

3.7.2007

CERT-FI

INFORMATION SECURITY REVIEW 2/2007

The denial-of-service attacks that appeared during the first quarter of the year continued during the second quarter. In May they hit the headlines particularly due to the attacks against the services of the Estonian public administration and the Finnish Broadcasting Company YLE. The methods of implementation and targets of the investigated denial-of-service attacks differed from each other and, according to the information received by CERT-FI, there was no direct connection between these two cases.

During the second quarter CERT-FI released in total 39 vulnerability notifications and 35 informational 'Tietoturva nyt!' blog articles. No warnings were published.

The traffic produced by computers infected by independently operating and spreading Allaple malware has disturbed the function of Finnish web servers for nearly a year. The effects of the attack are being fought by means of antivirus software which is distributed along with the upgrades of the Windows operating system.

Systems of public administration and banks were attacked in Estonia

Denial-of-service attacks hit the headlines, when the attackers tried to paralyse the internet services, particularly websites, of the Estonian public administration. In addition, servers of banks and news services were attacked. The attacks started soon after the outbreak of the so called statue dispute at the end of April and went on during several weeks.

At first the Estonians fought the attacks by restricting all incoming traffic from outside Estonia, which prevented a major part of the encumbering traffic. Later the traffic was filtered on the basis of IP addresses and the contents of messages.

Denial-of service attack appeared in Finland

In May attacks against Finnish services were brought to the notice of CERT-FI. On Monday 14 May a denial-of service attack was targeted at the web server of YLE and this was repeated in the same evening. The attack continued the following day and during that day the website www.yle.fi worked slowly or temporarily not at all. The attack was first fought by preventing international access to the service. Later attempts were made to distinguish disturbing traffic from normal users' connections by analysing the contents of incoming packages. In the attack against YLE, the server was loaded down by requests for connection of file distribution software based on peer-to-peer network which were conducted from more than a hundred thousand different IP addresses.

On Monday 14 May an attack against Eniro's website suomi24.fi was reported. This appeared as temporary breaks and deceleration in the service. To CERT-FI's knowledge, the attack was implemented in a different way than that against YLE. The targeted servers are located in Sweden. The attack was repeated on Monday 21 May.

The denial-of-service attacks aim at overloading the targeted service in a way to prevent its normal use. The attacks are usually implemented by means of self-spreading and self-operating malware or botnets. However, the attack against YLE exploited the flaws in the file distribution software operating in a peer-to-peer network.

3.7.2007

CERT-FI

Publicity of attacks also brought about unnecessary reports

News on simultaneous denial-of-service attacks led to false conclusions regarding usual interruptions in operation, as the functionality of services was monitored more carefully than usually. CERT-FI was not reported any exceptionally high number of cases that could be classified as denial-of-service attacks.

At the end of May CERT-FI published on its website two notices concerning denial-of-service attacks and preparation for them. In addition, CERT-FI organised, on May 22, a press conference dealing with denial-of-service attacks and also issued an extra information security review 1B/2007 to this effect.

Progress made in prevention of the Allapple network worm

Since July 2006 malware called *Allapple* has been spreading in information networks. Its sole purpose is to block certain network services. One of the targets is hosted in a Finnish network. As soon as it has been launched Allapple seeks to infect more and more computers and disturbs its targets independently without any command or control channel. The lack of command connection also means that once the worm has started spreading, the traffic produced by it cannot be stopped. The problem is not removed before all infected computers have been disconnected and the spreading of the malware stops.

To alleviate the harmful effects of the malware Microsoft has added a description of the Allapple network worm to the tool for removal of malware. The *Malicious Software Removal Tool* distributed along with automated Windows upgrades identifies and removes the Allapple malware caught by a computer. CERT-FI monitors the effects of preventive measures - so far the volume of harmful traffic has not decreased to a great extent.

Spyware familiar with thousands of on-line banks

Particularly the users of on-line banking services are attacked by scams where attempts are made to infect a customer's computer by spyware. Usernames, passwords and other information can be hijacked through it. There is also software by means of which a user's on-line banking connection can be hijacked so that the attacker feeds information to the banking service unnoticed by the user.

The volume of banking services recognised by malware continues to grow. Commonly used spyware is already functioning with thousands of different on-line banking services and these include Finnish banks as well. As far as CERT-FI knows, Finnish banking services have not so far been targeted by such misuse that would require from users of services any other measures than normal precaution.

Spyware is systematically spread either as attachments to spam messages or by attaching links that lead to a web page with malware. Usually a computer is infected by malware when the user clicks the relevant link by the browser. To transmit malware, such non-patched software vulnerabilities of operating systems or applications may also be exploited that enable unnoticed infection without any measures by the user.

Recently, information has been received on particular software for spreading of malware which is on sale in the internet. By means of the *MPack* software it is easy to abuse numerous different vulnerabilities for spreading of malware through quite harmless-looking websites. The transmitter

3.7.2007

CERT-FI

of malware installs the program into a hacked web server, and it starts when the pages are browsed. The program seeks to infect the user's computer by making use of several different vulnerabilities. One non-patched vulnerability is enough to allow malware infection.

Plenty of vulnerabilities detected as usually

A major part of the detected software vulnerabilities concerned software used in workstations. At the end of March a vulnerability relating to the handling of so called animated cursors (mouse pointer) in Windows was released. There was no patch immediately available. This vulnerability concerned several versions of Windows, the new Windows Vista as well, and it was easy to exploit it by means of a website or an e-mail message. Microsoft released a patch for the flaw faster than normally in early April. Several other vulnerabilities in Windows and Office software were also patched.

Numerous vulnerabilities were discovered in products related to information security, such as antivirus software and firewall equipment. Patches were also released for Mozilla Seamonkey, Firefox and Thunderbird software.

CERT-FI was informed of several websites which had been hacked by making use of the vulnerabilities of the PHP programming language.

Faults and interference

At Easter, from 6 to 8 April 2007, there was an interruption in TeliaSonera's e-mail service resulting from a technical fault. At its largest the fault affected ca 400,000 e-mail customers, and the connections of ca 200,000 customers were broken all the time.

Some hardware failures appeared in the transmission systems of the backbone network and these caused shorter interruptions in broadband services and the services in the fixed telephone network and the mobile network. Excavation work caused a few cable ruptures in the backbone network and regionally hindered telephone and data traffic.

Regional interruptions have occurred in the transmissions of terrestrial digital TV and the analogous television, which have resulted from interference in TV transmitters. The biggest disturbance occurred on 26-27 May 2007 in Joutseno, where a lightning struck the transmitter mast.

Future prospects

Electronic services have proved to be easy goals and denial-of-service attacks to them or attempts of breaches into systems will probably be seen in future, too. The disturbances in on-line services will be followed up in mass media more carefully than before, which makes them attractive targets to gain publicity.

In addition to hacked computers and those harnessed to attacks, command & control servers of botnets used in attacks have been discovered in Finland. It seems that so far the preparation of attacks in Finland has not been professional activity, but is performed for instance by young people eager to gain publicity and having access to a number of hacked computers. However, botnets can also be systematically used in criminal activity for gaining economic benefit or disseminating ideological propaganda.