

2.10.2006



SITUATION REPORT 3/2006

During the third quarter of 2006, CERT-FI reacted to information security events by releasing 36 news articles and targeted notices on top of that. The number of incidents was rather normal, but a few new occurrences were found.

CERT-FI learned of a case where data of tens of Finnish Internet users' was exposed to third parties. The data had been obtained with the help of Haxdoor spyware which infected the users' workstations. The case that was discovered now involved tens or hundreds of thousands of victims at global level.

Since July, many parties have released numerous vulnerabilities in workstation applications without any fix for them at the time of release. Several vulnerabilities were exploited for the purpose of spreading malicious software. Websites that spread malicious software were notably often found in the networks of same service providers.

No significant incidents threatening information security were reported during the ASEM summit held in Helsinki in September.

Internet scams

An attempt was made to steal data from Nordea Bank's Swedish customers by phishing scam websites resembling those of Nordea's Internet Bank. No Finnish Internet bank customers were targeted by the scam. However, there is a continuous attempt to spread spam containing links to scam sites that also concern Finnish internet users. For example, many Finns are customers of the eBay and PayPal services.

User information can also be stolen by spying the user's network traffic to genuine service sites. The Haxdoor spyware steals data the user has entered on website forms, such as usernames and credit card information, and forwards them to a collector server maintained by the attacker. Reports from around the world tell of nearly a hundred thousand computer break-ins by Haxdoor. CERT-FI has received reports of a few cases where user data of Finnish services had been uncovered over the spring and summer. Nothing points to the fact that the scam would have been targeted at specifically Finnish users or electronic services. The cases have been reported to service providers and the Data Protection Ombudsman.

Haxdoor, as well as Torpig and BZub, which have the same behaviour pattern, is an example of how a data system break-in aims at collecting data, which the attacker plans to exploit economically. It is difficult to discover a Haxdoor infection that has already occurred, but commonly-used and updated anti-virus software prevent infections.

Workstation vulnerabilities

H.D. Moore, known for his Metasploit project, wrote in his blog that he would publish one previously-unknown browser bug in need of fix each day during the month of July as part of "The Month of Browser Bugs" theme. In addition to Moore, other parties also released vulnerabilities of which some are still unfixed.

Several vulnerabilities affecting the security of workstation users were discovered in both the Windows operating system and Microsoft Office software. Some of them enabled the program code selected by the attacker to be run in the user's computer. In order to fix them, the vendor has

2.10.2006

CERT-FI

released system patching updates. According to CERT-FI's information, some of the vulnerabilities have been actively exploited.

At the end of the quarter, two vulnerabilities were discovered in the Windows operating system. In order to exploit them, it is enough that users of the Internet Explorer browser are attracted to the website used for an attack. A fix to the other one of the vulnerabilities was released exceptionally fast. But, it is still possible to exploit it against unupdated workstations. So far, there is no fix to the other one and it is exploited to spread malicious software. It is possible to protect against it by changing Windows settings.

A vulnerability discovered in the McAfee Security Center software can be exploited in a certain manner via overwritten websites. Flaws in information security solutions can prevent the detection of malicious software or break-in attempts.

Vulnerabilities were discovered in the device drivers of the wireless network cards (WLAN) used in laptops. Device vulnerabilities enable that the attacker's own program code can be run in the computer. Attacks are only possible in the workstation's WLAN coverage area, which limits the exploitation of vulnerabilities. Fixed device drivers have been released for vulnerable systems.

Server and network device vulnerabilities

During the quarter, vulnerabilities also affecting Internet service providers and network providers were discovered. A flaw discovered in the Juniper routers of the JunOS operating system caused a denial-of-service attack which originated from a flaw in the packet-handling of IPv6. Default settings in some versions of the Cisco's IOS operating system allow the router settings to be changed by the main user. A denial-of-service vulnerability was discovered in the Cisco Intrusion Prevention System. Two denial-of-service vulnerabilities were discovered in the most commonly used DNS (Domain Name System) server on the Internet, BIND (Berkeley Internet Name Domain). Software update patches for all these vulnerabilities exist. Patches for a large number of vulnerabilities in the Oracle database were issued.

There are security flaws in many software systems meant for providing content for websites and publishing websites. Some of them may result from insecure default settings. The attacker can exploit the vulnerabilities by for example trying to change the content of the website. It is also possible that the attacker's program code is run on the web server. Open source content management systems such as Joomla and Mambo have become more common among private persons who use them as website management tools.

Targeted attacks

Reports from around the world told about exploitation of a vulnerability in the Microsoft PowerPoint presentation graphics package. CERT-FI has received reports of planned attacks against Finnish companies and a break-in targeted at a school.

Future prospects

Hostile operations are concentrated on obtaining user information. The threshold to create malicious software is lower and requires less experience and programming skills than before. Software and their distribution services can be bought on the Internet at a reasonable low price.



2.10.2006

CERT-FI

Some network operators provide connections and domain name registration for the purpose of spreading and selling malicious software or scam websites, and do not respond to misuse reports. These sorts of operators are found in the United States, Russia and China.

Blacklists containing mail servers that spread spam may complicate e-mail delivery. Server maintainers use lists to deny receiving messages from servers listed as spammers. E-mail could not necessarily have been delivered because servers have ended up on being listed without cause. FICORA lists Finnish mail servers on a list containing reliable e-mail servers. Server maintainers can allow the distribution of messages from a whitelisted server even if it had been previously blacklisted. Also, corresponding international projects have been undertaken.

Domain names resembling those registered for international mass events are often registered for the purpose of making fun, mischief, propaganda or scam. Or, parties interested in the subject make their own websites to supplement the official websites. It is impossible to register all such domain names that can be used for various purposes, side by side with the real domain name.