



3.7.2006



INFORMATION SECURITY SITUATION REPORT 2/2006

The exploitation of vulnerabilities in web browsers detected at the end of the previous quarter continued in the second quarter. Corrective security patches for the Internet Explorer browser program were released in mid-April. The vulnerabilities in web browsers still remained a common means for hijacking computer systems.

CERT-FI was notified of several breaches of servers in Finnish networks which were used for phishing. The cases of phishing have not necessarily increased, but organisations suffering from phishing have started reporting the cases more actively.

The series of phishing attacks addressed to the Finnish customers of Nordea internet banking continued at the beginning of April. No other cases of phishing targeted to Finnish internet banking customers were reported during the second quarter.

Vulnerabilities in software

At the end of the previous quarter, four vulnerabilities were detected in the Internet Explorer browser. One of these vulnerabilities was immediately exploited by placing malicious program code on hundreds of websites. On 11 April 2006 Microsoft released a corrective security patch. During the second quarter Microsoft also fixed many other vulnerabilities in the Internet Explorer browser program and in the Windows operating system and Office programs as well. At the issue of this report, all known Office vulnerabilities have not yet been corrected and they may be further exploited.

During the period under review, several crucial vulnerabilities were detected in many database programs. Corrective security patches were published for several commonly used programs. Vulnerabilities in database software may enable access to systems containing confidential information.

Apple published several security upgrades for the Mac OS X operating system. Among the corrected vulnerabilities, the most important ones enable the execution of the attacker's own program code in a vulnerable computer system. In addition to Windows, there is an active search for vulnerabilities in other operating systems, too, and they are likely to be more extensively exploited.

Several vulnerabilities, even serious ones, were detected in Mozilla software such as Firefox browser software and Thunderbird e-mail software. Corrective security patches for these vulnerabilities were also released.

A vulnerability, which related to the processing of signalling and constituted a serious threat to the security of e-mail systems, was detected in Sendmail e-mail server software. The exploitation of this vulnerability is, however, technically so difficult that the tool of attack has not been published. The components of iCal and vCal dealing with calendar information in the Microsoft Exchange e-mail server software also proved to be vulnerable.

A great number of vulnerabilities relating to the processing of various picture formats were also detected. The older versions of Windows were updated because of the WMF vulnerabilities detected earlier this year.



3.7.2006

CERT-FI

Phishing

CERT-FI received several notifications of breaches of servers in Finnish networks which were used for phishing. The phishing through Finnish servers has been aimed at users of foreign on-line services.

The investigated cases of phishing have had in common the fact that the fake websites have been created by attacking servers with a Horde service installed on them. Horde is a webmail server program providing access to e-mail service by a web browser. Equally, on-line services implemented using the PHP script language have further been popular goals of security attacks. According to the findings of CERT-FI, the problem of several applications operated by web browsers is the lack of regular maintenance and upgrading routines, and therefore they are easy targets for attackers.

At the beginning of the quarter under review, a new phishing campaign was directed to Nordea's Finnish internet banking customers. Spam messages in English were again used in the attempt of phishing. In early May, Nordea's Swedish customers were also targeted in a phishing campaign. This attack used spam messages written in poor Swedish. The authors of these two attacks are not necessarily the same, as some difference in the technique could be observed.

Botnet malware

During the period under review, malware using other than the IRC protocol was detected more frequently than previously, such as malware using P2P based communication. The collapse of the network in connection with the shutdown of command servers can be prevented by means of the peer-to-peer protocol. Malware using a modified IRC protocol also appeared frequently.

Malware is further used in the pursuit of financial benefit. The collection of data has become more professional and the amount of data has increased. In order to remain undiscovered, the malware is not necessarily in continuous connection with its command server, but is sending data in bursts, when the transmission may escape the attention of the user.

Targeted attacks

At the end of May a vulnerability in the Microsoft Word program was largely in the headlines - and a corrective security patch was not released before 13 June 2006. The vulnerability was exploited in attacks against single enterprises and associations. However, CERT-FI has not been reported any such cases aimed at Finnish organisations.

Future prospects

Several CERT players have reported on a decrease in the total of cases reported, which may imply a proportional increase in targeted attacks. Defence against attacks and their detection is ever more difficult. The attacks are planned to bypass the most usual protection mechanisms in organisations, such as antivirus software and a firewall. Preliminary information on the selected goal helps the attacker create more convincing e-mail messages for the execution of targeted attacks.

With the evolution of methods of identification, the attacks are, instead of user ID harvesting, aimed at the content of the user connection. Malware installing itself as proxies and attempting to harvest banking identifiers and other confidential information transmitted during the connection is an example of this.