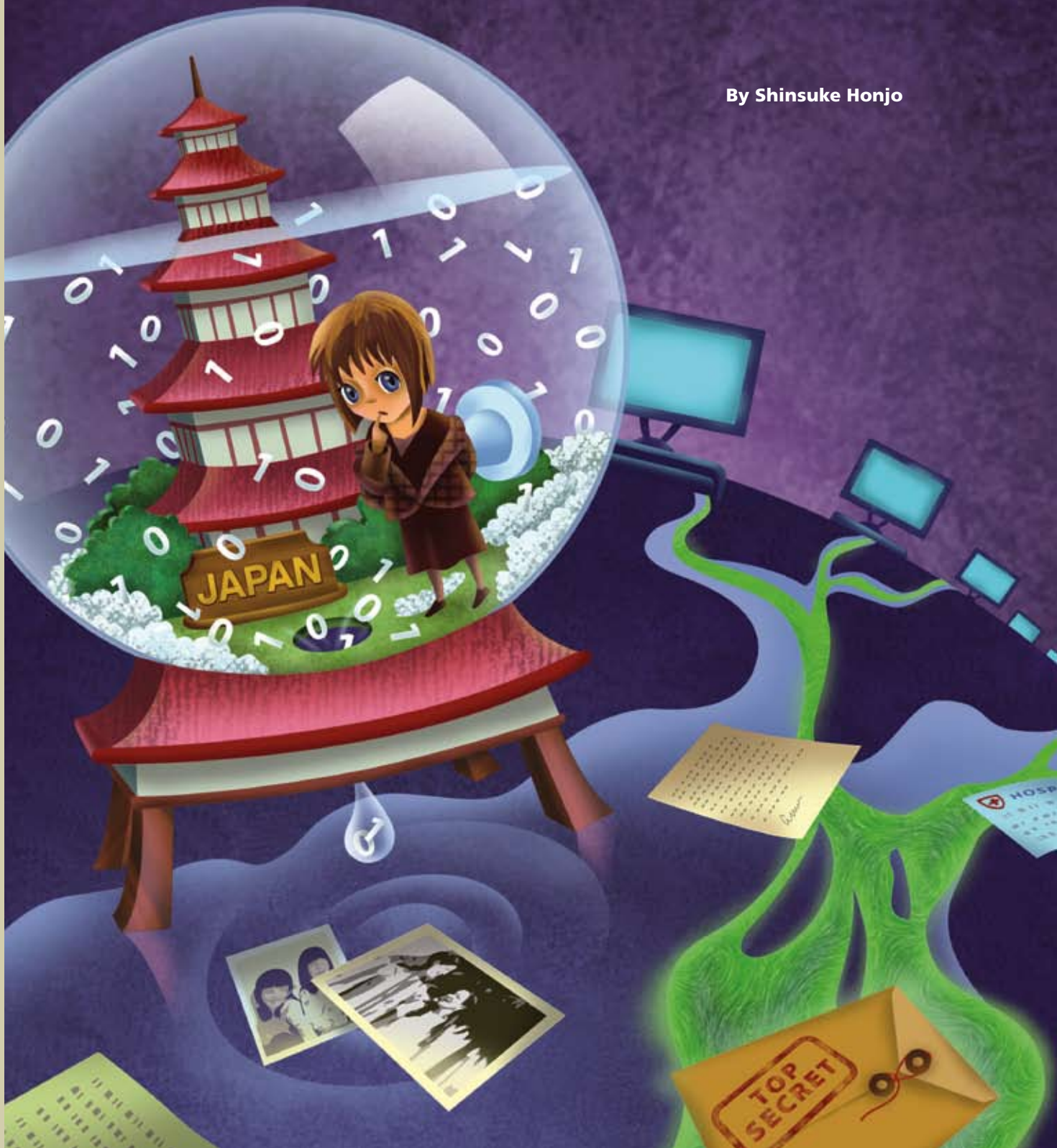


JAPAN: MALWARE SPREADS FROM PEER TO PEER

By Shinsuke Honjo



Japan faces many of the same threats that are popular in other countries. These include bot networks, password stealers, general exploits, and mass mailers. However, there is a class of malware that actively targets local Japanese applications and networks. In this article we'll take a look at the malware landscape that is unique to Japan.

Network threats

Winny is the one of the most popular peer-to-peer (P2P) network applications in Japan. It's well-known for its vulnerability to malware infections, which cause serious information leaks. It is also notorious for encouraging copyright law violations. As press interest in Winny-related incidents continues to grow, the activity emerges as a social issue that raises a debate over the pros and cons of using P2P applications.

