

CERT-FI Information Security Review

9 July 2008

CERT-FI Information Security Review

2/2008

The usability and information security of services provided on the Internet has been tested in many ways. Websites have been hacked and irrelevant contents have been added to the websites. Hacked websites have been used for spreading malware or their content has been altered. On many websites, users can be deceived by exploiting cross site scripting vulnerabilities. Attempts have also been made to overload servers in order to prevent them from functioning.

Password phishing and spreading of malware are targeted more and more specifically. Instead of scams spread to all Internet users, malpractices targeting specific organisations or other limited groups are becoming increasingly common. The phenomenon has also been discussed in public more than before.

Instant messaging software has been used to spread malware. Interesting messages that seem to come from other users have lured users to download malicious software files.

SQL injection vulnerabilities enable unauthorised editing of websites

The structure of websites has become increasingly complex and difficult to manage. Behind the front-end visible to users, a website often has a content-related back-end which comprises e.g. databases and content management systems. Users can access the information of such back-end systems through the website.

If the input validation and back-end database are not carefully made and protected, it may be possible to store information on the website or a database used by the website by injecting SQL statements to the back-end database via the web page. SQL is a query language for querying data and managing databases.

Edited websites can be used for, for instance, directing a user to a website from which an at-

tack code exploiting a known vulnerability is downloaded to the browser. This can be done by, for example, adding to the website a line of JavaScript code which downloads malware from another server. The aim of the attack may be to infect the user's computer with malware that collects information or to add the computer as a slave to a botnet. A hacked website can also be used for spreading malware or malware configuration files.

A more simple way to exploit website vulnerabilities is to transfer to the website, for example, political material aiming at affecting public opinion. At the end of June, Lithuania experienced a widespread website defacement campaign.

SQL injection vulnerabilities have been found on several websites. Microsoft and OWASP have published instructions and tools that help preventing SQL injection vulnerabilities in a Windows server environment.

Cross site scripting vulnerabilities still detected

The enthusiasm that rose in the beginning of the year for looking for cross site scripting (XSS) vulnerabilities has continued. CERT-FI has become aware of dozens of Finnish websites which have allowed attackers to inject misleading content to the websites with the help of the website users. In addition to pranks and defacement, XSS vulnerabilities can be used for e.g. deceiving the user and collecting passwords used in the service. CERT-FI has informed service maintainers of the vulnerabilities. Service maintainers have, for the most part, either corrected the vulnerabilities or removed the vulnerable service temporarily from use.

Effects of denial-of-service attacks only minor

At the end of June, a few popular Finnish websites were subjected to denial-of-service attacks. However, the effects of the attacks were fairly minor. The attacks against media company services received, nevertheless, a lot of attention and showed that service maintainers need to be prepared also for overload situations in order to avoid interruptions in the service.

Targeted attempts to spread malware

CERT-FI has been informed of cases in which Finnish companies have been specifically targeted by attempts to spread malware. Malware has been spread as e-mail attachment files sent to specific and carefully selected groups of recipients. A known person or organisation has been forged as the sender of the messages, and the subjects of the messages have been credible and related to the usual operations of the targeted organisations. A typical example of an attachment that includes malware is, for instance, a meeting or conference invitation.

Malware used in carefully targeted attacks have usually been versions that anti-virus software have not recognised at the time when the attack was executed. The aim of the malicious software is to enable remote administration of a user's computer in order to use it to obtain information about the operations of the organisation attacked.

User identification and password phishing carried out through e-mail

Attempts have been made to collect user identifications and passwords by sending e-mail messages requesting verification of user identification or password. Noteworthy in the messages is that they have been sent directed to users in the targeted organisations instead of distributing the messages to randomly selected addresses.

E-mail servers under occasional high loads due to spam

CERT-FI has been informed of cases in which e-mail servers have been occasionally overloaded because of error messages returned by mail servers. An e-mail server can be overloaded when large spam campaigns use forged sender addresses that belong to the same organisation or e-mail service provider. Because a considerable part of addresses of spam recipients are incorrect, large numbers of e-mails and error messages from mail servers are returned to the forged sender address.

