

27.12.2007

CERT-FI

CERT-FI ANNUAL REPORT 2007

Identity thieves are interested in the user information of electronic services. A great amount of user credentials has been found when malware and malpractice have been investigated. However, CERT-FI has not learned of alarming amounts of Finnish user information having been found.

Services provided in the internet are in many ways vulnerable to malpractice. The service itself may be easily incapacitated by directing enough network traffic to the server. Vulnerable servers can be used for the purpose of spreading malware, maintaining phishing websites or spying user information that has been saved on the server.

The number of malware reports in Finnish networks has somewhat declined although broadband subscription volumes continue to increase. CERT-FI and Finnish service providers have been quick to react to the perceived problems.

Denial-of-service attacks under focus

A denial-of-service attack was targeted at internet root name servers in February. The attack was initiated by a botnet network consisting of hijacked computers and lasted for about a day. The attack volume was significant, but the effects in practice remained insignificant as the majority of logical root servers remained operational. For Finnish users, the attack showed as occasional, slower internet speeds. Some of the servers under attack are also responsible for the name service of national top-level domains, and their service was also affected. The attacks did not affect the functionality of fi-domain names, however.

Around the same time, CERT-FI became informed of two large denial-of-service attacks which used name servers with too open configuration to reinforce the attack traffic. Some Finnish name servers were used in the attack as well. Maintainers of the servers were contacted and they were advised to change their server settings so that it would no longer be possible to exploit the servers for attack purposes.

As the so-called statue dispute broke in Tallinn in late April, the network services of the Estonian government were paralysed by denial-of-service attacks of progressively growing traffic volume. In addition, attacks were made at least against payment transfer systems and news services. The attacks were active for several weeks.

Once the Estonian attacks ceased, CERT-FI was reported about attacks against Finnish servers, too. During the attack against the web server of the Finnish Broadcasting Company, their web sites were slow or at times inaccessible. The attack directed connect requests of a peer-to-peer file sharing program to burden the server. According to CERT-FI's knowledge, the attack had no connection to the Estonian events. Smaller attacks were made against other web servers and e-mail servers, too. A denial-of-service attack was made against the FICORA and CERT-FI websites in September. Also, the large amount of spam messages has occasionally slowed down message delivery.

27.12.2007

CERT-FI

The attacks received a lot of publicity and led to partly false conclusions about the reasons for service interruptions as the functionality of services was monitored more closely than usual. Majority of the incidents reported to CERT-FI did not prove to be denial-of-service attacks. The attacks initiated active discussion on the reliability of electronic services in the event of an attack.

User information is collected in many ways

Malware and phishing site authors are interested in the information of the users of the services. In addition to collecting information via fraudulent web sites, malware monitoring browser connections can send information entered on web forms to collector servers where they will later be picked from for the purpose of making use of them. Over the year, CERT-FI has received reports about the information on Finnish users exposed to third parties in this way. The share of Finns over all found information has so far been low, only a couple of tens of participants.

In addition to collecting usernames, passwords and other identification information, malware can also make changes to the information the user has entered on the web browser and seen during the connection. The program can, for example, transfer money from the user's account to a predetermined account during an online banking session without the user realising it. So far, CERT-FI has not learned of such malware that would hijack sessions functioning in Finnish services. A sample analysed by CERT-FI has, however, been traced back to information relating to Finland. For example, a malware hijacking an online banking session transfers money unnoticed from the bank account of the user of the infected computer. After this, attempts are made to destroy the traces of cash flow by means of dummies i.e. straw men familiar from white-collar crime.

In October, there was a file containing about 80,000 usernames and passwords or password hashes of Finnish internet network service users spreading in websites and peer-to-peer-networks. The passwords have been obtained by exploiting vulnerabilities in self-made or third party software components.

The incident revealed flaws in the information security of many network services. The passwords of some services had been saved on the server in plaintext or were weakly encrypted. In addition to big companies, also private hobbyists provide social network services in the internet. However, their knowledge of the information security maintenance of the system or software is not always sufficient. Vulnerabilities are constantly found in software used in the services. There were also flaws in user behaviour. For example, using the same password for different services leads to that the exposure of the password of one service also compromises other services where the same password has been used. By combining the information from various services, the user's protection of privacy may be endangered and they can be used for the purpose of pretending to be another person in different services.

Botnets still serve as basic tools for malpractice

The botnets, networks of hacked computers, are still used for many sort of malpractice. They can, for example, be used for sending spam or implementing denial-of-service attacks.

