FEBRUARY 2008

McAfee®

Sage™

Security Vision from McAfee® Avert® Labs

Vol. 2 · Issue 1

ONE INTERNET, MANY WORLDS

Security Vision from McAfee® Avert® Labs • Vol. 2 • Issue 1

Contents

Sage

EDITOR Dan Sommer

CONTRIBUTORS Patricia Ammirabile, Christopher Bolin, Pedro Bueno, Toralv Dirro, Jeff Green, Shinsuke Honjo, Dirk Kollberg, Yichong Lin, Dr. Igor Muttik, Allysa Myers, Geok Meng Ong, Joe Telafici

ILLUSTRATIONS Carrie English

Acknowledgements

The editor of this issue would like to thank the people who helped make it possible. There are too many contributors to name them all, but we will cite the senior executives at McAfee, Inc. and McAfee Avert Labs who have supported this creation; our review board— Zheng Bu, Hiep Dang, Dmitry Gryaznov, David Marcus, Igor Muttik, and Joe Telafici; our author-researchers and their managers and teammates who have supported them with ideas and comments; marketing mavens Gloria Kreitman, Wilkin Ho, and Mary Karlton; PR pros Joris Evers, his worldwide team, and Red Consultancy Ltd.; our production agency, Sic 'Em Advertising, Inc.; Julia Cohn and her colleagues at RR Donnelley, our printer; and Derrick Healy and his mates in our Cork, Ireland, localization office, which has translated this publication into many languages. Thanks to all; we couldn't have done it without you!

—Dan Sommer
Editor

Address comments to Sage-feedback@McAfee.com.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com

WELCOME

LET'S TRAVEL **AROUND THE WORLD**

By Jeff Green

McAfee® Avert® Labs is proud to release the third edition of our security journal, *Sage*. We hope you will find it compelling. What is the mission of *Sage*, you ask? Simply put, this publication was created to ask "Why?"

In the first issue, we discussed the pros and cons of the open source paradigm and its effects on malware. In the second issue, we pondered the future of security. Is Microsoft Windows Vista more secure than XP? What are the security issues around radio-frequency identification technology? Will spyware take aim at mobile devices? These and the many other questions we have asked and answered have been met with agreement, annoyance, and even a little hostility in some cases. Regardless, *Sage* has been living up to its charter—to get people thinking outside their comfort zone in the world of computer security. (You'll find past issues of *Sage* on the white papers page of the McAfee Threat Center.[1])

The reasons and motivations for writing malware have changed greatly during the last several years. The Internet is bigger and more diverse than ever. As in a big city, there are good and bad neighborhoods that reflect the many cultures in the world. Malware, like the Internet itself, has undergone a remarkable shift—not only in why it is written but where and by whom. This past year has seen both the discussion of cyberwar (in Estonia) as well as the growth of a community of global users who have never before had access to the Internet. With new developments such as these, we have seen changes regarding where malware is written and whom it targets.

The cornerstone of Avert Labs is our worldwide team of security researchers. Their differing locales and cultures give McAfee a global understanding of malware and threats from day one of any outbreak. In this edition of *Sage*, some of Avert Labs' most senior researchers share their thoughts on the globalization of threats and malware. We travel from East to West in this edition: Our country-specific articles start in Japan and travel through China, Russia, Germany, Brazil, and finally the United States. In each country, we look at its unique threat landscape and discuss the types of malware and social engineering that are most effective in attacking those cultures.

We hope you enjoy your journey with the experts of McAfee Avert Labs. We look forward to reading your reactions at Sage-feedback@mcafee.com.

Jeff Green is senior vice president of McAfee Avert Labs and Product Development. He has worldwide responsibility for McAfee's entire research organization, located throughout the Americas, Europe, and Asia. He oversees research teams focused on viruses, hacker/targeted attacks, spyware, spam, phishing, vulnerabilities and patches, and host and network intrusion technologies. Green also leads long-term security research to ensure that McAfee stays ahead of emerging threats.

1 http://www.mcafee.com/us/threat_center/white_paper.html

ONE INTERNET, **MANY WORLDS**

By Joe Telafici

A couple of years ago I came to the conclusion that tracking country of origin or destination of a malware attack was a pointless exercise—useful only for marketing purposes—and had no real predictive or prescriptive value. This perception was engendered by a couple of fairly recent (at that time) occurrences:

- Mass-mailers, especially W32/SQLSlammer.worm, proved that you could infect basically the entire Internet in a matter of minutes.
- In an attempt to avoid attracting the attention of law enforcement officials, malware writers stopped including useful clues in malware about its origins.
- The primary motivation for malware at this time was ego: the more machines infected, the more fame.

Contrast this to the situation in the mid-1990s, when threats started in one part of the world and took weeks to reach other parts. Moreover, the threat was likely to contain strings or resources very clearly pointing to the country of origin, as well as to the intent of the author.

However, in 2002 through 2004, threats such as Klez, Bugbear, SQLSlammer, Blaster, Sobig, Nachi, MyDoom, Netsky, and Bagle were global phenomena that hit virtually the entire planet in the space of only a few minutes to a few hours. For a while, it seemed like the global dominance of Microsoft Windows as a platform, the explosion of broadband usage throughout the world, the ease of finding vulnerabilities, and the application of social-engineering techniques would ensure that no one connected to the Internet was safe for very long from any threat.