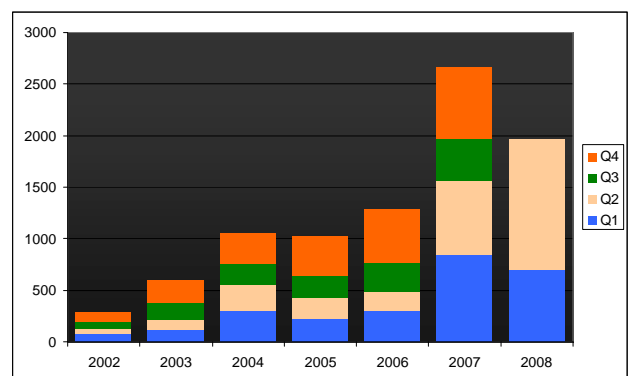
It is difficult to differentiate between an incident described above and a denial-of-service attack aimed at an organisation or a service provider, but on the other hand, such incidents

can be seen as indirect manifestations of denial-of-service attacks. Incoming e-mail traffic to a server cannot be filtered based on IP addresses because the connections are from e-mail servers which may send also real and appropriate messages.

The load can also be directed to an individual e-mail address if it has been forged as the sender of a large distribution of spam. In such cases, the user receives a large number of error messages. Spam can be sent also so that the actual target is the receiver of the error messages because error messages sent by servers may pass spam filters more easily.

Malware links spread through Windows Live Messenger

The Windows Live Messenger instant messaging service has been used to spread links to malware. The links have been accompanied by a Finnish text tempting the receiver to click on the link. Messages are seemingly from the users of the service, but are, in reality, sent by malware. The links are formed so that the target appears to be an image file, but following the link will instead cause a malware to be installed to the workstation. Malware spread in a similar manner was later detected also in Norway.



During the first half of the year, 1,961 handled contacts were entered into the CERT-FI incident control management system.

Software vulnerabilities published in a controlled manner

A conventional way of making software is to create it piece by piece using also parts created earlier. Software consists partly of new, old and freely available freeware or parts bought from other manufacturers.

Large software systems are very complex which makes quality control challenging. Flaws and bugs can be found in practically all software. Vulnerabilities are flaws that may compromise the information security of the software. Last year, approximately 8,000 vulnerabilities were announced. During the first half of 2008, CERT-FI has published 79 notices of vulnerabilities considered significant.

In addition to informing about vulnerabilities, CERT-FI is involved in coordinating the patching of vulnerabilities, which means determining

the vulnerable software or components and connecting the finder of the vulnerability and the manufacturer of the software. CERT-FI's priority is that a vulnerability is made public first after a patch exists for it. Therefore, coordination processes can easily be drawn out.

Vulnerabilities in commonly used OpenSSL and GnuTLS cryptographic software were published in May. The vulnerabilities were detected by Codenomicon Ltd. The SSL and TLS protocols provided by the software are used in securing client/server communications by providing a secure encrypted layer over higher-level protocols, such as HTTP.

The code in question is open source, and used by many products for encrypting data transmission. During the coordination process, also other software manufacturers were contacted, and among others many Linux distributors published patches for the vulnerabilities.

CERT-FI contacts per item	1-3/2008	4-6/2008	Total	1-6/2007
Interview	17	29	46	44
Vulnerability or threat	39	232	271	24
Malware	460	727	1187	1067
Guidance	64	87	151	177
Preparation for attack	32	27	59	3
Data break-in	14	88	102	27
Denial-of-service attack	15	26	41	41
Other information security problem	10	11	21	21
Social engineering	47	36	83	141
Total	698	1263	1961	1545

The number of incidents handled by CERT-FI has grown by a fourth from last year. Especially the numbers of notifications of software and Internet service vulnerabilities, attack preparations and realised attacks on information systems have increased compared to last year.