

cert-fi

**INFORMATION SECURITY REVIEW
2/2009**

3 July 2009

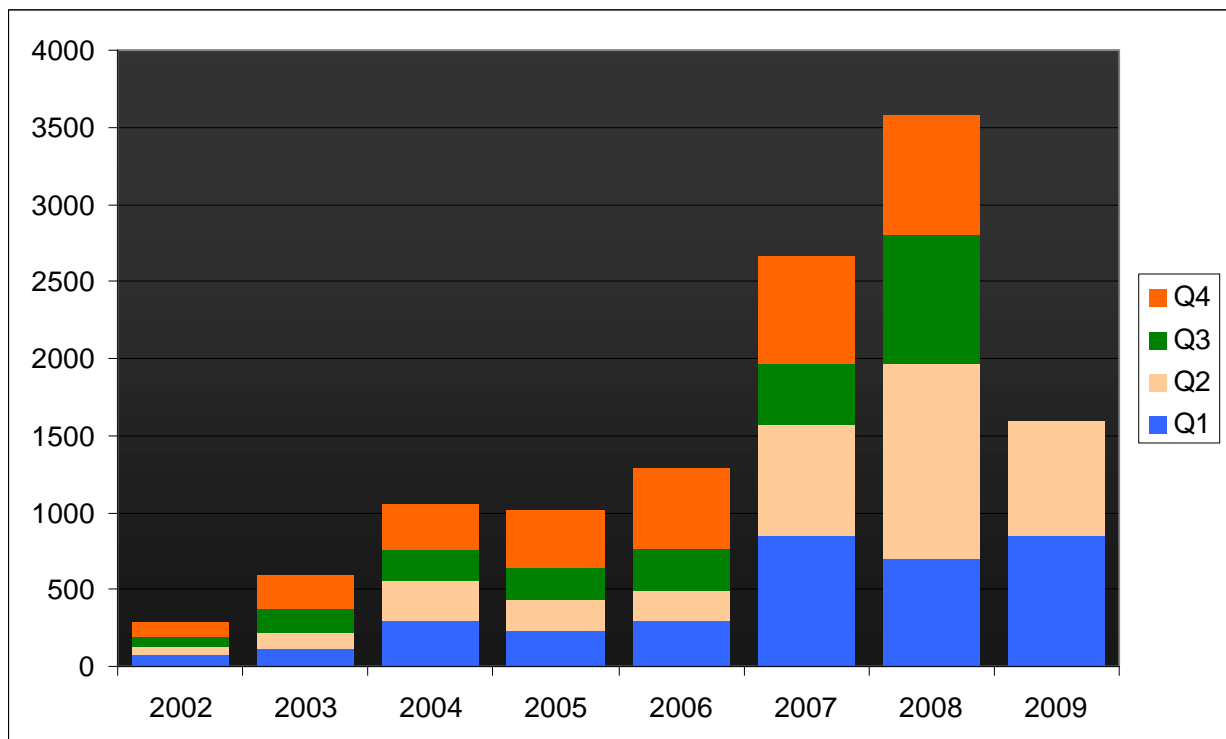
CERT-FI Information Security Review 2/2009

Introduction

Advertisements appearing on Web sites are also used for distributing malware. It has been possible to contract infection by malware through an advertisement appearing on a Finnish Internet discussion board. Containing the 'malvertising' phenomenon can be difficult, since Web site administrators do not usually control advertisements' content.

CERT-FI continues to be notified of computers that have been infected with the Conficker computer worm. For a short while, this worm even spread along with an operator-sold device.

Co-ordinating the rectification of vulnerabilities related to TCP implementation has proved challenging. Vulnerability-related fixes for dozens of manufacturers' software will be released in the future.



The number of cases processed by CERT-FI has dropped from last year's levels, now equalling the level seen in 2007.

Malware distributed through Web site advertisements

There is a documented case in Finland of malware having been distributed through an advertisement on a Web site. One could be infected by this piece of software through an advertisement frame that was hosted on a Finnish magazine's Internet discussion board. The malware did not download itself every time the advertisement was displayed; it was distributed randomly. This represents a conscious attempt to impede the correction of information security breaches.

Harmful content may enter otherwise safe Web sites by tagging onto outsourced advertising content. Thus far, this phenomenon, known as malvertising, has rarely been encountered on Finnish Web sites. As far as malware distribution is concerned, this is an efficient method against which site administrators have trouble protecting.

Web site administrators do not usually wield direct influence on the content of advertising; they provide space on their site, making an agreement with a service company that distributes advertisements. Advertisements are downloaded from an external server, their content varying with the occasion or depending on the country to which the visitor's IP address seems to have been assigned.

Harmful content seen on cracked Web servers

Malware is not the bane of Web sites in terms of advertising alone. On a weekly basis, CERT-FI receives reports of several Finnish Web sites on which someone has been able to enter harmful material.