During this period of intense malware replication, a trend began that, frankly, the anti-virus community as a whole failed to notice in its early stages. We discussed this phenomenon in our previous edition, "The Future of Cybercrime."[1] During 2004, an explosion of malware creation occurred that was larger in scale, but smaller in breadth, than anything seen to date. Bots, password stealers, and other static malware began to appear at alarming rates. Unlike the replicating viruses that characterized the last flurry in what I call the "digital graffiti" stage of malware development, these threats almost never rose to a global level for a variety of reasons. The main reason was that malware authors were not interested in drawing the kind of attention that the large-scale virus writers of Netsky and Sasser attracted from the law enforcement community.

Whether as a side effect, symptom, or cause of this low-and-slow paradigm shift, for these reasons malware has become more regional or localized in nature during the last two to three years:

- Better social engineering is now required for seeding attempts and to lure people to drive-by sites, phishing sites, or hosted malware. To appear legitimate enough to fool wary computer users, the kinds of egregious typos made by nonnative speakers are too obvious today.
- More vulnerabilities are being found now in more obscure software, including in some localized software (such as Ichitaro, a word processing package popular in Japan) due to the increase in vulnerability bounties, both from security vendors and from attackers.
- Malware authors show increased interest in limiting the sources of attacks to countries where law enforcement is likely to be lax.
- Malware authors are fond of attacking niche markets, whether to exploit a particular resource or to avoid law enforcement.

You'll see a number of examples of these kinds of country-, language-, company-, or software-specific attacks in the articles comprising this issue.

Although we can't ignore the motivations of the malware authors in focusing attacks, this activity takes place in a global environment that is quite different from that of even a few years ago. Political, economic, and social forces shape everything and have contributed to a whole underground economy and market whose diversification, breadth, and scope are larger than ever before.

One of the most significant factors increasing the possibilities for attackers is the growth in global broadband penetration. With broadband computers connected full-time to the Internet, the opportunity to attack systems in real time and to use spare bandwidth capacity on compromised machines for further attacks is a resource too tempting to ignore. But broadband penetration varies widely across the globe, with estimates ranging from nearly 90 percent in South Korea, to about 50 percent in the United States, to significantly less in parts of the developing world.

The expansion and diversification of the role of computers in modern society likewise contribute to expanded opportunities for those seeking to capitalize on cybercrime. From staggering growth in cell phone usage (upwards of 20 percent annually, with more than three billion subscribers expected by 2010), to online banking usage, online gaming, and e-commerce in general, there are enough money, vectors, and targets to ensure that the unscrupulous have plenty to keep them busy. But this technological storm is proceeding at a different pace in different parts of the world. For example, mobile technology is well ahead of the rest of the world in Asia, while online banking is at its most robust in Brazil, and online gaming is a cottage industry in China.

To some degree, cybercrime is a natural extension of what is probably among the world's oldest professions: theft. But we can't ignore the economic realities in many parts of the world that make this an attractive option. Particularly in Eastern Europe, where technical skills were widely taught during the Cold War but economic opportunities are limited, and in Asia, where population growth has stretched strong economic performance to the limits, the motivation to engage in questionable or illegal behavior increases. As a former virus writer remarked to me once, "I had to do something to feed my family."

As a former virus writer remarked to me once, 'I had to do something to feed my family.'

And it may not merely be the criminals getting in on the act. As the recent and ongoing distributed denial-of-service attack on Estonia's infrastructure demonstrates, political "hacktivists" may have an increasing interest in the Internet

1 "Sage," April 2007. http://www.mcafee.com/us/threat_center/white_paper.html

as a battlefield or potential theater. Whether nation states or military organizations have a similar interest is an unknown, though likely, assumption.

Given the variety of roles, motivations, and advantages of today's cybercriminals, how our society reacts is crucial to the maintenance of law and order in the Wild West of the Internet. It has become increasingly clear that human society is far from homogenous in its preparedness for and reaction to cybercrime. Here at McAfee® Avert® Labs, we work with a variety of law enforcement agencies in countries all over the world, and it is apparent to us that the legislative, financial, and technical resources available to crime-fighters in different parts of the world can be like night and day. And because it is rare for an attack to start, travel through, and end in the same country, this impacts our ability to impede or stop malware authors and crackers even when it is dead obvious who is involved. This inability to coordinate internationally is one of the largest factors contributing to the low-risk environment that characterizes cybercrime today.

Political 'hacktivists' may have an increasing interest in the Internet as a battlefield or potential theater.

