



5.1.2007



INFORMATION SECURITY REVIEW 2006

In 2006, security incidents still aimed at gaining economic benefit by acquiring and exploiting personal and payment data of people using the electronic services of computers and information networks.

The new phenomenon of distributing spyware to hacked computers became common. The software is used for the purpose of spying the information computer users have entered on websites and forwarding it to third parties. This is to say that user information is collected during the connection while using trusted network services and not by creating scam websites that imitate them. The software can, for example, hijack personal data, user identification, passwords and credit card numbers. The activities were large-scale and systematic, but CERT-FI received word of only very few cases where the information of Finnish users of electronic services had fallen into wrong hands.

A key malware used for spying user information is Haxdoor. CERT-FI participated in analysing how the Haxdoor spyware is built and released a program that removes the malware infection from the computer.

No specific security incidents were disclosed during Finland's EU leadership or international meetings arranged by Finland.

In particular, the most frequently-occurring vulnerabilities in 2006 were related to the most commonly-used web browsers, the Windows operating system and MS Office software. In addition to them, vulnerabilities were found in other operating systems and software.

The significance of economic threats caused by the distribution and exploitation of malware is great. Malware is distributed and used systematically for the purpose of gaining economic advantage. International cooperation between various authorities, companies and information security players is often required in order that activities are disclosed and the logic or authors are found.

From scamsites to spying telecommunications

Over the year, CERT-FI received numerous reports of websites imitating the look of trusted electronic services. The purpose of these websites was to collect user information (phishing). The most common targets of phishing attacks were auction sites (e.g. eBay), online payment services (e.g. PayPal) and bank websites. In Finland, fake websites of Nordea Bank services were disclosed. But, fake websites of widely-used international services also have many Finnish users.

In addition to fake phishing sites of trusted online services, attempts were made to spy user identification, passwords, credit card numbers and other confidential information. This was done by spying the information users had entered on trusted online service sites. In order to hijack information, the aim was to transmit spyware to the user com-



5.1.2007

CERT-FI

puter whose purpose was to monitor web connections. The spyware then would hijack information and forward them to a third party who uses the information for false purposes.

The difference between scam websites and spyware is significant for example because it is usually possible to identify phishing sites during the online connection, whereas pharming involves intercepting information by installing a spy program on the computer without the user knowing about it. The programs use the so-called rootkit technologies in order to hide from users and anti-virus software. If the infection occurs before the anti-virus software is updated to identify the malicious software, it may be very difficult to discover it later. Protecting the web connection with a SLL connection does not prevent information interception, because the program hijacks the information before they are even encrypted to be forwarded via network connection.

The first incidents of a spyware called Haxdoor reached CERT-FI in February. Haxdoor is a program that hides from the user and anti-virus software once it has infected the computer. It then collects the information the user has entered on the website form and forwards it via the network to a collector server. A key malware used for collecting user information is Haxdoor. CERT-FI participated in analysing how the Haxdoor program is built and developed a program that removes the Haxdoor infection from the computer. The program was published in October.

In July, CERT-FI received word from its international cooperation network that information of tens of Finnish users of electronic services fell into the hands of third parties. However, nothing points to the fact that the scam would have been targeted at specifically Finland, but the majority of the hijacked information concerned other than Finnish users and services.

CERT-FI has discovered that websites distributing malware are notably often found in the networks of same internet service providers. It is very important to enhance international cooperation in order to prevent malicious attacks.

Exploitation of software vulnerabilities

Vulnerabilities caused by software errors may help infect the computer with a malware. Software vulnerabilities are systematically sought and automatic testing methods are also being developed to ease the search. A technology used for searching for vulnerabilities is fuzzing: the capacity of the software to handle an unexpected feed is tested by automatically going through a large amount of crashed use cases. This can, for example, be done by intentionally manipulating the file contents used by the software. CERT-FI has actively striven to seek closer cooperation with vulnerability researchers. The objective is a controlled chain from discovering faults to finding a remedy for them and releasing information in a responsible manner.

The single most threatening software vulnerability incident was a software error found in the handling of Windows metafile files and affecting all versions of the Windows operating system. This was widely exploited at the beginning of the year before a software update patch was released and the systems were updated. It is difficult to protect from a vulnerability whereas it is easy to exploit it via websites, e-mail, instant messengers and peer-to-peer networks. The impact of the vulnerability was less than feared. Cooperation be-



5.1.2007

CERT-FI

tween CERT-FI players, telecom operators, anti-virus companies and software manufacturer Microsoft played a decisive role in the combat against the ill-effects of the vulnerability.

