

CERT-fi

ANNUAL REVIEW 2008

16 January 2009

CERT-FI Information Security Review 4/2008

Introduction

Vulnerabilities in the internet's infrastructure emerged in 2008. A vulnerability in the internet domain name service (DNS), if left unpatched, would have made it possible to misdirect the user or divert e-mail to a false address. CERT-FI issued a warning on the vulnerability. The DNS servers were soon upgraded to fixed versions, and the vulnerability was not widely exploited. However, the incident proved that the domain name service is inherently vulnerable to attempts to forge data. Another vulnerability found in TCP protocol implementations may affect many devices and software to be connected to the internet.

Malicious activity in the internet proved to be more clustered than expected. The volume of spam in the networks dropped radically for a short period as a service provider hosting a number of command and control servers for large botnets was dropped from the network last November.

The contents of many Finnish web pages have been repeatedly modified, without authorization, by exploiting common vulnerabilities in server software. Server break-ins nowadays usually aim at exploiting sites for the purpose of distributing malware, and connecting new, hacked computers to botnets. Right at the end of the year, a malicious worm spreading independently in local area networks was discovered. It infected workstations and networks both in Finland and abroad.

In 2008, CERT-FI published two information security warnings, 156 vulnerability notifications and 83 Information security now! articles.

Far-reaching vulnerabilities reflect the age of the internet

The Internet's protocols and software partially date from 30 years ago. When they were developed, the networking environment was totally different from today. The design was guided by simplicity and performance with the slow connections and computers of the time. No particular attention was paid to information security as the Internet was planned. It has been difficult to modify or replace many of the established protocols later.

The operational environment of the network has become more hostile because the massively growing number of users. Therefore, many shortcomings of early design choices have become problematic. They also make it more difficult to make the internet safer and to prevent malicious activity.

DNS vulnerability is based on insufficient authentication of the communicating parties

In the summer of 2008, Dan Kaminsky published a vulnerability in the internet domain name service (DNS) that raised quite a lot of concern among the information security community. The vulnerability was based on the fact that UDP protocol is used by the DNS and a two-way handshake is not required to establish a connection. This makes it possible to send DNS queries and, in particular, the responses related to them by using a spoofed IP address. It is also almost impossible to trace the actual sender of UDP protocol packages.

Name server queries and responses have an identifier which binds the query to the response given by the server. In certain circumstances it was relatively easy for an attacker to guess the next identifier to be used and inject forged responses to the host sending the query. The name server software was fixed so that the choice of query identifier was more random.

However, the patches are not sufficient to completely fix the inherent flaw of the DNS query protocol. Name server queries can still be made by using spoofed

addresses and thus use name servers in denial-of-service attacks. It is not possible to verify the authenticity of the server responses, which makes it possible to misdirect the users by instructing the host to use a rogue name server. At the end of the year, CERT-FI was informed of a piece of malware functioning as a DHCP server, and changing the name servers of computers in the local area network. The new servers gave forged responses to certain queries, for example to direct the users to fake network banking pages.

The DNSSEC extension designed for the DNS protocol makes it possible to authenticate the name server responses. So far, the DNSSEC has not become more common, however, because of a few deployment challenges. It causes more load to the name servers and creates more network traffic. The management of encryption keys may be problematic, and also a political issue.

Problems found in the implementations of the TCP protocol

Over the years, several improvements have been made to the TCP protocol and its implementations. The TCP has been designed for reliable data transmission and its faults have mainly related to its complexity.

In September, the Swedish company *Outpost24* reported that they had discovered vulnerabilities related to TCP protocol implementations. Information about vulnerabilities was presented in the Swedish Sec-T and Finnish T2 information security conferences. Later, Outpost24 contacted CERT-FI in order to coordinate the patching of vulnerabilities with different manufacturers. The coordination process has progressed as expected. CERT-FI and its international cooperation partners have contacted software manufacturers so that they can assess the impacts of the vulnerabilities on their own products. Further details on the vulnerability are expected to be published in 2009.