27.12.2007

CERT-FI

The Storm Worm is a malware first discovered in January 2007 and is spread via e-mail attachments and websites. During the summer and autumn, a lot of spam went around containing a link to a website spreading the Storm Worm malware. Once the program infects the computer, it also installs a rootkit i.e. aims at hiding itself from the user and antivirus software. Therefore, it is difficult to detect and remove it from the computer. Currently, the Storm Worm is one of the most widespread malware in the world.

Computers infected by the Storm Worm are part of the very large Storm Worm botnet. The network of hijacked computers is commanded efficiently by a decentralized mechanism similar to peer-to-peer networks without centralized command server. This makes it difficult to detect the functions and structure of the network. A botnet can also launch a denial-of-service attack as a counter-measure in order to protect itself from the investigation of its operations. The significance of the Storm Worm malware for Finnish users was not quite clear at the beginning of the year. Neither has CERT-FI learned of any significant numbers of infected computers in Finnish networks after that. However, the botnet may have been used for attacks against Finnish targets since that.

Software vulnerabilities facilitate malpractice

The vulnerability disclosure campaigns appearing at the shift of last year faded and no more were seen. However, a lot of vulnerabilities were still found in software. Vulnerabilities related to the components of operating systems, office applications and browser software concern a great majority of work station users. They are most often exploited for the purpose of spreading malware and hijacking computers as zombies for botnets.

As far as server vulnerabilities are concerned, attention should be paid in particular to PHP programming language and vulnerabilities in PHP-based content management systems. The vulnerabilities may allow unauthorized editing of website content. Hacked web servers are widely used for e.g. phishing websites and hosting malware. Vulnerabilities were also found in the software of routers used by Internet operators. They could have been used for the purpose of disturbing network operation. According to CERT-FI's information, vulnerabilities were not, however, exploited. The device manufacturer has delivered the software update patches to registered customers.

Attempts are often made to exploit software vulnerabilities commercially. Information on vulnerabilities has been publicly on sale since 2002. However, during the last year, trade on vulnerabilities has become livelier due to the Swiss website WabiSabiLabi auctioning vulnerabilities. Vulnerability information is bought by for example manufacturers of information security products for the purpose of using it in their products which also benefit from the marketing. Normally, vulnerabilities are released after some time in cooperation with the manufacturers of vulnerable software.

Vulnerability trade involves problems, too. Malware authors can get information of vulnerabilities by analysing information security products where the information bought has been used. There is no guarantee of the reliability of vulnerability traders and vulnerability information is sought-after and valuable information among the network criminals. Unreleased vulnerabilities can be exploited in targeted attacks, in particular.

27.12.2007

CERT-FI

Websites spreading malware focus on certain foreign networks

Servers that spread malicious content seem to have concentrated as customers of the same network operators or server hotels. Some internet operators seem to have blocked traffic to some of the most notorious network addresses. Public objections have been expressed on the operations of Russian Business Network, in particular. It seems that it has sought to change the IP address spaces it used at the end of the year.

Future prospects

CERT-FI released nearly 200 alerts on software vulnerabilities and seven warnings. Since the beginning of this year, vulnerability alerts and warnings have been separately released and the grounds for releases have been adjusted. In addition, CERT-FI published over 100 Information Security Now! articles on current information security issues in Finnish.

The significance of software vulnerabilities is still great. Vulnerabilities are also found in more closed environments, such as applications used in the industry. Systems in the planning of which the possibility of the spread of malware has been ignored can be extremely vulnerable.

In addition to several minor cases, last year, CERT-FI has worked on a major vulnerability coordination project affecting the products of several manufacturers. The results are expected to be released in early 2008.

Unpatched and unreleased vulnerabilities can be exploited in targeted attacks where attempts are made to spread the malware tailored for the purpose to the selected target only. The objective can, for example, be to obtain information about the target organisation.

E-mail is still used for spreading malware either by attaching files containing malware or incorporating links to messages that lure careless users into websites exploiting well-known vulnerabilities.

The technical development of malware brings along new challenges and it is more difficult to find out how the new botnets function due to their distributed command structure. Electronic services are still rather vulnerable to denial-of-service attacks which can be implemented either by botnets or peer-to-peer networks. It is possible that malware monitoring or hijacking browser connections expand the group of services they know to Finnish services as well. Information security viewpoints familiar from computers can also be taken into consideration in the use of mobile phones.

As the number of broadband subscribers continues to grow, the number of malware discoveries seems to be decreasing in Finnish networks. Smooth cooperation between telecommunications operators, information security companies and information security authorities, as well as national legislation and information security regulations have contributed to the positive development. The Finnish model functions as an example in international circles such as the EU.