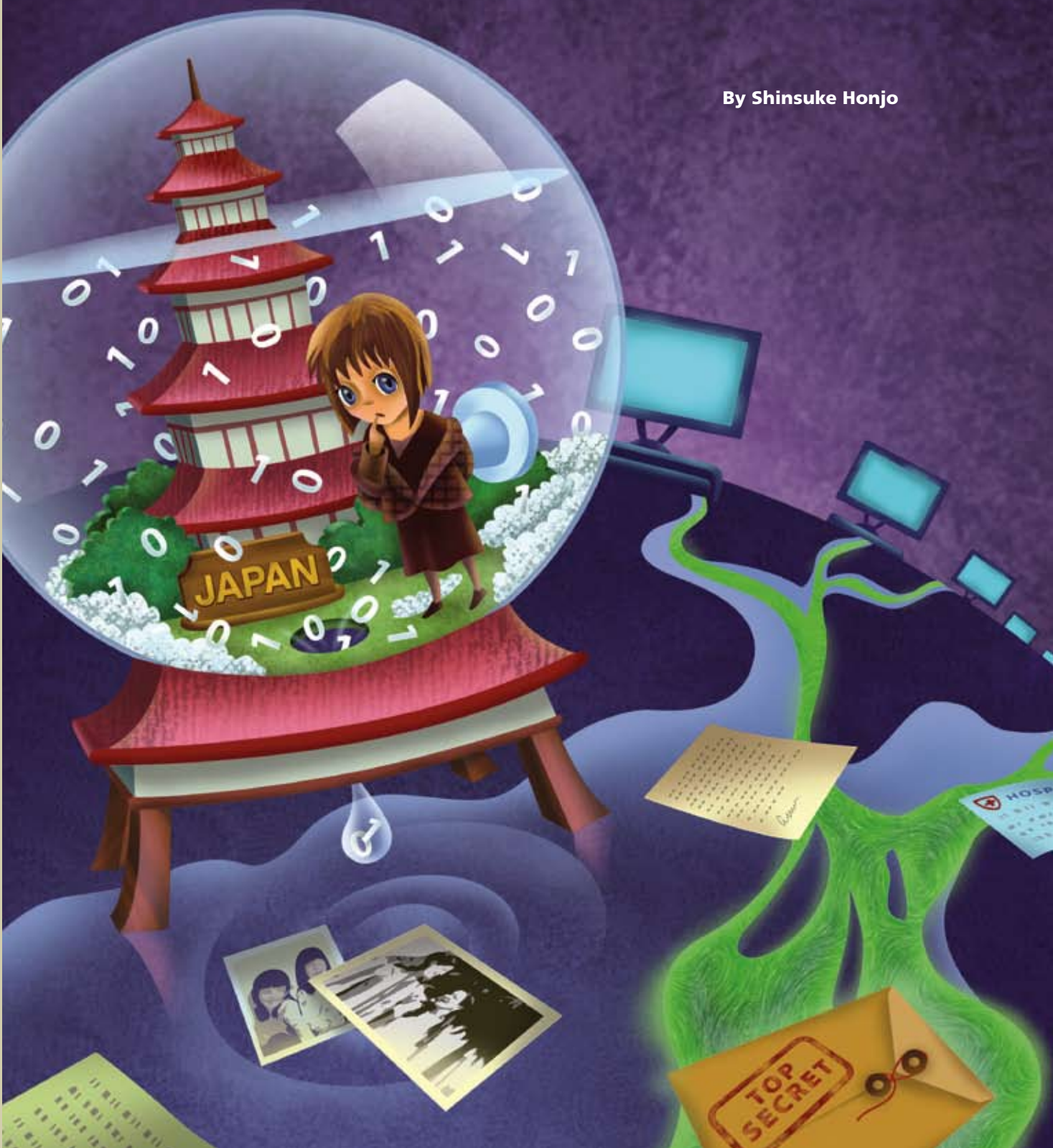
In the following pages, you will hear from some of the world's most talented researchers based in, or with close ties to, the country whose security situation they are describing. I hope that you find the articles educational, informative, and thought provoking. Although every nation faces different challenges in today's interconnected personal and business world, you cannot avoid affecting and being affected by the situations next door and across the sea.

Joe Telafici is Vice President of Operations for McAfee Avert Labs. He has management responsibility for researchers in 16 countries on five continents. With more than 10 years of experience at Symantec, CyberMedia, Tripwire, and McAfee in both consumer and corporate security products, Telafici is responsible for coordinating McAfee's response to global security threats, as well as the daily production of security content, customer support tools, and research into next-generation threats and technology. He has briefed Congress on technology issues, is quoted regularly in the press on virus- and spyware-related issues, and has been published in *Virus Bulletin*. Telafici is from New Jersey and, although he misses the New Jersey Devils, he gets better beer and coffee in McAfee's Beaverton, Oregon, office.

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

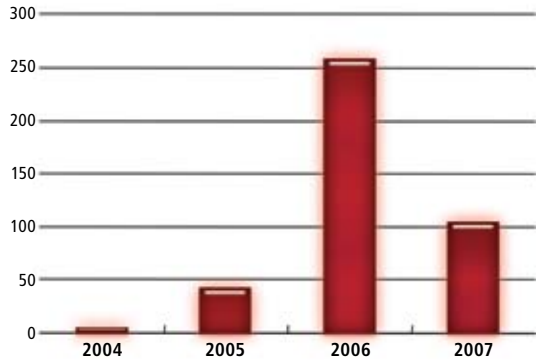


Figure 2: The number of the media-reported incidents of data leakage through P2P malware increased by more than six times from 2005 to 2006.

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 polices 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

CHINA:

PAINTING **THE THREAT** LANDSCAPE

By Geok Meng Ong and Yichong Lin

Few events today are changing the world's political and economic landscape quite like China's rapid rise among the great powers. In 2006, China's Gross Domestic Product (GDP) grew by 10.7 percent, the highest figure in 11 years; this occurred only one year after China overtook the United Kingdom as the world's fourth-largest economy. At this time of tremendous growth and change, China's Internet threat landscape is also changing rapidly. Why are we seeing this increase in malware coming from and moving into China?

Rapid Internet growth

In 2007, 12 percent of this enormous nation—37 percent of all Internet users in Asia, or 137 million people—were online. Dr. Charles Zhang, chairman and CEO of Sohu.com, a Chinese Internet portal, offers his interpretation of what this means.[1] Chinese Internet users spend almost two billion hours every week online, he says, or more than 15 times longer than American Internet users. He attributes this phenomenon to the lack of a free press in conventional media in China. In September 2006, Chinese lawmakers passed a new ruling requiring all foreign news agencies to release information through the state-owned Xinhua News Agency.[2] China's Internet population skyrocketed at an effective growth rate of 509 percent during the last five years. In comparison, the world has seen a 200 percent and the United States a 121 percent effective growth rate during the same period.

Booming local Internet apps

In the age of the Internet boom, there is a need to grow localized content, as the audience develops an appetite for more.

