

11.10.2007



INFORMATION SECURITY REVIEW 3/2007

Extensive attempts have been made to spread malware used for creating Botnet attack networks by e-mail. The Storm Worm malware is actively spread via spam, making it is one the most widespread malware.

CERT-FI has learned of targeted attacks against firms. These attacks aim to infect the information systems of internal corporate networks with malware unknown to antivirus software. Malware can, for example, be used for spying information related to business activities from the company's systems. It is more difficult to detect the targeted attacks than malware distributed in massive spam campaigns

Many vulnerabilities were still found in software. During the third quarter, CERT-FI released 60 advisories on serious software vulnerabilities and 26 Information security now! blog entries. No warnings were released.

Storm Worm spreads via spam

The Storm Word is a malware first detected in January 2007 and is spread via e-mail attachments and websites. During the summer and autumn, a lot of spam has gone around containing a link to a website spreading the Storm Worm malware. Currently, the Storm Worm is one of the most widespread malware in the world. However, CERT-FI has not received word about considerable amounts of infected computers in Finnish networks.

Computers infected by the Storm Worm are part of the very large Storm Worm bot network. The network of hijacked computers is commanded efficiently by a decentralized mechanism similar to peer-to-peer networks without centralized command server. According to information passed on to CERT-FI, Storm Worm bot networks are used actively for the purpose of launching denial-of-service attacks and spam.

The successful spreading of Storm Word is based on attractive messages, often written in English about current events or otherwise interesting topics. These messages lure readers into following the links in the message or open attachment files containing malware. The Storm Worm installs a rootkit as it attaches itself to the computer, which makes it difficult to be detected.

The Storm Worm does not exploit any specific software vulnerability, but recipients are lured into installing it on their workstations by clicking the links pointing to malware. Websites spreading malware strive to exploit known web browser vulnerabilities and the malware can install itself into the computer without the user knowing it. It is possible to reduce the likelihood of imperceptible infection by running regular software updates.

The Microsoft Windows operating system's Malicious Software Removal Tool is able to detect the Storm Worm malware and to remove most of its versions.

Attacks targeted at companies

Denial-of-service attacks made against corporate websites have received a lot of publicity in the media. In addition to denial-of-service attacks, corporate information security can be endangered by targeted attacks which aim at infecting corporate information systems with malware. The objective may be e.g. to use spyware for the purpose of obtaining information about the

11.10.2007

CERT-FI

company's business operations. CERT-FI has received word of such cases which have also involved Finnish companies.

Targeted attacks aim at accessing a specific company's or organisation's systems. A malware specifically programmed for this purpose and unknown to antivirus software may be used for the attack. These malware adaptations can also be bought via the internet. Instead of spreading large amounts of malware attached to e-mail easily recognizable as spam, only small quantities are sent to carefully selected recipients. The attacker aims at not being detected which would save the attacker from countermeasures.

Malware used in the attack are usually sent in a document attached to e-mail messages. The document exploits one of the known vulnerabilities in office software. The content of the message and distribution addresses have been carefully chosen so that even the company's own employees have difficulties noticing anything suspicious in the content. This method differs from spam messages spread as mass distribution. The message may concern factual matters related to the company's business and it may have been sent to the company's internal e-mail distribution lists.

The detection and prevention of targeted attacks can be challenging because automatic prevention systems do not necessarily detect them. Both the malware and methods used for the purpose of infecting malware have usually been skilfully selected. Patching known software vulnerabilities by installing the upgrades provided by the manufacturer reduces the risk of infection. Signing messages digitally would help the reader of the message to verify sender's identity, but it is only seldom used.

Many vulnerabilities are still found

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 e.g. as slave for bot networks. Vulnerabilities were found in e.g. instant messaging applications and media players.

Some of the vulnerabilities related to web browsers are related to plugin extensions and the same vulnerability can impact several applications.

As far as server vulnerabilities are concerned, attention should be paid in particular to PHP programming language and content management system vulnerabilities implemented by it. They can enable the unauthorized editing of website contents. Hacked web servers are widely used for e.g. fake websites and spreading malware. Also, vulnerabilities were found in several information security products, such as antivirus software.

Thunderstorm caused disturbance to communications networks

On 22 August 2007, a thunderstorm crossed Finland causing major problems to communications services. Mobile base stations experienced disturbances in the thunderstorm area. The thunderstorm also caused problems in the operations of fixed telephone network and broadband connections. As far as mass communications networks are concerned, a break in the transmission of YLE in the province of Uusimaa temporarily blocked the possibility of sending official and emergency notices in the Helsinki metropolitan area for a short while. However, the disturbances were quickly remedied.

11.10.2007



Spam jams e-mail servers

According to CERT-FI's information, the e-mail servers of Finnish operators have from time to time been overloaded due to large amounts of spam. The load has occasionally caused delays in message delivery. The load situation is, however, under control now. Other short-lasting problems in e-mail services have been caused by e.g. hardware faults and mishaps in routing.

Major outage in Skype service

Skype is an internet phone call software based on peer-to-peer network technology allowing users to talk and send messages to one another over the internet without telephone charges. A widespread disturbance hit the Skype service in the middle of August. The situation emerged as Microsoft launched its monthly software updates. According to Skype, the problem resulted from a software fault, which caused the overload of several computers using the Windows operating system as they tried to re-register with the network after they had restarted themselves. The users experienced problems in registering into the Skype network for several days.

Denial-of-service attack against CERT-FI web server

A denial-of-service attack was made against FICORA's website on the last weekend of September. Due to the attack, FICORA's websites, such as www.cert.fi and www.ficora.fi, could not be accessed for awhile.

Future prospects

It is probable that new denial-of-service attacks launched by botnets can be expected in the future. It appears that parties controlling the attack networks also defend actively against those investigating their activities. Some attacks can be seen as revenge against those investigating the activities or structure of these networks.

CERT-FI has received word of only a very few botnet controller computers in Finnish networks. The number of detected hacked zombie computers of Finnish users is somewhat bigger. They have been removed from the network together with internet service providers.

Network games have increased in popularity and attention should be paid to vulnerabilities and misuses related to games, too. Most often it is about luring players into revealing their usernames and passwords.