Winny

Winny was developed in 2002 by Isamu Kaneko, a research assistant in computer engineering at the University of Tokyo. His goal for the P2P network was to provide effective file sharing and an anonymous communication channel.¹ Because of the anonymity, Winny is considered a perfect tool for exchanging illegal digital content; it is one of the major free applications in Japan. One study showed there were 290,000–450,000 users a day during the period from December 2006 to January 2007.²

In 2004, Kaneko was arrested by the Kyoto police for his alleged abetting of copyright law violation. In December 2006, he was found guilty and was ordered to pay ¥1.5 million (yen, about US\$13,136). His appeal to the Osaka High Court is pending.

P2P malware

As the Winny network has grown, an increasing amount of malware has targeted P2P users. The most common malware family that spreads via Winny is W32/Antinny .worm, which attempts to expose files on victim machines to the network share. Recent variants of this worm are also spread via other P2P networks, such as Share.

Trojans can be downloaded from the network. The Del-500 Trojan family deletes all potentially pirated files, such as picture, audio, and movie files from the victim's machine. Some variants show the picture in Figure 1 to make fun of victims who are using Winny.

Teasing victims



Figure 1: The Japanese message reads, "Even though Mr. Kaneko was found guilty, you are still using Winny. I really hate such people."

Data leakage increases

Malware that exposes files delivers a cruel blow to victims whose confidential or personal files are disclosed to other users on the P2P network. There has been lots of press coverage of these data leaks during the last four years. Figure 2 shows the number of media-reported incidents listed at one Japanese-language Web site.³ The numbers of incidents increased dramatically in 2006.

Data leakage sees rapid growth

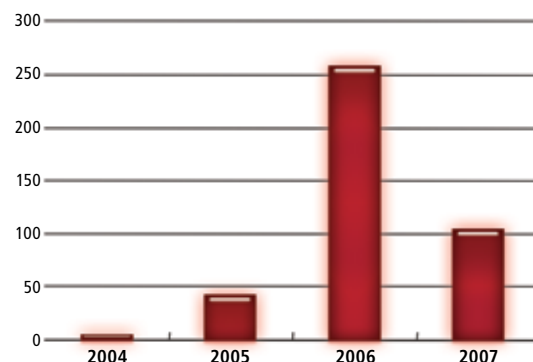


Figure 2: The number of the media-reported incidents of data leakage through P2P malware increased by more than six times from 2005 to 2006.

1 "Winny", Wikipedia. <http://en.wikipedia.org/wiki/Winny>

2 "Changes in the numbers of Winny nodes" (in Japanese), One Point Wall. <http://www.onepointwall.jp/winny/winny-node.html>

3 "Winny—Personal Data Leakage" (in Japanese), Winny Crisis. http://www.geocities.jp/winny_crisis/

Here is a list of the major P2P data-leakage incidents reported.

DATE	VICTIMS	DATA AT RISK
2005		
December	A business partner of a nuclear electric plant	3,000 files from the plant
2006		
February	Japan Maritime Self-Defense Force	Call sign of JMSDF fleets, muster roll, signal books, random-number list
February	Ministry of Justice	10,000 files, including personal information of imprisoned criminals
March	Okayama Police	Personal information of 1,500 victims and crime suspects
March	Cooperative bank	Data on 13,619 customers
April	Newspaper company	Data on 65,690 members
May	Japan Ground Self-Defense Force	Documents of the land-to-sea guided missile
May	Telecommunication companies	Data on 8,990 customers and 1,800 company files
June	Cable TV company	Data on 15,400 customers
November	Hospital	Data on 264,700 patients
2007		
February	Yamanashi Police	610 investigation files
June	Tokyo Police	10,000 investigation documents, including data on sexual victims
June	School teacher in Chiba	Data on 269 students
August	Hotel	Data on 19,700 customers

The media reports help reveal security breaches but they also have negative effects on the victims: Before the press covered the JMSDF case in February 22, 2006, no more than 14 users per day had downloaded the exposed files. After the report, however, the number of users who downloaded the files numbered 627 on February 23 and 1,188 on February 24. By March 2, 3,433 unique users had downloaded files.⁴

Expanding the trouble, those who attempted to download the exposed files without adequate security protection became potential victims of the malware. Some employees were reprimanded or fired. The worst case was that of one victim who committed suicide.⁵ These users not only infected their own systems with the malware and spread the files to the network, but they also exposed the data of other careless P2P users. Private pictures, movies, and email messages became objects of curiosity for many.

Government action

Some Winny incidents evolved into political and diplomatic problems. After the successive incidents of the Japan Self-Defense Forces, the prime minister ordered the responsible government ministries to prevent a recurrence. In 2006, the cabinet secretary announced that people should no longer use Winny. Allied countries that share

military secrets became alarmed when data on the Aegis naval combat system leaked from a naval officer via his wife's computer; security flaws in the JSDF's information management is an urgent concern. One consequence was that in August 2007, the media reported that the United States had temporarily suspended supplying the highly confidential parts for the Aegis destroyers to JSDF because of these data-leak incidents.