Online gaming

A quarter of all Chinese Internet users are online game players; as of April 2007, 33 percent of players were between 19 and 22 years old. Online gaming addiction is burning across China like wildfire, so much so that the Chinese government introduced a unique "Game Fatigue Regulation" system: Each time an under-aged gamer plays for more than three hours in a day, he or she loses "experience points" in the game. Playing beyond five hours a day costs a gamer all the points. In today's 31-million-player gaming market, the business of online gaming has a new meaning.

Virtual commodities

Real Money Trade (RMT), the concept of trading virtual gold or goods collected from computer games for real money, is rapidly catching on with online gamers. The popularity of online gaming in China creates a ready market for RMT, which industry observers estimated to be worth up to US$900 million. A quick search of Chinese keywords "Gold" and "World of Warcraft" on China's number-one auction portal, Taobao.com, yields 32,891 finds; with "Power Leveling Service" and "World of Warcraft," we got 19,982 results.

The sellers include gaming workers or "gold farmers," who play online games day and night to harvest virtual currency, goods, or magic spells in "virtual sweatshops." Each gold farm can employ hundreds of young workers, each making up to US$250 a month.[3] It is estimated that there are more than 100,000 such gamers in China supplying virtual commodities to both domestic and foreign demands.

Online gaming addiction is burning like wildfire, so much so that the Chinese government introduced a unique 'Game Fatigue Regulation' system.

1 "China Surpasses U.S. In Internet Use." Forbes.com. http://www.forbes.com/2006/03/31/china-internet-usage-cx_nwp_0403china.html

2 "The Administration of Release of News and Information in China by Foreign News Agencies," Xinhua. http://news.xinhuanet.com/politics/2006-09/10/content_5072446.htm

3 "Ogre to Slay? Outsource It to Chinese." The New York Times. http://www.nytimes.com/2005/12/09/technology/09gaming.html?ex=1291784400&en=a723d0f8592dff2e&ei=5090

Instant messaging

RMT is not limited only to online gaming. Instant messaging (IM) in China is more than what the name implies. Beyond instant messages, it has developed into a platform providing telephony service, entertainment, email, gaming, and remote assistance. To sell virtual amusements to Chinese Internet users, Tencent retails one virtual QQ coin for ¥1 (1 yuan, about US$0.13) on the street. With few restrictions when initially introduced, the QQ "currency" has been traded for real currency in black markets, creating an avenue for money laundering and making the RMT of QQ accounts and currency profitable. Even online casinos and pornography sites trade QQ coins, raising an alarm with the Chinese authorities due to its wide abuse.

In a survey conducted by the Chinese media, 70 percent of users have had their QQ account stolen at some time.[4] Tencent, owner of the QQ network, recognizes these increasing threats and provides free security education and services on their Web site.[5]

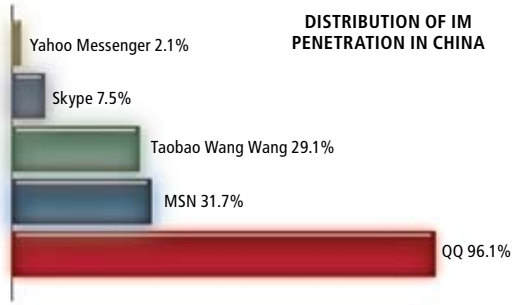


Figure 1: Tencent QQ dominated the Chinese Internet messaging market in 2007.[6]

Anonymous payment modes

To widen the scope of money laundering and RMT, most people in China do not have a credit card or a personal computer to make online payments. Many Chinese gamers hang out at Internet cafés, and prepaid game cards are the preferred payment method not only at the cafes, but also in online stores and gaming centers. Without the need for registration, prepaid cards are virtually anonymous. In real-world cases, cyberthieves with stolen online bank accounts or credit numbers buy the prepaid cards and sell them online. Cybercriminals have also penetrated prepaid card networks to steal prepaid card numbers. The anonymity and wide use of prepaid cards increase the complexity for law enforcement agencies to track down rogue transactions and cybercrimes.

Malware activities in China

We have seen how virtual commodities trading has become a multimillion-dollar business, and we have seen enterprising gold farmers making use of low-cost labor to increase their gains. It's no surprise that those with access to the technical know-how to achieve these goals in a bigger and faster way are using malware. As we have seen, the majority of malware originating from Chinese domains are password stealers. At first targeting the main platforms—QQ, World of Warcraft, Lineage—today password stealers cover every possible target of RMT.

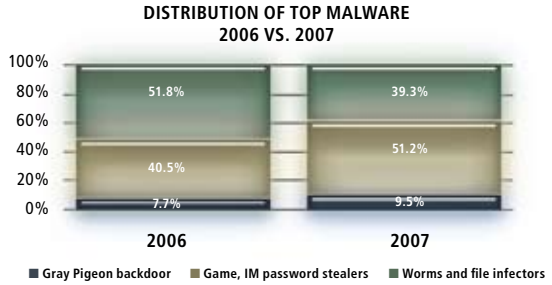


Figure 2: The last year has seen a big increase in password stealers in the Chinese market.

McAfee® Avert® Labs reported an increasing trend in game password-stealer threats in 2006 that peaked in October, and the trend is evidently continuing in 2007. From the earliest PWS-QQPass, PWS-WoW, and PWS-Lineage Trojans, we now see "cocktails" such as PWS-OnLineGames and PWS-MMORPG targeting multiple online games and communities. Multivector worms such as W32/Fujacks and Web exploits continue to increase the opportunities to commit crimes.

Cybercriminals are not necessarily expert hackers. As in traditional sales channels, they follow a chain of supply and demand.