Through the year, numerous other vulnerabilities were disclosed for widely-used software such as the Windows operating system, Microsoft Office software and web browsers. Some of these vulnerabilities were also actively exploited to spread malware.

During the year, vulnerabilities were disclosed in devices and applications critical to the operation of the Internet, such as the operating systems of the router manufacturers Cisco and Juniper, Sendmail e-mail server software and BIND name server software. CERT-FI cooperated with device and software manufacturers and Internet operators in order to coordinate information concerning vulnerabilities. Vulnerabilities were little exploited before the software was patched.

Vulnerability releases politicised

It appears that some vulnerability researchers are changing their vulnerability release policy into a more radical direction so that vulnerabilities are released even before the software manufacturer has time to patch it. The objective is to press software manufacturers to patch the errors in their software faster than currently.

In July, H. D. Moore published in his blog one previously-unknown browser bug each day as part of "The Month of Browser Bugs".

In November he continued along the same lines: "The Month of Kernel Bugs". A new operating system vulnerability was released on each day of the month. Among the targets were not only Windows, but also Linux, MacOS X, FreeBSD, Solaris and various wireless network device software and device drivers.

Information security researcher Cekar Cerrudo intended to release vulnerabilities in the database software manufacturer Oracle and will use the title "The Week of Oracle Database Bugs" in order to prove that Oracle's software is insecure and to criticize the company's slow reactions in patching the software vulnerabilities, but later withdrew his intentions.

Targeted attacks

A malware distribution may be directed to a restricted group of users, e.g. the employees at a specific company or products of the company. The objective of the attacks can be to find out how the organisation can function under exceptional circumstances or collect internal information on the company, but also personal motives.

A few attacks against Finnish companies or services were reported to CERT-FI. Generally speaking, there has not been much growth, although some of them are particularly difficult to block.

Typically, the attack method used was a malware disguised as a true e-mail attachment file planned for the attack and unidentified by anti-virus software. The software exploited



5.1.2007

CERT-FI

the vulnerability unknown to software manufacturers. The attacks were also targeted at public services, such as websites and e-mail servers, maintained by organisations.

Faults and interference

Interruptions in mobile networks in sparsely populated areas were the most critical among telecommunications connection interference. Some of the interference are due to interruptions in electricity distribution and some are due to telecommunications connection problems caused by device fault or configuration errors. The faults have been patched relatively fast and the interruptions were usually short.

At the end of the year, CERT-FI received word about strong growth of spam and malware spread via e-mail.

Future prospects

Security incidents against computer users keep occurring. The focus of data system break-ins remains in public or corporate servers instead of in the computers of ordinary users. Attempts are made to send malware to home user computers by exploiting vulnerabilities in software and operating systems. E-mail, skilfully-edited e-mail attachment files or websites exploiting browser vulnerabilities can still be used as distribution channels. Spam senders seek to develop new methods to penetrate spam filters and formulate their messages so that they pass the filter software most-commonly found on the servers of telecom operators and companies as well as possible, or so that messages intend to harm the filter functions.

Malware and command servers and connections designed to exploit malware develop and it will become increasingly difficult to disclose botnet networks and software. Malware are increasingly more efficient in hiding from the operating system and anti-virus software.

A significant number of operating system upgrades will be made in the near future as the new version of the Windows operating system "Vista" will be released. The transfer to a new system can increase the risk of new vulnerabilities and exploitation.



5.1.2007

CERT-FI

Terminology

Malicious software, malware= a common definition for "malicious" software aimed at hostile purposes. Malware can e.g. collect information, distribute spam, scan information networks, attack servers or destroy user information.

Phishing ="Fishing" user information by tempting users to enter it on an online service looking trusted, but in fact controlled by a spy. An invitation to phishing sites imitating trusted services may be received via links sent as e-mails. Servers themselves are often found in hacked home computers where the hacker has remotely installed a server program.

Spyware = malware installed in the user software which collects user information by monitoring the user's web browsing or telecommunications. For example, the software hijacks the information entered on an online form and transfers it via network connection to a collector server controlled by a spy.

Rootkit = a common definition for the technology and software tools used for the purpose of gaining maximum possible number of user rights to a computer. They also make it possible to hide from users, operating system and other software - such as anti-virus software - and disable firewall software protection.

Haxdoor = Spyware that uses rootkit technology in order to hide from users and anti-virus software.

Denial-of-service attack = An attempt to complicate or block the server or service functions by overloading it. The attacker may have control over a large number of hacked computers that were involved in overloading the target by for example generating a large quantity of network traffic or connection attempts to the server.

Botnet = A network of hacked computers and commander servers. Hacked computers are remotely-controlled and used for sending e-mail or denial-of-service attacks without the use even knowing of it.