WHITE PAPER: SYMANTEC SECURITY RESPONSE

Regional Threats

Kaoru Hayashi
Symantec Security Response, Japan

Regional Threats

Contents

New families and new variants of threats, such as W32.Sober, W32.Blackmal, and W32.Beagle, attack systems across the world every day. These threats attempt to infect any system they can reach and propagate worldwide. They can be referred to as global threats. Meanwhile, we are also seeing an increase in attacks that are targeted at specific geographic regions or languages.

Targeted Attacks

An example of a targeted attack is W32.Fanbot.A@mm, which is an IRC bot worm based on the HellBot worm. It attempts to propagate by mass mailing and exploiting the MS05-039 vulnerability. The worm also attempts to propagate through file sharing and P2P networks. It has a list of words, such as 'kazaa', 'share', and 'download', and searches for folder names that contain any of the words in the list. If a match is found, the worm copies itself to the folder. The list includes several Chinese words, which suggests that the author of the worm is aiming to infiltrate Chinese language operating systems.

Recently, users of online games have been targeted by malware. The attacker attempts to steal account information by using Trojans and can make money by selling items or virtual money through Real Money Trade (RMT) sites. Particular games tend to be popular in particular regions, hence malware targets these regions as well. Trojan.Okarag and PWSteal.Wayi are examples of Trojans that attempt to steal information from certain games that are popular in Asia, and close the windows of several security products, including Chinese security products. Some adware and spyware programs also target specific regions or languages.

W32.Antinny

W32.Antinny is a worm that targets the Winny P2P file-sharing network. It is the most notorious worm in Japan. Winny was developed by an anonymous author called Mr 47, and is available only for Japanese versions of Windows. In much the same way as other P2P programs, a lot of people use Winny for piracy.

When I first saw the W32.Antinny worm in 2003, I was interested in two points: the fact that it was the first worm for the Japanese P2P environment and the fact that it utilizes Japanese words for file names. Obviously this means that the worm cannot propagate globally and resides only on Japanese Windows with Winny – so, initially, I thought the worm wouldn't be a significant problem. However, I was wrong.

A few variants later, W32.Antinny had a payload that would cause significant social problems: information leaking. The worm searches many files, such as Office documents, text, email boxes, photos, and movie files on the compromised computer. It archives those files in a .zip file with a gripping name in Japanese and then copies the file to the upload folder, which allows other Winny users to search for and download it from the Winny P2P network. Therefore, Winny users were suddenly

finding lots of private information in the download files instead of what they were expecting.

Table 1 contains some examples of the information leaked by W32.Antinny as reported in the media last year. In some cases, highly sensitive information was leaked by the worm. According to Virus Bulletin's malware prevalence table[1], instances of W32.Antinny have consistently been very low. For example, the number of instances of W32.Antinny in October 2005 was just 11, representing less than 0.01% of all virus reports in that month. However, in November 2005, Microsoft reported that in one month it had removed more than 200,000 W32.Antinny files from 110,000 computers using the Malware Removal Tool in Windows Update[2]. The company also stated that a few hundred thousand machines were still infected with the worm. This must be the first verified case of a regional threat having propagated on such a large scale.

Date	Source	Information
December 9, 2005	Air Carrer	The password for restricted areas in an airport.
December 9, 2005	University Teaching Hospital	Information about three patients, including patient name and history for both the patients and their families.
December 8, 2005	Power Company	Nuclear plant meeting minutes and documents.
November 6, 2005	Public Hospital	Information about a dozen patients.
November 14, 2005	Prefectural Office	Personal details of 354 staff members, including names, addresses, and bank accounts.
November 17, 2005	Police Department	Home addresses of 33 police officers.
September 16, 2005	Power Company	Technical documents of a thermal power plant and customer information.
August 30, 2005	Heavy Industry Company	Maps, photos, and inspection report of a power plant.
July 21, 2005	Public Agency	Inspection report of a nuclear power plant.
June 27, 2005	Police Department	Documents of criminal investigations, including personal information about suspects and eyewitnesses.
June 23, 2005	Electric Company	Inspection reports and photos of 27 power plants, including seven nuclear power plants.