4 "Tencent Introduces QQ Security Card," Sohu.com. http://digi.it.sohu.com/20070906/n251998008.shtml

5 "Tencent Safe, " Tencent. http://safe.qq.com/

6 "QQ Extends Its Market Leadership in 2007," "Taobao Wangwang Catching Up With MSN Q1," iResearch. http://www.iresearchgroup.com.cn/Consulting/instant_messenger/DetailNews.asp?id=65222

Organized crime

With Chinese malware, we see a massive Internet community and RMT market supporting its growth; substantial profits provide the means for exploits to get better and bigger. China's Computer Emergency Response Team (CNCERT) noted, in its recent half-yearly report, an increase in Chinese Web sites used for phishing and the hosting of malicious code; the increase alone is greater than the overall figure for 2006.

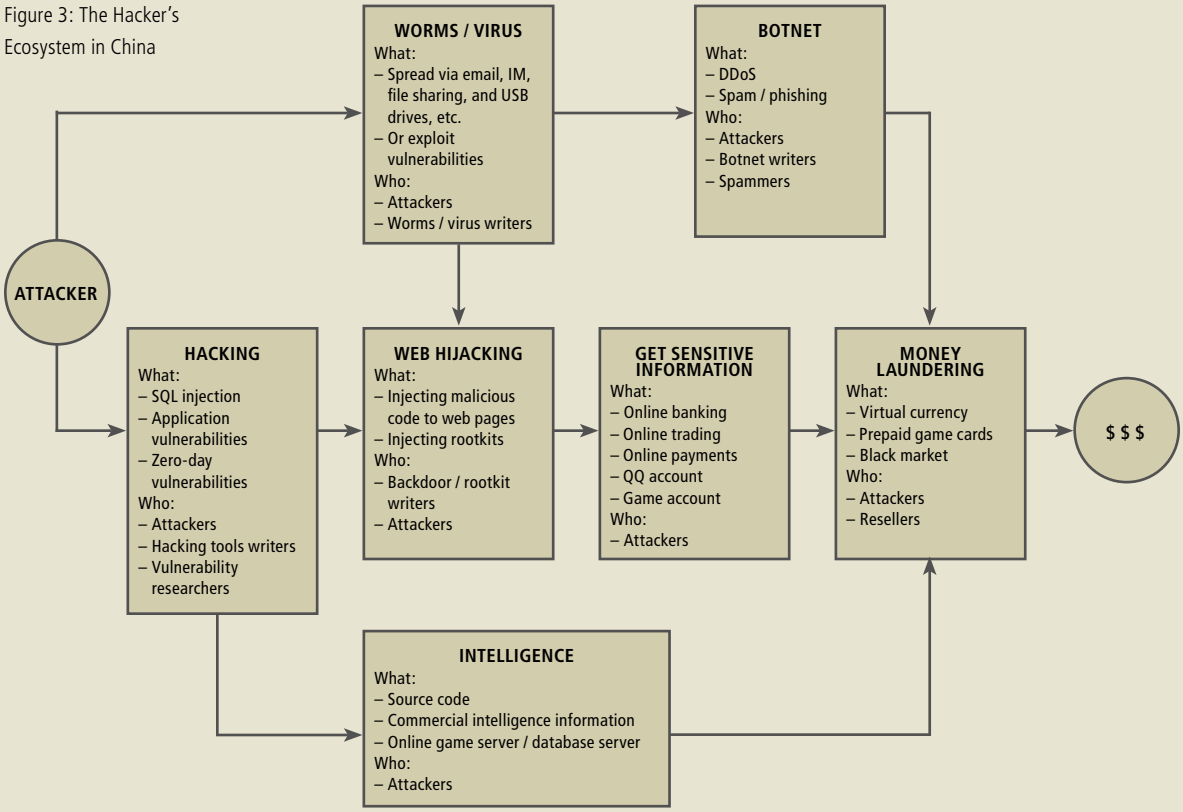
In 2007, McAfee SiteAdvisor™ has found 0.2 percent of all Web sites registered in China to be hosting exploits; that's more than twice the global average. These sites include a good mix of .org.cn, .gov.cn, .com.cn, .net.cn, and other domains. Many of these may be legitimate sites that have been hijacked by criminals to host malicious code, allowing unaware users to risk infection while browsing their regular "clean" sites. What is more alarming is the wide use of zero-day exploits such as Exploit-AniFile.c. File-infecting worms such as W32/Fujacks and man-in-the-middle or address resolution protocol–poisoning threats such as NetSniff act as catalysts for wide propagation.

Cybercriminals are not necessarily expert hackers. As in traditional sales channels, they follow a chain of supply and demand. In February 2007, Xinhua reported a group of 50 resellers in Zhejiang province helped sell stolen user accounts and virtual commodities from Li Jun (the W32/Fujacks author) and his accomplices. They were also reportedly part of a syndicate to perform phishing and release adware to commit fraud. None of the resellers were computer experts; one of them worked as a chef in a restaurant.

In an organized cybercrime chain, various tools and roles typically work hand in hand. Exploits target unpatched vulnerabilities to provide an entry for intruders, bots and backdoors provide command and control, and password stealers and spyware collect sensitive or profitable data.

BackDoor-AWQ.b, or Gray Pigeon backdoor as it is called by its creators, has been commercially marketed and sold as a "remote administration tool" on its Web site since 2003; it costs just ¥100 (US$13) for an annual subscription. Users get updated versions with enhanced features such as rootkits, distributed command and control, keylogging, etc. The site was shut down by its owners in March 2007, following the arrests of the W32/Fujacks authors. Security analysts worry that this group could be moving its operations underground, and will be even harder to track.