Vulnerabilities in mobile software

Mobile malware or significant vulnerabilities have so far been rare. Right at the end of the year, a vulnerability in the S60 operating system in mobile phones emerged. It makes it possible to make a denial-of-service attack against mobile terminals. A software error in the processing of text messages was found in the phone's software. If a maliciously formatted text message was received by a phone with vulnerable software, the phone could no longer send or receive further messages unless a factory reset was performed. The Finnish mobile operators have begun to filter messages known to be malicious.

CERT-FI was also informed of other vulnerabilities affecting the information security of mobile devices. No decisions have yet been made on when they will be published.

Vulnerability coordination kept CERT-FI busy

The vulnerability coordination of CERT-FI has been active in other respects, too. In March, test material compiled by the Oulu University Secure Programming Group OUSPG, for testing the functionality of numerous packing and archive formats was published. The test material helped to find vulnerabilities for which updates have been released along the year.

Vulnerabilities in commonly used open source OpenSSL and GnuTLS cryptographic software were published in May. The vulnerabilities were detected by Codenomicon Ltd. Other manufacturers using the vulnerable code in their software were contacted.

In September, Codenomicon Oy also found another vulnerability in the ICMPv6 implementation of KAME project's open source IPv6 stack. CERT-FI was given several coordination tasks during the last quarter of the year, which are likely to be published in 2009.

Confidentiality of communications is tested

There has been a lot of discussion on the confidentiality of communications in context with the preparations for the amendment to the Act on Protection of Privacy in Electronic Communications. At the beginning of 2009, the Swedish National Defence Radio Establishment (FRA) was given the right to perform signal intelligence for communication transmitted in fixed networks via Sweden. The majority of the Finnish internet traffic to other countries is transmitted via Sweden. Signal intelligence may be targeted at unencrypted communication, in particular.

E-mail messages may be transmitted unencrypted between email servers. Tapping the network traffic opens access to the content of the messages. It is possible to encrypt the content of confidential messages and provide them with an electronic signature. However, this must be separately agreed upon with the recipient, because none of the encryption methods of e-mail messages has become so common that it could be easily assumed to be used by the recipient, too. In any case, the identification data of the message, such as the recipient's e-mail address, must be sent unencrypted in order for the messages to be delivered.

The SMTP protocol used for transmitting e-mail messages does not require the verification of the sender's address, which makes it possible to send e-mail messages under anyone's name. E-mail is the largest distribution channel of unwanted content such as unsolicited advertising and malware. The majority of spam is sent by botnets consisting of hacked computers of individual users. The problem is mitigated by spam filtering programs.

The significance of botnets is still great

In recent years, botnets have become established as the most important medium of information security crime. Even server break-ins are currently made almost exclusively to expand the botnets instead of stealing data on the server.

Search engines are used to find vulnerable servers in order to use them for spreading malware.

Users are lured to hacked sites where a botnet malware is infected on their computers and the malware contacts the botnet management server. Botnet computers can be commanded from the command and control server to collect and deliver information contained in the computer, spread malware further to new servers, send spam or initiate denial-of-service attacks. The malware can also spy and forward data that is saved in the computer or during a web session to third parties.

New versions of malware are continuously spread to prevent anti-virus software from recognizing them. They are also able to update themselves automatically.

Temporary collapse of spam

Server hotels that approve or disregard criminal activity, domain names registered for criminal purposes and traffic peering agreements are important factors in the prevention of cyber crime. Botnets of hacked computers are also important. In order to expand the botnets, malware is spread to new computers.

Server hotels focusing on malicious content and their network operators have proved to be significant factors. These service providers are sometimes called "bullet-proof hosting" or "anti-abuse-resistant hosting".

