



30.1.2006



ANNUAL INFORMATION SECURITY REPORT 2005

In 2005 the goal of security violations was more and more often financial benefit and they were targeted at the weakest link in the information security, the human being using a computer. A form of hoaxing called *phishing* not previously experienced in Finnish or Swedish speaking countries landed in Finland last October. Through phishing financially exploitable information, such as personal data, user ID's and passwords, or credit card numbers, are acquired for illegal purposes. It is typical of phishing that the hoaxer tries to make the user to deliver the data voluntarily.

Various kinds of malicious software continued to be used in attacks against unprotected information systems connected to the internet. Present-day malware is remote-controlled; it can be executed and updated at distance. CERT-FI has learned that there are hundreds or even thousands of Finnish computers that are victims of remote-controlled *bot malware*. The data in the compromised computers and their internet connection are exploited in malicious activities as parts of bot a.k.a. robot networks. Worldwide millions of victims have been reported.

As to server systems, the vulnerabilities most commonly exploited appeared in PHP technology and implementations. PHP is a programming language commonly used in creating www services. CERT-FI also continues to receive reports of automated password harvesting, and cases where passwords have been collected by means of Trojans installed to servers. At the end of the year unprotected domain name servers of several Finnish organisations were exploited by a worldwide denial-of-service attack.

Particularly at the end of the year it seemed that information security had become part of the regular flow of news in the mass media and the general public also took an interest in this subject. With the spreading of broadband access, the internet is no longer a privilege of technically fluent users. Safe use of communications networks by citizens can best be promoted by efficient dissemination of knowledge.

Exploitation of vulnerabilities

The most extensively exploited vulnerability during the past year proved to be that of *Universal Plug and Play (uPNP)*, a subsystem of the Windows operating system. Worms infected thousands of Finnish home users' computers and their spreading provoked various levels of disruption for numerous business networks.

Another extensively exploited vulnerability in Windows environment was based on a design error detected in the *Windows Metafile (WMF)* picture format. The first malware exploiting the vulnerability had been launched even before the software producer had been able to release a corrective security patch. The vulnerability exposed the users of computers to malware infections, for instance through www, e-mail, instant messaging and peer-to-peer networks. The problem was extensive and shall not be understated, as all versions of Windows were concerned. Fortunately the vulnerability has so far been exploited less than predicted, even though extensively.

Numerous information security problems were detected in the most commonly used client software, such as web browsers, instant messaging software and VoIP software, as well as in multimedia software. Dozens of security updates were published for browser software alone. The



30.1.2006

CERT-FI

weaknesses of web browsers have already been exploited for several years, as they provide an attack vector that passes through network filters and bypasses other information security controls. For the same reason instant messaging software and applications based on peer-to-peer networks provide a large area to be exploited by those who prepare malware attacks.

During the year, CERT-FI published altogether 12 advisories regarding vulnerabilities detected in the products of the most important anti-virus houses. Most of the vulnerabilities concerned the handling of compressed files. CERT-FI has not heard that the vulnerabilities had been used for bypassing the protections of computers. The exploitation of vulnerabilities was probably hindered by the fact that anti-virus software is usually updated automatically requiring no user intervention.

With the increase in web chats, bulletin boards and *blogs* the information security violations aimed at them also become more general. Vulnerabilities detected in systems using *PHP* were largely exploited. At the beginning of 2005, CERT-FI published warnings concerning the popular phpBB software and monitored attempts to exploit *XML-RPC* vulnerabilities.

In November CERT-FI published an advisory of several vulnerabilities that were detected in implementations of *ISAKMP* protocol suite. Research of the vulnerabilities and the publication of corrections had been coordinated since the beginning of the year confidentially in cooperation between dozens of software producers, the OUSPG group at the University of Oulu, who had developed a testing system for the investigation of vulnerabilities, CERT-FI and the British NISCC. The list of vulnerable software and hardware producers has been updated several times after the initial release of the advisory, as the producers have published new security fixes. CERT-FI has not been informed of cases where the vulnerabilities published would have been successfully exploited.

In January 2005 the vulnerabilities found in the software used in the backbone routers of IP networks could be corrected and the patches installed in time before any attack exploiting the defect could be started. The confidential cooperation between software producers, main security actors and telecommunications operators was found to be of great importance and gave good results.

Evolution of malware

The focus of the production of malware has little by little changed over from the traditional virus and worm malware to remotely controlled bots with a variety of properties. Bot malware is almost always written on Windows platforms, most probably due to its large market share. Malware managed by a botnet is frequently detected behind phishing, diffusion of spam, spyware and denial-of-service attacks.

An example of the scope of this phenomenon is the arrest of three persons in the Netherlands last October. The persons concerned occupied a network of, modestly estimated, 1.5 million information systems infected by *toxbot* malware. The exploitation of malware is professional with symptoms of organised crime. The activity involves persons specialised in their task at different levels: vulnerability researchers, spam authors, botnet administrators and intermediaries of the financial benefit obtained from the activity.