Figure 3: The Hacker's Ecosystem in China



Talent pool vs. unemployment

In Beijing alone, the number of university graduates reached an all-time high of nearly 200,000 in 2007. However, only 43 percent are expected to be employed. In rural regions, unemployment can be worse. In fact, many "gold farmers" came from rural and suburban China, working 12-hour shifts and making US$250 a month, which is a pretty good wage in the poorest parts of the country.

Li Jun, 25, having been unsuccessful in securing a job after graduating from a computer school in 2005, desperate for money, and armed with malware-writing skills, has since authored and released W32/QQPass.worm and W32/Lewor, in addition to the now infamous W32/Fujacks.worm. He sold the source code of W32/Fujacks to more than 120 buyers, making a profit of over US$13,000 in a city where the per capita annual salary is around US$3,000. There could easily be more young people like him. Hackbase.com is one of largest "hacker" training Web sites in China; they claim to have more than 10,000 members. At sister site hackerbase.net, they explicitly offer paid hacking services.

Government policies

In September 2007, Li Jun was convicted by the Chinese court to four years in prison. Will that deter other malware authors from committing cybercrimes? During the trial, Li Jun's lawyer presented an offer letter from an IT company in Hangzhou for the position of CTO. He claimed that there were ten other offers from various companies to pay Li Jun more than ¥1 million (US$133,000) annual salary. In fact, the spread of worms in China has not declined following these arrests in early 2007. The fact that the W32/Fujacks source code was sold didn't help.

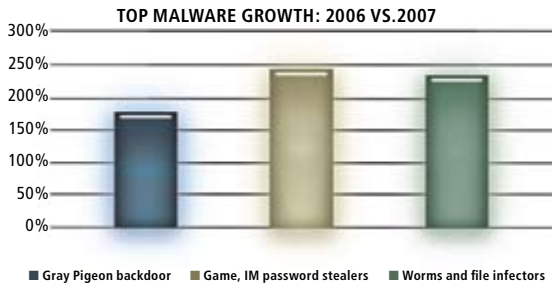


Figure 4: Password stealers are growing at a faster rate than other malware.

Have recent changes been too overwhelming in China? At least in Internet security, we can see that the rapid adoption of technology has been far quicker than government policies, corporations, and traditional culture can catch up.

ICBC, the largest state-owned commercial bank, reported e-banking transaction volume hitting ¥170 billion (US$22.6 billion) in the first quarter of 2005 alone, up from only ¥15.4 billion (US$2 billion) in 2000. In 2005, the China Banking Regulatory Commission (CBRC) revealed that

Analysts reportedly said that the popularity of QQ currency has reached a point where it threatens the value of the yuan.

policies passed in 2000 were not able to regulate the management and monitoring of the additional risks associated with Internet banking. New "E-banking Business and Relevant Security Evaluation" criteria were introduced by CBRC in 2006 to cover the new risks in the virtual world.[7]

Now that QQ currency has been available for five years, Chinese regulators have finally ordered restrictions on its circulation—after concerns of abuse and money laundering. Analysts reportedly said that the popularity of QQ currency has reached a point where it threatens the value of the yuan.

What's next?

We have seen how the Chinese threat landscape has been shaped by its unique local cultures, politics, and economics. Regulation and controls have been playing catch-up at a peak of China's growth and changes. The popularity of the Internet, combined with widespread unemployment and a large talent pool, has created an environment that encourages malware writers. Current conditions have pushed these hackers to become cybercriminals going for the money.

On the positive side, the recent conviction of cybercriminals such as Li Jun shows that Chinese lawmakers are taking cybercrime seriously.

