

11.4.2007



## INFORMATION SECURITY REVIEW 1/2007

During the first quarter of the year, CERT-FI received word about an unusual number of denial-of-service attacks or attempts of those. The most noteworthy attacks were targeted at Internet name servers and the network services of a Finnish company. Unexpectedly, an independently operating malware was behind the attack against the Finnish target.

A widespread spam campaign advertised for fake websites which lure Internet users into revealing their banking usernames and passwords. Some of the fake servers and domain names directing the user to them stayed active for as long as weeks. All of them originated from foreign networks. So far, spyware attacks against Finnish services have been rare, although signs of change are evident.

In addition to workstation software, vulnerabilities were discovered in Internet routers and SCADA systems used for industrial process control. Releasing vulnerabilities under thematic campaigns for given software or operating systems continues.

### Denial-of-service attack against root name servers

A denial-of-service attack was launched against *Internet root name servers* in early February. The attack was initiated by a botnet network consisting of hijacked computers and lasted for about a day. Although the attack volume was significant, the effects in practice remained insignificant as ten root servers retained to operate. The operational obstruction of three logical root servers showed as occasional, slower Internet speeds for the majority of users.

At the time of the attack, reports were received on access being denied to name services of some national top level domain names. Part of the disturbances resulted from the fact that the name services of the concerned top level domains were initiated from the same system as that of the Internet root.

The attacks did not affect the service level of fi-domain names, although the level of readiness was raised for awhile together with parties maintaining name servers. It was decided that the introduction of the FI root server monitoring was advanced as a result of what happened.

### Open servers as denial-of-service attack tools

Since the name service system does not validate the queries, it is susceptible to address spoofing. By abusing this characteristic, it is possible to enable the so-called *recursive resolver* to function as an amplifying attack mirror. This can be done by directing the results of DNS queries produced by the server to a third party who is under attack. When forged queries are sent to several name servers, the target suffers from a distributed denial-of-service attack. It is often difficult to find out who the source of the traffic is, and it requires the active cooperation of several parties.

On 9 February 2007, CERT-FI received word about a widespread denial-of-service attack which also exploited Finnish name servers. The attack repeated on 28 February 2007. Maintainers of Finnish servers were contacted at both occasions and they were advised to change their server settings so that it would no longer be possible to exploit them for attack purposes.

11.4.2007



## "Fire and forget" style denial-of-service attack

Since July 2006, a malware named Allapple has been spreading in information networks. Its sole purpose is to prevent certain information services from operating. What makes the case interesting is that one of the targets is hosted by a Finnish network, and the malware's unusual functioning method.

Denial-of-service attacks normally exploit a remotely-controlled botnet network. However, the Allapple network worm operates differently. The malware spreads itself only and generates disturbing network traffic to the addresses determined by the malware designer. After the malware has been released, it works independently without any command or control connection.

Lack of command signifies that it no longer is possible to stop the traffic caused by a worm that has started spreading. The problem only vanishes when all contaminated computers have been removed from the network and the malware stops spreading. It is difficult to filter malicious network traffic caused by the malware, because connections originate from different parts of the world, and the traffic looks the same as that of authorized users.

Allapple has caused its targets serious difficulties despite the major efforts of operators to filter network traffic.

## Denial-of-service attacks against e-mail servers

CERT-FI learned that denial-of-service attacks had also been targeted at Finnish e-mail servers.

One of the attacks was lengthy and its objective may have been to detect the performance of the target system. The increased number of connections shows as a growth of server load, but the service is not, however, completely blocked. The attack burdened the server by sending messages to fake addresses.

At the end of March, a serious attack was targeted at the servers of a Finnish e-mail service provider. As a result, e-mail traffic to firms using the servers was blocked for several hours. The attacker opened a large amount of connections to the server, but left them to wait for time-out.

It is difficult to prevent these kinds of attacks by filtering connections, because the attack traffic reminds that of authorized e-mail transmissions. There may be hundreds or thousands of computers in different networks that are exploited for attacking purposes. It is difficult to use Finnish computers as attack tools, because, according to the FICORA Regulation 11/2004 M, SMTP (Simple Mail Transfer Protocol) traffic from consumer subscriptions is, in principle, only permitted to the Internet operator's own e-mail server.

## New wave of Internet scams

In March, a widespread phishing operation was detected where attempts were made to lure, among other things, the customers of Nordea Bank to reveal their usernames and passwords. Millions of spam messages contained links to scam pages founded in several different countries. This time, Finnish customers were also lured to the website.

The majority of the domain names used on the scam websites were registered in Hong Kong and servers were found e.g. in Estonia, Rumania, Bulgaria, Korea, Chile, France and the United States.

11.4.2007



Nordea was not by far the only scam target, but scam websites imitating tens or even hundreds of different services operated simultaneously on same servers.

The implementation of the websites refers to the use of the *Rock Phish Kit* tool, which contains complete settings for creating websites that resemble several Internet banks. The tool kit enables the fast creation of a large amount of sites that can be used for the purpose of collecting usernames and passwords.