Malware is offered for download on cracked servers onto which content can be sneaked by means of SQL injection – one way of taking advantage of unprotected or incorrectly programmed input handling on the server. Usernames and passwords that are intended for site maintenance and have been pinched via data-stealing malware can also be used for modifying page content.

Malware is most commonly offered to users from Web sites through addition of an iframe element in the page's source code while its visibility in the browser is cloaked by modifying the CSS style sheet definitions. The concealed iframe includes a cloaked JavaScript script or link through which the actual malware is downloaded onto the site user's computer.

The user may not notice anything out of the ordinary, and the malware may be downloaded without the user clicking on any of the links on the page.

The malware that is distributed via cracked sites often attempts to utilise known vulnerabilities in browsers and browser add-ons such as Flash and Java. The user can minimise the possibility of contracting malware by making sure that his or her Web browser, operating system, and anti-virus software are always updated to the latest version.

If someone manages to add harmful content to a popular Internet site, a piece of malware may be able to spread extensively through this site. However, malware and associated tools that automatically seek Web sites to be cracked do not differentiate sites according to their popularity, meaning that harmful content may appear on any vulnerable site.

Activeness of site and Web server administrators, server software updates, and monitoring of changes made to site content are all essential to keeping Web sites malware-free.

Information leaks from a poorly protected server

In May, a case was made public in which a Web server allowed the downloading of files that were not intended for public display.

This was a case of carelessness in determining site protection, resulting in a situation in which the directories on the server could be browsed and the files on it could be downloaded. These types of cases are not particularly rare, with some being reported to CERT-FI from time to time.

Conficker worm still common

Released in December, the Conficker Web worm, also known as Downadup, is still a common nuisance. CERT-FI receives reports of infected computers on a daily basis.

In the second quarter, we also saw the first signs of computers infected with Conficker being utilised for criminal activities. The peer-to-peer network created by this computer worm was used for downloading a piece of malware onto infected computers, and this software was used for carrying out a spam e-mail campaign. For reasons yet unknown, the piece of malware that was intended for spamming was programmed to self-destruct a month from its installation. This, however, is a one-off case; computers that are infected with Conficker have not been systematically used for criminal activities outside this case.

During the second quarter, CERT-FI sent out 22,000 notifications related to the Conficker worm to users. In Finnish networks, computers infected by this worm have been detected at around 5,300 different IP addresses. In the first quarter, some 14,000 notifications were sent out, concerning 3,600 addresses.

Conficker was briefly in stores

One of Conficker's distribution methods is the malware copying itself to USB memory units. In May, a case was publicised in which the memory card that was bundled with a USB communications Internet stick sold by a mobile operator contained the Conficker worm in addition to the operators' date security software.

Several dozen memory cards containing this worm were sold. The operator has contacted the customers who purchased a device that may have come with a piece of malware. When these Internet sticks were sold, all of the common anti-virus programs were able to recognise this version of the malware, making it likely that the repercussions in this case were modest.

GhostNet extended to Finns too

In our previous information security review, we detailed an extensive series of information system break-ins using targeted malware distribution. The perpetrators attempted to obtain information on the targeted organisations by means of the remote-controlled Ghost malware. According to CERT-FI's information, no Finnish parties were among the distributors of this malware.

CERT-FI received notice of two hijacked computers located in a Finnish network, albeit after considerable time had passed since knowledge of the malware became public. Information on the matter was conveyed to the appropriate persons.

Publication of information on TCP-related vulnerabilities draws near

The co-ordination process aimed at the publication of fixes for vulnerabilities related to Transmission Control Protocol stack implementation has progressed satisfyingly, in view of the complexity of the matter. The publication date for these fixes has been pushed back from the planned time. Such delays are common when the vulnerabilities concern various software and hardware manufacturers.

CERT-FI has contacted 65 manufacturers with regard to these vulnerabilities, 38 of which have since engaged in active co-operation with us. Most of the manufacturers have already been able to correct the vulnerabilities, but some are still in the process of creating a reliable rectification system. CERT-FI intends to publish all of the fixes in a co-ordinated manner; accordingly, we still cannot confirm a definite publication date.

Also, differing estimates of the seriousness of the vulnerabilities have been voiced among software manufacturers. It has been shown that they can be used to seriously hamper the use of many pieces of software, operating systems, and active network devices.

CERT-FI has published a statement, last updated in June, concerning the vulnerabilities. A link to this statement can be found at www.cert.fi.

The recently discovered serious software vulnerabilities have garnered some interest on the EU level as well. In late March, the European Commission held a workshop¹ on vulnerability management, in which other Finnish representatives participated in addition to CERT-FI experts.

