



3.4.2006



INFORMATION SECURITY SITUATION REPORT 1/2006

At the end of the first quarter of 2006, the number of threats was increased by vulnerabilities detected in web browsers. The vulnerabilities were effectively exploited for instance in installing botnet malware in home users' computers. A modern web browser program is a very complicated and large entity, which with its huge extent of program code is particularly exposed to programming errors. The browser, being the most commonly used individual user interface for applications, is a goal for active search for vulnerabilities and development of malware.

The series of phishing attacks directed to Nordea's internet banking customers, which started last year, continued in January, but after that no further similar attempts were reported. Globally, phishing is a continuously growing phenomenon.

During the quarter, three major security upgrades for Apple's Mac OS X operating system were published. First examples of malware exploiting vulnerabilities in the Apple systems were reported. The maintenance of information security in the Mac OS X operating system requires continuous updating so as other systems.

Software vulnerabilities

At the turn of the year, malware authors were busy with an exploitable behaviour in the processing of the Windows Metafile (WMF) picture format. The first malware exploiting this vulnerability was launched before the software company had been able to release a corrective patch. This vulnerability affected all versions of the Windows operating system. New malware exploiting the WMF vulnerability is further developed, even though a corrective patch has been available since the beginning of the year. It is probable that there is a great number of non-upgraded computer systems connected to the internet through which this vulnerability can be exploited.

Web browser software is the most common user interface for internet services. The same browser software is also frequently used as an interface for the internal services of an organisation. A special risk lies behind the vulnerabilities in the browser software enabling the execution of the attacker's own program code. Typically the exploitation of the vulnerability only requires a visit to a website that has been maliciously created by a vulnerable browser program. At the end of March, four vulnerabilities were detected in the Internet Explorer browser. One of these was immediately exploited by placing malicious program codes on hundreds of websites. At the issue of this report, a corrective patch for these vulnerabilities has not yet been released.

Apple published three important security upgrades for the Mac OS X operating system. Easily exploitable vulnerabilities were detected in Apple's Safari browser software and e-mail software Mail. It is obvious that from the viewpoint of malware authors and researchers of vulnerabilities in Apple systems are becoming more interesting than before.

Phishing

Phishing means that the users' electronic identity (usernames, personal data) is acquired by the attacker. Typically, the attacks are performed by appealing to the credulity or helpfulness of the user of a network service. The hijacking of another party's electronic identity is made for financial benefit.



3.4.2006

CERT-FI

The phishing addressed to Nordea's internet banking customers continued in January. This series of frauds is up to now the largest one directed to Finnish internet services dealing with financial data. Internationally, phishing is spreading vigorously. The international Anti-Phishing Working Group (APWG) reported in its latest statistics of January a considerable increase, over 30%, in the number of fraudulent websites. In January the APWG was reported 9715 different falsified websites.

Not only banks are targets for phishing. All kind of electronic identities for different systems are of interest for the attackers. In the United States, phishing attacks particularly to the tax authorities' on-line services and other public services have distinctly increased.

According to the APWG, the interception of a text written by a computer keyboard and its further distribution by means of malware called keylogger is expanding as a method of phishing.

Botnet malware

The use of computer networks infected by malware can already be regarded as a professional activity. A major part of infected computers are used for instance for installing advertising software on an infected computer, for pay-per-click frauds, phishing or blackmailing by denial-of-service attacks. Stealing of data is becoming an important purpose of use. The design of malware has also become more complicated than before. In order to make the analysing more difficult, the malware authors are increasingly using an encrypted command channel for the commanding of a malware network. Modified and protected server programs are used in the maintenance of a botnet. The code structure of the malware itself is also frequently protected by various encryption methods and so called logic bombs.

Nowadays the attacker wants to keep a computer infected by malware under his/her control for a longer time. For this aim, the malware searches for and installs a rootkit program on the infected computer, enabling the attacker to hide the malware and traces of it in the system. By means of the rootkit program the attacker can hide processes from security software and the user. It also allows the use of a network connection without being noticed by the user or the firewall possibly installed on the computer.

Targeted attacks

The internet domain name system (DNS) provides a worldwide decentralised database of addresses for resolution between domain names and addresses. Too openly configured name servers connected to the system may be used for malicious traffic aiming at denial-of-service. An inquiry with a false source address and addressed to a record formatted in a special way produces a return message that is by far bigger than the inquiry. By sending a request to a great number of name servers allowing recursive inquiries, the falsified address receives in reply a large amount of unwanted messaging. System administrators should take care of that the name servers do not answer recursive inquiries coming from outside their own service area. This matter was first reported in a CERT/CC report in 2000.

On-line services implemented using the PHP script language are popular targets of security breaches. The reason for this is that the attack tools are easy to use and the network capacity of the targeted web servers is relatively high. The vulnerabilities detected have not typically resulted from the insecurity of the PHP language itself. The problems have usually originated from a programming error in PHP applications or from software libraries used by PHP-based applications. At the beginning of the year, several break-ins were made to Finnish PHPbb chat platforms by disguising the front page with religious propaganda. The series of breaches is related to the



3.4.2006

CERT-FI

caricature case in Denmark. There is nothing to imply that the attacks should particularly have been aimed at Finnish platforms. In connection with the breaches thousands of PHPbb forums were abused all over the world.

The most usual method of attacking Unix type operating systems is an attempt to break the password of the administrator's username by using a SSH protected terminal connection and an extensive list of the most common passwords. The attempts of break-in may often go on for a long time, if the administrator of the targeted information system is not regularly monitoring unusual attempts of login in the log files of the system.

Faults and malfunctions

During the first quarter of the year, there were some significant events of malfunction in the IP backbone network which affected the function of communications services over these networks. In addition, at the beginning of February there was one serious case of malfunction in the e-mail service which affected a great number of Finnish customers. In the centralisation of services, special attention must be paid to the back-up of accessibility, for instance by decentralising crucial services.

Future prospects

The attention of researchers of vulnerabilities and authors of malware will be focused on browser programs. A special challenge are cases when the software company concerned is not first confidentially notified of a vulnerability so that they could prepare a corrective security patch. Selling of information on vulnerabilities and even methods for the exploitation of vulnerabilities seems to become more and more general.

Efficient hiding of malware for instance by means of rootkit techniques is evidently gaining strength. The properties of rootkit software are further developed.