Motivation

It is clear that these malware writers are not motivated by money, as their malware just exposes or deletes files on the victims' machines. The malware also does not include state-of-the-art techniques for self-protection. In fact, this type of malware is too simple to do anything to establish or enhance the authors' reputations. One suggestion is that this class of malware might be targeting P2P users who violate copyright rules. However, some W32/Antinny variants have attempted to create a denial-of-service attack on the Japanese Association of Copyright for Computer Software site. This organization works to protect software copyrights. So it is uncertain what is driving the malware writers; mere curiosity is a possible motive.

Countermeasures

About 30 percent of P2P users have used their P2P-hosting computers for business purposes, according to one study.⁶ IT managers have long recognized this fact. After these information leak incidents, many companies are now refining their security policies to not allow employees to bring their private computers to the office. Providing enough computers for employees is one of the most effective solutions to prohibit the use of private (and unsecured) computers for business. In 2006, for example, the Ministry of Defense spent ¥4 billion to purchase 56,000 computers for the staff. Many companies have introduced tools to monitor the employees' computers and prevent the installation of unauthorized software—including P2P applications.

Targeted attacks

Another remarkable malware threat in Japan is targeted attacks against companies and governments. In these attacks, victims receive email messages with attachments that exploit vulnerabilities in local applications.

Ichitaro

A common application target for malware in Japan is the word processor Ichitaro, which is quite popular, especially in public institutions. When users open the specially crafted Ichitaro document with an unpatched application, the

4 "Press Release: 3 May 2006" (in Japanese), One Point Wall. <http://www.onepointwall.jp/press/20060303.txt>

5 "School teacher who leaked information through Winny committed suicide" (in Japanese), ITMedia. <http://www.itmedia.co.jp/news/articles/0706/08/news086.html>

6 "Survey on business users' usage of P2P applications" (in Japanese), NetSecurity https://www.netsecurity.ne.jp/3_6308.html

Trojan embedded in the document runs. The malware opens an innocent Ichitaro file that is also embedded, so users never see any suspicious behavior. We saw two zero-day attacks against Ichitaro in 2006, and another two in 2007. In all of these cases, backdoor Trojans cause the damage. Because these backdoors can control victim machines as well as monitor keystrokes, the motive of the attacks is to steal information from those companies and government organizations.

Freebies and Office

Recently, we observed targeted zero-day attacks exploiting local free decompression tools Lhaca and lhaz. These tools are not as popular as commercial applications, yet the attackers seem not to care about the number of potential victims. They target any applications or tools that they can exploit.

Microsoft Office also suffers from targeted attacks: We've seen email with Japanese subjects, text bodies, and attachments with Japanese filenames and text. If you think that email-borne malware that spreads all over the world has never been localized to Japanese before, those times have gone.

Targeted attacks do not employ only exploits. Executable files with the Microsoft Word icon try to slip by, carrying long filenames filled with many white spaces before the .exe extension. When a victim opens the fake Word file, the Trojan starts and opens an innocent embedded Word file—just as we saw in one Ichitaro example.

How far have the attacks spread?

These specially crafted documents are not as widely spread as other types of malware. According to research by Japan Computer Emergency Response Team, 6.5 percent of companies have received a spoofed email message with an attachment that appears to come from a business partner.⁷ Further, eight companies have gotten one of the malware-laden Word documents that the government is reported to have received. Some of the victims might not be aware of the attacks and the infections. The report also said that 25 percent of the companies are not sure whether they have received any of the spoofed messages.

Where did these spoofed messages come from? There is not enough evidence to answer the question. As they are spoofed and possibly sent by bot networks, it is not easy to trace the actual origins. However, one example shows at least some of them originate outside Japan. In some of the innocent Word files opened by these Trojans as a deception

the Word text was in Japanese; however, the text was in the Chinese font called SimSum. Because the Japanese never use this font, it is clear that these documents are created in the Chinese version of Word.

Dropping a Trojan

McAfee® Avert® Labs has received more than 40 samples of identified targeted attacks from Japanese customers during the past two years. Few of these are Trojans that are dropped by either specially crafted OLE documents or fake Word files. Most we identify as BackDoor-CKB, BackDoor-DKI, BackDoor-DJD, and BackDoor-CUX. We don't have enough evidence to draw firm conclusions but we can guess that these attacks may be carried out by a very limited number of authors.

Conclusion

The increase in the number of threats against Winny and other P2P networks has raised people's awareness of the need for security. However, some companies end up only slapping a band-aid on the data leaks from P2P networks. Japanese corporations and government offices need to deal comprehensively with the present danger by establishing clear policies along with thorough enforcement to put an end to P2P vulnerabilities.



Shinsuke Honjo is a virus research engineer with McAfee Avert Labs. He is an expert in Trojans, viruses, and exploits, and has analyzed

zero-day threats discovered in Japan. When he's not fighting malware, he enjoys practicing karate with his sons.



⁷ "Targeted Attacks" (in Japanese), JPCERT/CC http://www.jpCERT.or.jp/research/2007/targeted_attack.pdf