In mid-November, *Intercage*, having lost their network connection in September, was joined by another service provider called *McColo* in San Jose, California. Their disconnection was preceded by articles written by information security researchers and the media about

malicious traffic detected in their network. Command and control servers of spamming botnets were detected in the *McColo*'s network addresses. The effect of the suspension of internet access of the service provider was a surprise: according to different estimates, the spam volume in the internet was cut by half.

In a few months, spam volume returned closer to its former level. There are still several hosting service providers focusing on malicious services or tolerating them in various parts of the world.

So far, no service providers that systematically favour malicious services have been found in Finland. Cooperation between CERT-FI and Finnish internet service providers is effective. The information security incidents discovered in the networks of Finnish providers of hosting services are usually the result of neglected software updates and other information security problems of web services.

Domain names registered under false information for illicit purposes

Domain names registered under false information are commonly used for spreading malware and phishing. The identity or contact information of the party registering the domain names is seldom verified.

The malware often contain pre-coded domain names they use later for establishing a connection to their command and control server. The software may also contact the random-looking domain names which have been formed on the basis of date and time, for example. This makes it more difficult to block the control servers, because the address used by the malware may change on a daily basis and their formation method may remain unsolved.

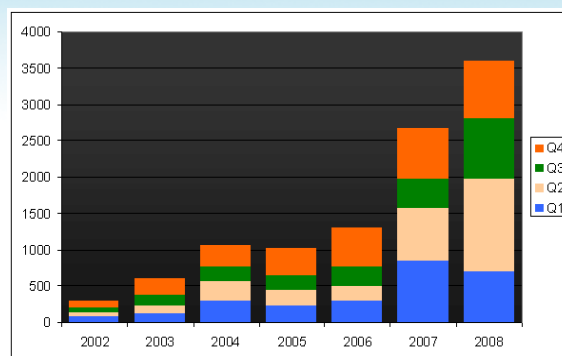
Such domain names have not been registered in Finland, but malware has used international domain names. Many international surveys show that the *fi*-domain name is the safest in the world.

Intervening in malpractice is often slow

So far, intervening in the activities of bullet-proof hosting service providers has been rather occasional and unorganized. The reason of internet service providers to intervene in their activities is based on business decision, because customers that appear to be involved in criminal activities can hinder the operator's business and damage its reputation. The authorities' role in disconnecting Intercage and McColo from the network seems to have been slight. The apparent inefficiency of preventing information network crimes has inspired information security researchers to publish reports on the malicious traffic in the networks of the service providers in question. This seems to have led the operators that provided network connections to Intercage and McColo to terminate their contracts. Large telecoms operators with their service contracts are in a key position if an individual player needs to be isolated from the network. It can be stated that this operations model reminds of an approach of "taking law into their own hands".

ICANN, International Corporation for Assigned Names and Numbers, and the European IP address administrator RIPE have reacted to some cases of malpractice. ICANN revoked the right to register domain names from a domain name provider named Estdomains. Domain names registered through the company have been transferred to another service provider. RIPE, for its part, has revoked the IP addresses granted to the notorious service provider Russian Business Network.

ICANN and RIPE base their solution on contract breaches related to the use of technical network resources. However, it is not sufficient for bringing the offenders to justice. In addition to the active surveillance by the internet service providers and CERT community, there is a need for improved efficiency within the international police cooperation in order that the considerably complex activities of criminal organisations at the international level in information networks could be influenced in an efficient manner.



The number of incidents handled by CERT-FI grew from the previous year.

Shortage of IP addresses, major challenge ahead

Still, the majority of the internet traffic is based on the IP protocol v4, although it has a limited number of IP addresses. Despite the arrangements made to avoid the problem, e.g. Network Address Translation i.e. NAT, IP addresses are running out. According to the current estimate, they will last for a couple of years.

The IP protocol v6 has been designed to replace the current one, and has significantly more addresses available. The protocol is already used to a certain extent, mainly as a trial version, but its share over internet's telecommunications traffic is so far extremely small.