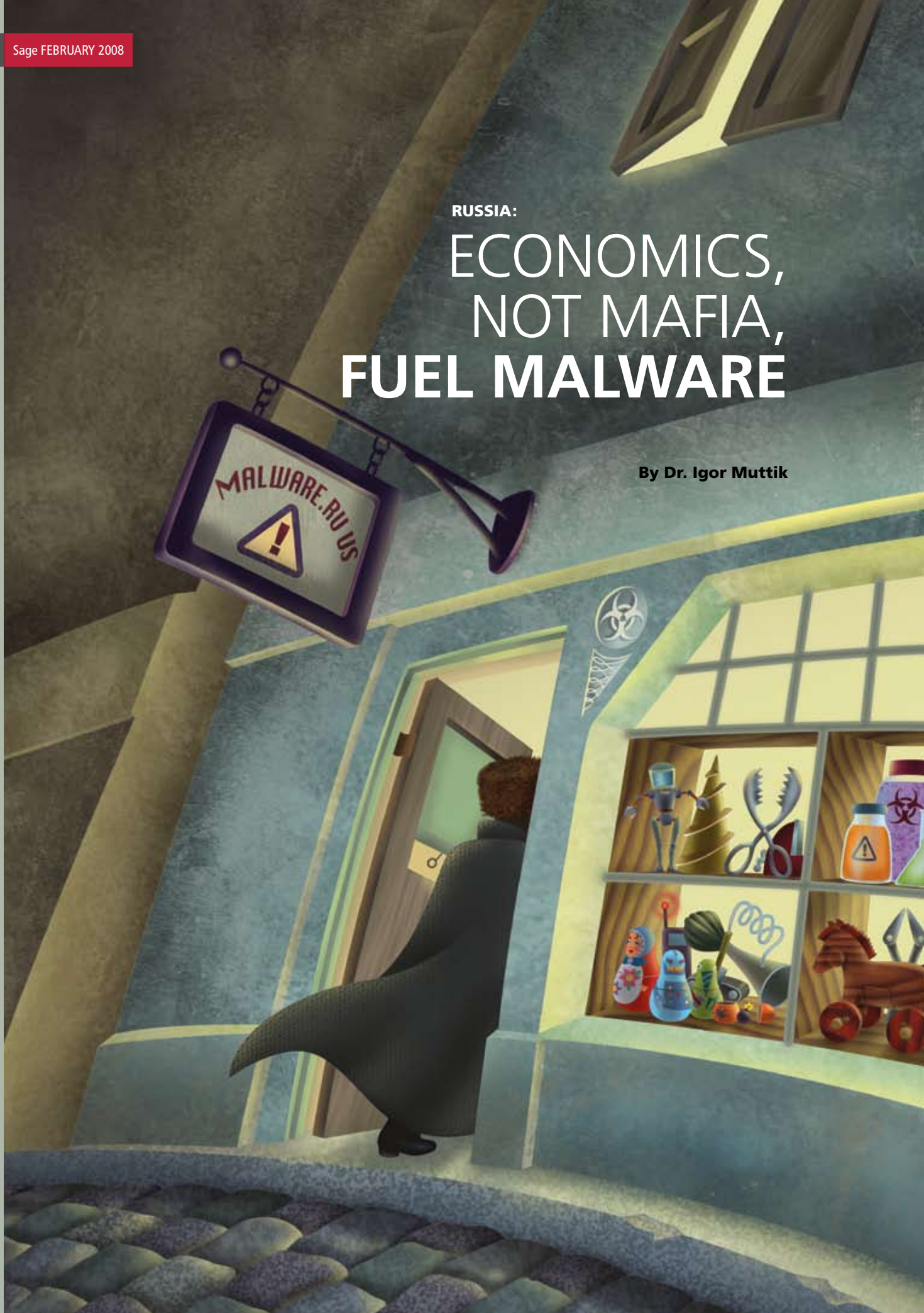
7 Q&A with China Banking Regulatory Commission. http://www.cbrc.gov.cn/chinese/home/jsp/docView.jsp?docID=2243

On the positive side, the recent conviction of cybercriminals such as Li Jun shows that Chinese lawmakers are taking cybercrime seriously. The impact of local cyberthreats has also hastened the development of government policies and local applications to introduce new measures to deter cybercrimes. The only way to ensure the continual growth of this market is to develop the necessary security measures to protect its users.

Geok Meng Ong manages a team of security researchers in the Asia Pacific and Japan regions for McAfee Avert Labs. By chance, he discovered the dark side of the cyberworld, which fuelled his passion for security research. In the spirit of Singaporean kiasu-ism,[8] he joined McAfee to master the zen of world-class security. A hands-on researcher himself, Ong focuses on malware heuristics and vulnerability research, and is often quoted in the media for his analysis of new malware trends and exploits that are prevalent in this region.

Yichong Lin is a security researcher at McAfee Avert Labs. He focuses on intrusion-detection technology and vulnerability research. Both authors have studied the Chinese security market for many years.

8 "The calculating obsession that inflicts people who believe that they must get their money/time/effort's worth (the greater the returns the better!)" Urban Dictionary. http://www.urbandictionary.com/define.php?term=kiasuism



RUSSIA:

ECONOMICS, NOT MAFIA, **FUEL MALWARE**

By Dr. Igor Muttik

Many assume that the mafia and the secret police service (FSB, formerly known as KGB) must stand behind the attacks coming from Russia. But are these organizations really the prime movers? We'll answer that question in this article, but first we need to take a short look into the history of local malware development and the main forces behind it. We shall discuss current laws, as well as the successes and failures of law enforcement agencies. We shall also dive into the black market to know what is on offer and what one might expect to pay for malware, malware builders, associated tools, and the functionality they offer. Finally we'll make a few predictions about how this is likely to evolve.

A short history of malware development

The traditional focus of education in the Soviet Union was more on technical and practical sciences than on the humanities. For that reason in Russia and the other former republics of the U.S.S.R. there are many highly skilled young people with advanced knowledge of mathematics, computing, and programming. The combination of relatively low salaries, high unemployment, and wide availability of networked computers makes malware development an area that attracts quite a lot of people. Also, as in many other countries, "hackers" are perceived by the public as exceptionally clever individuals. Consequently, malware writers carry the aura of being special.

In the past Russian programmers created many sophisticated viruses. One of the most notable was a multipartite Zaraza virus (a.k.a. 3APA3A), which used a novel technique of infecting disks by creating a duplicate of the io.sys file. This virus forced a redesign of anti-virus engines! Another exceptional virus—W32/Zmist—was written by a notorious, prolific, and imaginative virus writer who calls himself Z0mbie. This parasitic virus decompiles and reassembles files upon infection so that the virus is seamlessly integrated inside the host. Security researchers from all anti-virus firms unanimously agree that this technique is the hardest to detect.

In recent years financial motivation has played an increasing role in driving up the production of malware.[1] Spam and spam tools are also in demand. These areas also intertwine; for example, botnets are frequently used for spam distribution.

At the same time, there are many organizations in Russia that use low-level skills for legitimate purposes: for instance, top-notch vulnerability research (www.securitylab.ru) or widely used copy-protection technologies (http://www.star-force.com). The world-class software analysis toolkit IDApro (www.idapro.ru, www.idapro.com) is the leading program for reverse-engineering. Software protectors AsPack and AsProtect (www.aspack.com, www.star-force.ru) are frequently used to package commercial software. And, naturally, there are some gray sites (http://wasm.ru, www.xakep.ru) devoted to disassembling and modifying software, including an excellent resource for reverse-engineering (http://www.cracklab.ru). The skills used in these areas may come in very handy for malware development; a very high return on investment for computer crime could be the magnet that attracts many young, inexperienced people.