There is evidence that the standard features of malware more and more often include the capability of hiding from the users of computers and anti-virus software. During the year, widely spread malware was detected with several new versions appearing daily. The purpose of these versions is to keep the antivirus-software protecting the victims' computers always a step behind. Other methods of hiding are for instance the disabling of security software and the hiding of the operation of a program by so called *rootkit* techniques.



30.1.2006

CERT-FI

Malware written for mobile phones did not cause significant security problems in 2005. Meanwhile, a bigger problem was the capability of multichannel diffusion of malware through short range *bluetooth* radio links and *multimedia messages*. The risk of epidemic has so far been curbed by the fact that the installation of all known malware requires the user to specifically accept the installation. Spreading through bluetooth is most effective in mass events, as could be seen during the games for World Championship in Athletics in Helsinki last August. About twenty cases of infection were then reported to CERT-FI.

Phishing landed in Finland

The spreading of phishing from English speaking countries to smaller language areas was already predicted in CERT-FI's quarterly review 3/2005, as it had already reached the German speaking area. During the last quarter of 2005 this phenomenon also reached the Nordic countries.

The first phishing attack on customers of Finnish internet bank was started at the end of October. Further attacks of this type were made three times during November and December. In the first attacks spam messages in English were used, but later on the language was changed into poorly written Finnish. The number of messages per a single phishing campaign was approximately 500.000 and the websites used for collecting user identifications has been spread to cracked www servers all over the world. Up to now, Finnish banks and companies processing data of payment instruments in their internet services have not fallen victims to similar hoaxing to a greater extent.

Targeted attacks

Cases of information system break-in aimed at Finnish organisations and reported to CERT-FI did not increase last year. In data acquisition tailored malware was used more often than in the previous years and it was sent to the users in the target organisation as attachments to e-mail. An alternative method of attacking a workstation in the internal network of a single organisation was to tempt the user into a certain website, through which malware was installed by exploiting vulnerabilities in the workstation.

As in the previous years, numerous cases of break-ins were globally reported, where the attacker got hold of a great number of Finnish or foreign credit card numbers, usernames or other personal identifiers. The data had been obtained by hoaxing from the users themselves, by stealing by means of spyware installed on a computer or by breaking into the database of a commercial service or a payment intermediary.

The denial-of service attacks on Finnish organisations which have been brought to the notice of CERT-FI have been mainly aimed at www and IRC services. Globally, the number of attacks and the damage caused has been fairly modest.

At the end of the year, there were signs of a worldwide denial-of-service attack, which exploited the openness of DNS servers used in resolving hostnames and IP addresses, and the insufficient protection of broadband networks against the use of spoofed source addresses. Even though the attacks were not directly aimed at Finland, several Finnish domain name servers were used for boosting the attack. The attack exploited a vulnerability in the DNS system which was first reported five years ago, but still existed. CERT-FI and telecommunications operators forwarded notifications and instructions for protection to the administrators of name servers.

30.1.2006



Faults and malfunctions

The most significant defects in communications networks used for speech transmission were related to breaks in unsecured backbone network connections and long-lasting regional power failures due to difficult weather conditions.

The incidents in IP based high capacity backbone networks caused particularly in January and February breakdowns in connections extending to large geographic areas. They mainly affected data communications. The malfunctions were generally due to incorrect network configurations introduced in connection with the maintenance work, software errors or their combined effect. Considerable malfunctions due to hardware failures were also reported.

Future prospects

Security violations directed to the user instead of the computer continue during the current year. The letters for hoaxing are made increasingly convincing. Successful hoaxing has not so far required very advanced techniques. The acceleration of international payment service and increase in electronic billing also encourages to malpractices that are technically feasible. Not only banking services but all on-line services dealing with online banking or credit card information, or other financially exploitable data are exposed to hoaxing.

Systematic attacks will be mainly implemented through information systems outside the Finnish borders. The investigation of the cases is thus made more difficult. CERT-FI continues to develop its already extensive international cooperation network.

The heavy increase in broadband connections highlights the importance of automated information security processes in network management. Service providers should advise customers on practical measures of protection, as the information security threats are particularly focused on end-users.

In future, new operating systems are safer owing to tighter access control and other ready-made information security properties. For this reason the malware is likely to be focused besides hoaxing, on exploiting software vulnerabilities bypassing communications security measures. Such applications may be, besides browsers and instant messaging, file sharing software and software exploiting peer-to-peer technology. It is to be recommended that the functioning of bot malware be hindered by restricting the outgoing communications from information systems. Simultaneously, the ability to detect malware would improve.

At the end of the year FICORA issued Regulation 13/2005 on information security and functionality of internet connections. The regulation and a recommendation based on it clarify internet service providers' rights and obligations concerning the information security of their services. Best practices of network security have been incorporated in the regulation. Special attention has been paid to the security matters in connection with the delivery of a subscriber connection. This regulation is complementary to the previously issued Regulation 11/2004 on information security and functionality of e-mail services. The information security in Finnish communications services will be maintained at international top-level by regulation.