The introduction of the IPV6 will be a long-term project which is likely to affect nearly all internet-connected computers and active network devices. Some of the devices may become completely useless and software updates are necessary for the majority of them. The transfer period will be long, too.

So far, there is not much experience of systematic use of the IPV6. It is expected that new functional and information security-related flaws will be revealed in the protocol and design of solutions relying on it.

Despite the small share of IPV6 users, in 2008, CERT-FI was informed of the first malware in Finnish networks using native IPV6 connections.

Malware are spread via hacked websites

The spreading of malware is often based on the use of search engines to look for e.g. SQL injection vulnerabilities which makes it possible to modify the contents of the web site. When the infected server is found, a small piece of JavaScript code is attached to the page to lead the users accessing the site to a site hosting malware. The additional link attached to the page can easily be missed by the maintainer of the site.

New vulnerabilities are continuously found in popular content management systems that enable malicious code to be injected to the web pages. Therefore, it is important to make sure that the software is kept up to date and patched to fix the vulnerabilities.

Software vulnerabilities in the user's computer are not necessarily exploited to infect computer. Malware can be disguised as e.g. a program or codec needed for watching video files or even as a security program, such as spyware remover, firewall or antivirus software. The users are lured into installing programs themselves on their computers. In some cases, the user may even buy and pay for the installation of such a software. Pirated software packages or licence key cracking programs are also often infected.

In addition to websites and e-mail messages, links to malware were spread via instant messaging.

Network worm spread at the turn of the year

A self-propagating piece of malware was discovered at the end of the year. The worm has infected computers both in Finnish and international networks. It aims to spread between computers in many different ways. After the infection, it tries to contact the incidental network addresses to update itself. These network addresses are formed on the basis of date and time.

Phishing sites and e-mail messages have hardly bothered Finnish users

The phishing sites discovered during the year have not been very convincing from the Finnish users' point of view. The majority of the actual phishing sites seem to be focusing on the customers of international services. Several pages copying popular international services have been found in hacked Finnish web servers.

In the spring, e-mail messages with a malicious link were spread. If infected, the user's online banking session may have been hijacked. The message was about "a nuclear power plant accident in Mikkeli" or "Tatjana looking for company" and it fooled many into installing a malware on their computer. The same message and malware were spread in many other European countries.

Off-season in network activism

No significant numbers of denial-of-service attacks targeted at Finnish services or stained sites occurred in 2008. No particular information security incidents were related to the arrangements of the Organization for Security and Cooperation in Europe (OSCE), which was chaired by Finland.

During the Georgian conflict, some local web servers were hacked in Georgia and propaganda content was added to their sites.

Future prospects

According to CERT-FI, spreading remote-controlled and updatable malware to computers remains a significant threat to the users' information security. Malware are becoming more versatile. Once a computer is infected, it can be reused for many sorts of malicious purposes by updating the malware features.

The distribution methods of malware will continue to develop. Hacked websites and luring e-mail messages will still have a significant role. Extensive campaigns and more targeted distributions help infect the software.

CERT-FI contacts per item	1-3/2008	4-6/2008	7-9/2008	10-12/2008	2008	2007	Change
Interview	17	29	21	21	88	80	+10%
Vulnerability or threat	39	232	52	71	375	64	+485%
Malware	460	727	532	437	2156	1678	+28%
Guidance	64	87	92	116	359	393	-9%
Preparation for attack	32	27	12	16	87	3	+2800%
Data break-in	14	88	45	40	187	119	+57%
Denial-of-service attack	15	26	31	24	96	64	+50%
Other information security problem	10	11	12	10	43	48	-10%
Social Engineering	47	36	44	62	189	197	-4%
Spam (no statistics in 2008)	-	-	-	-	-	18	-
Total	698	1263	841	797	3580	2664	+34%

The majority of contacts handled by CERT-FI are related to various malware and information security threats caused by them. Reports of malware alone form two thirds of all contacts.