised money transfers. So far, the number of malware targeted at Finnish banks is small.

Statistics from CERT-FI's Autoreporter system show that the number of malware detections increased significantly in 2009 in comparison to the previous year. Nearly half of the reports on malware were on the computer worm Conficker. In 2009, CERT-FI sent out almost 100,000 reports concerning Conficker malware infections.

Incidents by type 2009



Conficker alone comprised nearly half of the malware reports in 2009.

Passwords of the Älypää game site made public

At the end of March, it was discovered that someone had managed to steal all usernames, passwords, and e-mail addresses used for registration with the alypaa.com site.

A file containing the personal information of more than 125,000 users was made available through several file-sharing systems, and the news spread rapidly over the internet.

Signing into the Älypää game site was quickly blocked, but the users' information security was compromised also because many people had used the same password for other online services. In many cases, a person's e-mail address was used to guess the username, and then the password stolen from the Älypää service was tested.

CERT-FI has received reports on, for example, the unauthorised use of a person's Gmail account or Facebook login credentials.

Passwords leave much to be desired

Usernames and passwords are the most common way of verifying users' identity online. More attention needs to be paid to choosing and storing the passwords.

A review of the passwords stolen from the Älypää game site reveals many passwords that are much too easy to guess or too short. Use of the same password on several online services should be avoided, and everyone should take precautions in case the password system of any online service gets cracked or the password ends up in the wrong hands some other way.

Shortcomings in the implementation highlighted

According to CERT-FI, stealing passwords from the Älypää game site may have involved taking advantage of the site's out-of-date implementation as well as its design shortcomings when it comes to information security.

Apparently, the passwords were stored in plaintext format in the database. The database may have been accessed through a type of SQL injection technique exploiting the system's vulnerability caused by insufficient input validation.

Homepages of politicians defaced

Some cases of unauthorised editing of public figures' homepages came to light in March.

According to CERT-FI, the site administrator's password, which had been either guessed or obtained through some other means, was used. The content of the pages had been edited through their usual administrative interface.

Insufficient input validation may enable data leaks or defacement

More and more websites include a database controlled through SQL commands. These commands can be used to search for or edit information in the database.

The database may contain website content, usernames and passwords required by the service, or data used to create the pages shown. The database may be accessed through, for example, Web forms included on the website, or a URL for the website.

If user input validation is insufficient, it may be possible to pass commands to the database that, in turn, make data search or unauthorised editing of the website possible. Passwords should never be stored in the system in plaintext format.

CERT-FI continuously receives reports of websites vulnerable to various types of SQL injection. There are easy-to-use programs available for searching for vulnerabilities and testing exploitability of web sites.

Data theft through malware

The credit card numbers of more than 100,000 card-owners were stolen from the computer server of a coffee shop in Helsinki in February. Credit card numbers are the most common target of data-theft malware. Credit card numbers can be used for shopping or resold for criminal purposes.

Malware reports increased in 2009

Statistics provided by the Autoreporter system of the year 2009, published by CERT-FI, show that the number of malware reports has increased significantly from that of the previous year.

The growth in the number of detections has been influenced in particular by the computer worm Conficker, which spread especially rapidly in the first half of 2009.

Among all malware detections reported that year, 45% were caused by Conficker malware alone. One per cent of detections were related to cases of intentional data breach, and the remaining 54% involved unspecified types of botnet malware used for purposes such as sending spam mail.

Because Conficker can be categorised as a type of botnet malware too, it is easy to conclude that malware detection related to botnets has grabbed almost all the attention.

In 2009, CERT-FI sent out nearly 100,000 reports on detection of Conficker malware. In the space of one year, malware infections were detected in connection

with more than 25,000 IP addresses in Finland.

CERT-FI's outreach to chronic malware targets

According to CERT-FI's monitoring, the same addresses often keep reappearing in reports of malware infections.

For instance, the vast spreading of Conficker has forced CERT-FI to reach out actively to the owners of computers whose addresses frequently appear in reports of malware. Throughout the year, CERT-FI will continue actively reaching out to users who frequently get targeted by malware.