Table 1: Examples of information leaked by W32.Antinny.

Two Issues with Regional Threats

Acquisition and analysis of samples can be problematic where regional threats are concerned. If an antivirus company does not have a local office or support, it may be difficult to acquire enough samples of the threat. Most antivirus and security companies provide customers with a variety of ways to submit samples, such as by email, or via the Internet. However, most of these methods are presented in English or another specific language. If the user is not familiar with the language, they may hesitate to submit the sample through those means.

Global threats, such as W32.Sober and W32.Beagle, are reported by many people in many different countries. But regional threats are reported by a limited number of people in limited places. Such samples may easily be overlooked or assigned a low priority.

The next issue is analysis. As mentioned earlier, many regional threats contain languages other than English. An unfamiliar language in a threat can cause delay in analysis or even insufficient analysis. For example, PWSteal.Bancos.AA checks the Internet Explorer window text and starts logging key strokes if it matches with certain strings. Most of the strings are in English, but there are a few strings in Russian as well. These could easily be missed or ignored.

Technology can also be an issue in cases where we find files that are developed with particular tools. Trojan.Kakkeys was originally written in Ruby script language and converted into a Windows portable executable file by Ruby-Exerb[3]. Hot Soup Processor (HSP)[4] is another example. It is a kind of basic language and is also able to create Windows portable executable files. We found some tiny Trojans written in HSP. Both Ruby-Exerb and HSP were developed and used mostly in Japan. The portable executable file that is created with those tools contains huge runtime code so that the file seems clean at first glance. These files are likely to be false positives or false negatives.

Along with understanding foreign languages and technologies, analysts also need some knowledge of regional software usage. Winny is available only for Japanese versions of Windows and is the most popular P2P program in Japan. QQMessenger[5] is the most popular IM program in China.

Even without understanding the specific language or the software that the threat targets, analysts can analyse the threat and recognize what it is or what it does. But it is likely they will provide insufficient analysis, and give a lower priority to the analysis of the threat. It is reported that more than 4 billion accounts of QQMessenger exist and 20 million users are online at any one time[6]. If a new worm that targets only QQMessenger is released, it will be big problem – but only in specific regions.

Conclusion

Fortunately, only a few regional threats have become significant problems so far. However, anyone can obtain malicious code or ideas from the Internet and use them for profit-gain, and the number and variety of threats – including regional threats – will continue to rise. To gain profit, authors of malware don't need to create a threat that attacks computers worldwide. There is a lot of software that supports local languages only, and in certain regions (particularly China and Japan), such programs and services are more popular than ones that support only English.

AV and security companies need to be careful to acquire and analyse samples. If it's difficult to acquire samples from some regions, cooperation with other groups, companies or local organizations may be necessary in order to support customers in those regions. Even if a file looks clean, it's

possible that the file spreads rapidly but only on specific language operating systems, hardware, software or services we have never heard of.

References

[1] http://www.virusbtn.com/resources/malwareDirectory/prevalence
[2] http://www.microsoft.com/japan/presspass/detail.aspx?newsid=2504
[3] http://exerb.sourceforge.jp/index.en.html
[4] http://www.onionsoft.net/hsp
[5] http://www.tencent.com
[6] http://comm.ccidnet.com/art/1522/20051026/358525_1.htm

About Symantec
Symantec is the global leader in information security, providing a broad range of software, appliances, and services designed to help individuals, small and mid-sized businesses, and large enterprises secure and manage their IT infrastructure. Symantec's Norton™ brand of products is the worldwide leader in consumer security and problem-solving solutions. Headquartered in Cupertino, California, Symantec has operations in 35 countries. More information is available at www.symantec.com.

Symantec has worldwide operations in 35 countries. For specific country offices and contact numbers, please visit our Web site. For product information in the U.S., call toll-free 1 800 745 6054.

Symantec Corporation
World Headquarters
20330 Stevens Creek Boulevard
Cupertino, CA 95014 USA
408 517 8000
800 721 3934
www.symantec.com

04/05 10406630