Smartphone information security threats surfacing

Information security professionals have long been providing estimates on the increase of the information security threats that concern smartphones, including vulnerabilities and malware. Whereas computers have presented inviting targets for people wishing to hamper network operations and for information network crime, smartphones have thus far been spared the pernicious by-products of information networks.

With regard to both features and usage, smartphones are starting to resemble computers, increasing their allure in the eyes of intruders. Recently, more information security threats related to smartphones have surfaced in the wild. Forming the basis for this phenomenon is an increase in research into smartphone-related information security issues.

In the second quarter of 2009, information security problems discussed in public have included threats related to smartphones' installation messages and WAP Push messages. These are related to the remote management of phone settings and WAP implementation, as well as users' ignorance regarding the risks related to accepting SMS control messages that have been created with malicious intent.

Usually, these configuration messages are SMS messages sent by the operator that are used for conveying to phones settings that are related to Internet use, such as name service settings. However, such messages can also be sent in order to deceive users. Through changing of the

name servers used by the phone, users can be misled – directed to harmful Web sites. Some mobile phone models also enable remotely controlling phone functions by means of configuration messages.

The majority of the mobile devices on the market check the origin of the configuration messages they have received, while also asking the user for permission before accepting a configuration message. Cautious users should accept configuration messages only when their phone contacts a new operator network for the first time or when they have requested an operator to send settings to their phone.

Use of information networks in political activities proliferates

In 2007 and 2008, the political unrest in Estonia and Georgia could be witnessed in information networks too. Such methods as denial-of-service attacks were used to disrupt network operations and information society services. Cracked Web sites were used for publishing political statements. However, foreign states may not necessarily have been behind these attacks.

The Iranian presidential election in May 2009 brought out a new breed of network activism. Social networks and publishing services became a channel through which private persons communicated information and opinions on the events in Iran in the prevailing extraordinary circumstances.

Discussion boards and blog sites were also used for disrupting the distribution of dissenting opinions. These sites were used for instructing regular computer users on how to engage their workstations and Internet connections in denial-of-service attacks. In the associated attacks, botnets were used relatively sparingly; instead, the actions were carried out by means of, for instance, Web sites that were designed to generate HTTP requests.

Latvian malware distributor disconnected from network

CERT-FI assisted international authorities in solving a case involving a piece of mal-

¹ http://ec.europa.eu/information_society/policy/nis/strategy/activities/ciip/impl_activities/vulnerabilities_workshop/index_en.htm

ware that was used to steal banking information. This malware was being distributed through the Web addresses of a Latvian ISP.

During the investigation, it became apparent that the same network was used as the distribution platform for various pieces of malware. CERT-FI contacted the Latvian CERT organisation and the upstream network operator of the ISP in question. It turned out that several reports of this ISP actively engaging in activities that compromise network information security had been made.

As a result of this chain of events, the ISP's upstream operator cut off its network connections on the basis of breach of the terms of use.

Autoreporter awarded

CERT-FI's Autoreporter service was honoured in a contest² organised by FIRST (the Forum of Incident Response and Security Teams) and CERT/CC (the CERT Coordination Center). The contest was held in order to determine best practices for detecting and preventing information security violations.

Future prospects encouraging

In the latter part of 2008, the quantity of spam e-mail circulating on the Internet temporarily dropped to around half as operators distributing malicious content were cut off from the Internet. Since then, the figure has climbed back to its previous level, with some nine messages out of 10 constituting advertisements, messages attempting to distribute malware, or messages inviting people to engage in criminal activities.

In the international co-operative bodies, there are signs of an increased willingness to find solutions to these problems. However, jointly determined methods for interfering with infractions are still poorly developed. ICANN, which co-ordinates the Internet's address and domain name management, and APWG (the Anti-Phishing

Working Group), which concentrates on the prevention of theft activities, have begun efforts to increase their efficiency.

The Anti-Phishing Working Group is initiating a project that would enable use of domain names that has been set up with false information where those domains are used for phishing activities to be shut down within hours of the detection and reporting of the fraud; ICANN, in turn, is improving the monitoring of, and instructions for providers of, registration services for domain names. Both parties emphasise the need for close co-operation, particularly with national CERT organisations such as CERT-FI.

2

<http://www.cert.fi/tietoturvanyt/2009/06/ttn200906301435.html>

CERT-FI contacts by subject type	1-6/2009	1-6/2008	Change
Interview	61	46	+33%
Vulnerability or threat	65	271	-76%
Malware	1,055	1,187	-11%
Guidance	178	151	-59%
Preparation against attack	24	59	-69%
Information break-in	65	102	-32%
Denial-of-service attack	40	41	-2%
Other information security problem	46	21	+119%
Social engineering	59	83	-29%
Total	1,593	1,961	-19%

In the first half of 2009, reports of malware still comprised the majority of the information security cases processed by CERT-FI. For more statistics, please visit www.cert.fi.