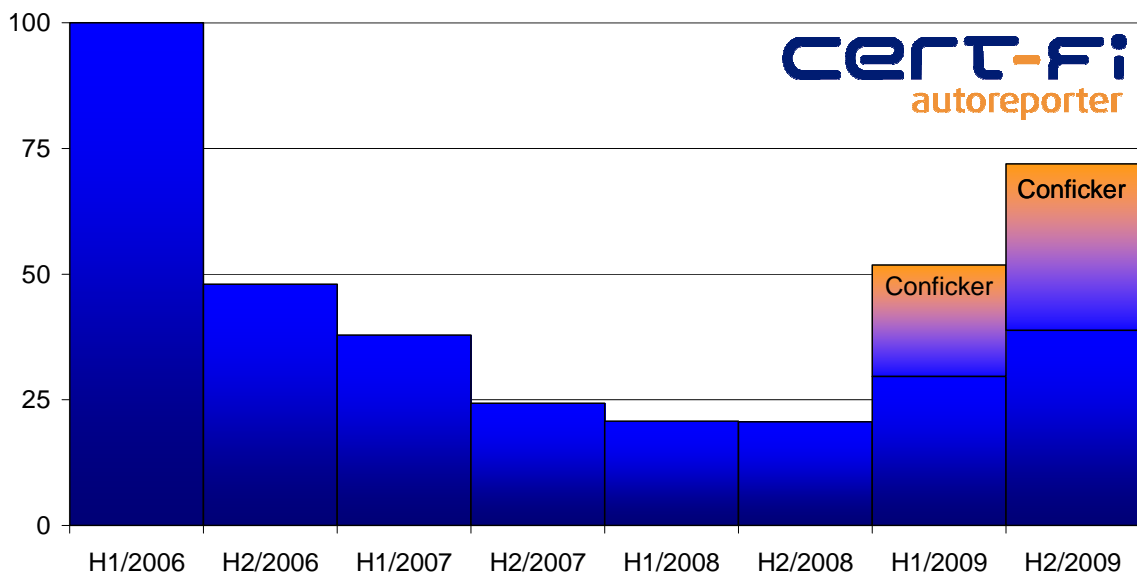
Conficker as a continuing threat

Conficker malware has infected millions of computers, around the world. Computers infected by Conficker are still waiting for a software update and further instructions. For now, the botnet of computers infected by Conficker is not being exploited on a wider scale.

It is noteworthy that computers infected by Conficker also become vulnerable to infection by other malware, because Conficker disables some security features of the operating system.

Malware Incidents per broadband customer

(H1/2006=100)



Malware targets online banking service users' money

Haittaohjelmat, joiden avulla pyritään verkkopankki-istunnon aikana tekemään luvattomia rahansiirtoja käyttäjän tililtä, toimivat jo myös suomalaisissa verkkopankeissa.

Malware targeted for performing unauthorised money transfers from users' accounts during their online banking sessions have evolved to include also the Finnish online banking services.

Although the number of malware targeted at users of online banking services is still fairly small in Finland, in CERT-FI's view the phenomenon appears to be permanent.

Through international co-operation, several internet service providers spreading malware and providing services used to hijack online banking sessions have been successfully removed from the internet.

Banks are considering countermeasures to prevent unauthorised money transfers made through the use of malware. Unusual transfers may require verification, for example, by means of a text message or a phone call.

A verification system unaffiliated with the online banking environment helps to ensure that unauthorised money transfers do not go through.

Abuse of SMS messages has increased

The amount of 'spam' sent via SMS has increased in recent years. The trend has started to reach Finland's mobile phone users as well: a growing number of fraudulent SMS messages are targeted at mobile phone numbers registered in Finland, and the messages are often in Finnish.

CERT-FI has been notified about a case where a mobile phone number in Finland was forged as the sender of fraudulent SMS messages. As a result, people who received these messages reciprocated with a large number of angry SMS messages and phone calls to that particular mobile phone number. Because of the large volume of SMS messages and

calls to that phone, normal use of the mobile connection became impossible.

Traditional telephone and mobile networks are often designed to presume that other networks and network devices are reliable. For this reason, in some cases the investigation and prevention of abuse exploiting phone networks has proved difficult.