### More discoveries of stolen data by spyware

The birth of a new generation of malware stealing information and controlling computer users can be pinpointed to February 2006, when the Finnish antivirus company F-Secure received first reports of a malware called Haxdoor. In July 2006, CERT-FI received the first reports of Finnish victims of malware attacks. In addition to Haxdoor, malware known as BZub and Torpig have been involved in these cases, too.

Early this year, CERT-FI found out of many log servers that had been harnessed for the use of spyware to store information stolen from malware-infected computer users. Log servers can, without exception, be tracked down to foreign countries and often to same networks. Insofar, it is too early to say whether the growth of reported log servers results from the fact that spyware are becoming more common or parties keeping their eye on the malware situation have intensified their monitoring.

CERT-FI has discovered that the users of Finnish services are not the main target of the scams or spyware, but the tool kits used for creating phishing websites and malware are familiar with Finnish services, too. It seems that as malware develop, small and local electronic services may also end up being targets of phishing attempts.

### Workstation software vulnerabilities

Several vulnerabilities were disclosed in workstation software during the first quarter of the year, and some of them still need to be patched.

In late March, a vulnerability related to the handling of the Windows so-called animated cursors (mouse pointer) was released. There was no patch for it. What made the flaw interesting was that it affected many different versions of Windows, also the new Vista, and that it was easy to exploit it via a website or e-mail message. Microsoft hurried to release a patch for the flaw on a faster timetable than normally as early as early April.

### Vulnerabilities in industrial software

In March, vulnerabilities in SCADA products were released. They are used in the industry to control the processes in factories and to forward test data. No special attention has been paid to the security of SCADA products earlier, because they are used in closed networks in production plants.

The SCADA products set high demands for the safety of network and data processing environment. Even conventional network disturbances can cause serious fault situations. Information security incidents related to SCADA systems have increase over the past years.

CERT-FI estimates that the vulnerabilities released in March may also have posed a threat to systems that are the most critical with regard to society's fundamental services. Specifically-targeted notices and analyses of vulnerabilities were sent to system holders.

11.4.2007

CERT-FI

The vulnerabilities now released were discovered with the help of an independent player's test material. In all likelihood, this method will help discover more vulnerabilities in other SCADA systems.

### **Network device vulnerability led to traffic filtering**

A vulnerability in the Internet router devices used in the Cisco IOS operating system released on 25 January was exploited in denial-of-service attacks before all devices were updated to patch the vulnerability. In order to prevent the attacks, some operators decided to filter network traffic, which users may have noticed as non-access to certain network services.

### **Vulnerability release campaigns continued**

The politicization of vulnerability releases, which began last year, has continued. Thirty previously-unpublished vulnerabilities related to Apple software were released in January. The objective of the people behind the "The Month of Apple Bugs" theme month was to encourage Apple to act in a more responsible manner with regard to vulnerabilities in their products.

In March, 44 PHP vulnerabilities were released. PHP is a popular programming language used in network applications. Also, "The Month of PHP Bugs" was an answer to the software developers' manner to handle vulnerabilities found in them.

### **Faults and interference**

No major fault or disturbance situations occurred. In the morning of the 19th of February, a fault was discovered in TeliaSonera Finland's consumer and corporate e-mail services. It prevented users from checking their e-mail messages for about three hours. In addition, consumer customers were not able to send messages.

### **Future prospects**

CERT-FI estimates that users of Finnish electronic services, as well, will become targets of systematic malpractice attempts in the future. Tool kit collections used for creating malware and fake websites already now contain network addresses of Finnish services, names and other key words.

Many electronic services have proved vulnerable to denial-of-service attacks and we may have to witness more attacks against them. The attacks may be targeted at e.g. web servers, e-mail servers or name servers. Service providers should be prepared for the possibility of hostile attacks. Attacks can be implemented either by self-spreading and self-operating malware or botnet networks.

Vulnerability release campaigns will probably be seen in the future, and finding patches for the vulnerabilities released in them will keep software manufacturers busy. Not all campaigns announced so far have been implemented or their effects have remained rather insignificant in the light of information released to public.



11.4.2007



## Terminology

**Denial-of-service attack** = An attack whose purpose is to prevent the normal operations and use of the targeted service.

**Root name servers** = The thirteen name servers at the top of the hierarchical Internet name service system, which are the point of departure in search for name service information.

**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.

**Resolver** = A name server an Internet-connected computer uses for making dns queries. The searching party is given an answer from the resolver, which takes care of the dns query on the behalf of the searching party from that point on.

**Recursive dns query** = A dns query where the resolver finds the requested piece of dns information without the computer, which is the searching party, needing to directly contact the authoritarian name server of the target of the query.

**Authoritative name server** = Name server that is responsible for authoritative data for a domain or an IP address.

**SCADA (Supervisory Control And Data Acquisition)** = A system for industrial process control and test data acquisition.

**PHP** = A programming language used for producing and editing the contents of websites

**SMTP (Simple Mail Transfer Protocol)** = An Internet protocol for sending e-mail messages to the e-mail server and transmitting messages between e-mail servers.