Tracking down a harasser can be difficult, especially if that person has direct control over mobile network devices, such as an SMS service centre.

Vulnerability coordination slow in early 2010

In recent years, CERT-FI has analysed several wide-effect vulnerabilities related to software libraries, file formats, and protocols. However, early 2010 has been quite ordinary so far when it comes to vulnerability coordination.

In January 2010, CERT-FI published two vulnerabilities; one for Linux IPv6 implementations and the other related to GNU Gzip file compression software.

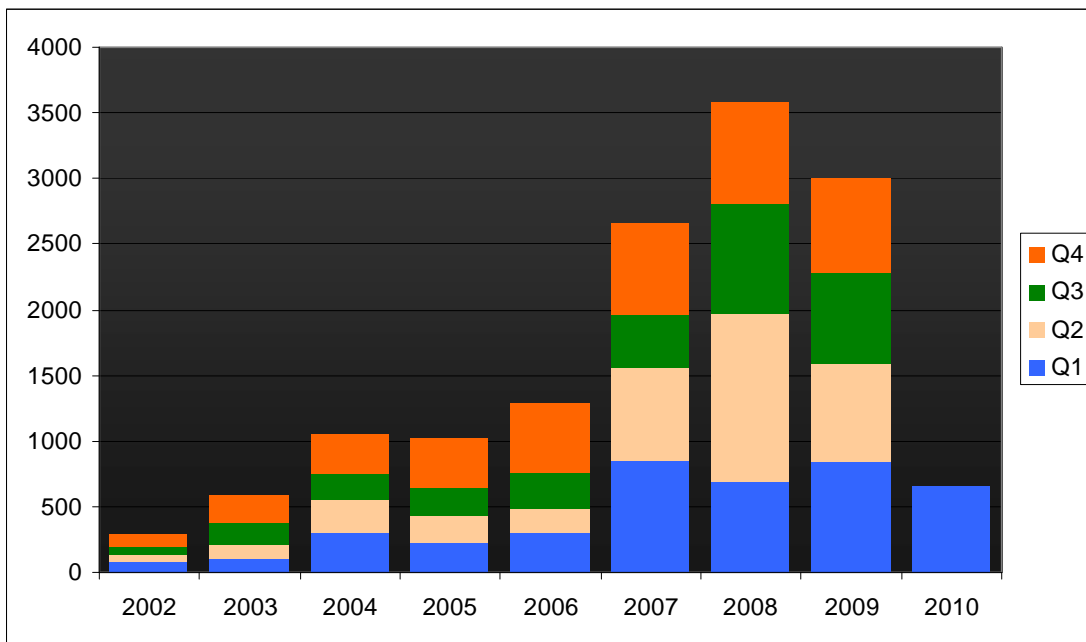
In both cases, the software manufacturer provided an updated version of the software, and most operating system distributions quickly added the updated versions to their software packages, helping to keep the threat of vulnerability to users fairly low in all phases of the coordination project.

Future prospects

In the near future, more cases of misuse related to stolen passwords published recently may come to light. By guessing other people's usernames and passwords, one might steal, for example, a person's e-mail account and identity.

CERT-FI continuously monitors the development of malware designed to steal information and hijack online banking connections, and we participate in international co-operation to minimise the harm caused by such malware.

| CERT-FI contact by subject type | 1/2010 | 1/2009 | Change |
|------------------------------------|------------|------------|--------------|
| Interview | 32 | 35 | -9 % |
| Vulnerability or threat | 63 | 20 | +215 % |
| Malware | 317 | 577 | -45 % |
| Guidance | 130 | 93 | +40 % |
| Preparation of attack | 11 | 10 | +10 % |
| Information break-in | 36 | 28 | +29 % |
| Denial of service attack | 15 | 23 | -35 % |
| Other information security problem | 10 | 23 | -56 % |
| Social Engineering | 43 | 33 | +30 % |
| Total | 657 | 842 | -22 % |



The number of contacts handled by CERT-FI remains approximately at the same level as in the past few years. Almost half of the contacts handled manually are still malware reports, despite of added automation.