So what's stopping these young programmers from turning to crime? Let's have a look at the legal controls in this space.

A very high return on investment for computer crime could be the magnet that attracts many young, inexperienced people.

1 "Money changes everything," Sage Vol. 1, Issue 1, Page 13. http://www.mcafee.com/us/local_content/white_papers/threat_center/mcafee_sage_v11_en.pdf

Current laws

Russian laws covering crimes related to computing came into force in June 1996 (in Chapter 28 of the Criminal Code of the Russian Federation). Some amendments were made in November 2001. There are three key paragraphs, and they cover the following crimes (this is not an official translation):

#272) Unauthorized access to computer data if that causes a loss, blocking, modification, copying, or disruption to the operation of a computer, system, or a network.

#273) Deliberate creation of computer programs or change of existing programs if that causes a loss, blocking, modification, copying, or disruption to the operation of a computer, system, or a network. Also using and distributing corresponding programs or computer media with such programs.

#274) Interfering with the normal operation of a computer, system, or a network by a person who has access to a computer, system, or a network that causes a loss, blocking, modification, copying, or disruption to the operation of a computer, system, or a network if this causes significant harm.

Penalties start from a mere fine or a community service, but for crimes that cause serious consequences (or if they were committed by an organized group) punishment can include imprisonment for a period of four to seven years.

In 2006, the Russian legislative body—the Duma—enacted laws protecting personal data (http://www.akdi.ru/gd/proekt/097697GD.SHTM) and data protection (http://www.russianlaw.net/law/laws/t3.htm). The former requires consent from a person for using personally identifiable information (with very few reasonable exceptions). This is very much in line with common international practice.

In July 2006 lawmakers also passed a law that requests advertisers to follow the "opt-in" model of distributing advertisements. That temporarily caused a drop in spam levels in Russia, but in about four months the volume returned to its usual level—about 80 percent spam in normal email traffic (http://www.cnews.ru/news/top/index.shtml?2007/02/19/236529).

As we can see, legislation is on the rise and is gradually covering the hot spots. But does it work in the area of malware production?

Successes and failures of law enforcement

There is a Russian saying that the severity of the laws is offset by the fact that it is not necessary to obey them. Thus we need to perform the acid test and check to see how these laws are applied in practice.

As with all high-technology crimes, the laws are always a bit behind current developments in their misuse. Russian computer crime laws, though, are fairly generic and were used to prosecute one spammer (http://www.ifap.ru/eng/projects/as02.pdf) even though the implications of spam were not in the thoughts of lawmakers when the respective laws were first enacted.

Another hacker was prosecuted—under paragraph #273—for unauthorized modifications to a computer system (www.internet-law.ru/intlaw/crime/tumen.htm), and a student was charged with running a Web site that offered about 4,000 malware samples for download.

Concerning international computer crime, a court in the Saratov region, 530 miles southeast of Moscow, has sentenced three Russian hackers to eight years in prison each, as well as a $3,700 fine (http://www.whatreallyhappened.com/archives/cat_computersinternetsecurity.html). Their crime was attempting to extort $4 million from world Internet companies.

Computer-based crimes frequently cross national boundaries. Sometimes the criminals do so, too. When they do, they become subject to local laws and can be apprehended and prosecuted. In August 2007, U.S. authorities reported an identity theft ring that specialized in targeting rich Americans. The head of the group was arrested in New York when he flew from Russia to the States to retrieve $7 million in gold that he thought had been purchased with money stolen from one of his victims (http://www.informationweek.com/security/showArticle.jhtml?articleID=201800899).

Attacks across borders on Web servers are quite common. They are usually made to compromise the servers and to plant malware (or malicious links to malware). In one case Web administrators from several countries noticed attacks originating from the same network registered in St. Petersburg.[2] Such a coincidence indicates that the frequency of this activity is quite high.

At the August 2007 Internet Security Operations and Intelligence III conference, in Washington, one of my colleagues heard that the overwhelming majority of major e-crime scams appear to be linked to Russian or ex-Soviet cybercriminals.

2 "Go Away, Russian Business Network!" Dusting My Brain. http://dustingmybrain.com/archives/002375.html and "More on the Russian Business Network!" Dusting My Brain. http://dustingmybrain.com/archives/002379.html

In July 2007 the Russian exploit package MPack caused massive compromises of Web servers in Italy. (You can read a nice graphical description of how this works at Symantec's blog.[3]) Dealing with such attacks requires the close cooperation of lawmakers, law enforcement agencies, and ISPs across national boundaries—a monumentally difficult task.

Another serious problem that law enforcement agencies face is that finding resources and funding for computer-crime units is far from trivial. (This is a common problem all over the world.) Because the authorities are not as successful in combating computer crime as people would expect them to be, non-governmental and even international bodies have appeared to help (http://www.crime-research.org/about/). The Computer Crime Research Center offers a document detailing the state of computer crime laws in former Soviet republics (http://www.crime-research.org/library/Criminal_Codes.html).

A similar non-governmental organization, the Open Forum of Internet Service Providers, created a set of fair network-use rules in 2002. These were adopted as a precedent (http://www.ofisp.org/documents/ofisp-008.html) in confirming a court decision regarding the ISP MTU-Intel terminating Internet access for a spammer.

In July 2005 the story of how the most prolific Russian spammer—Vardan Kushnir—was killed was circulated by the media. The widespread belief that his murder was related to spam distribution collapsed after the real killers were detained in August 2005.[4] It's ironic, though perhaps typical of how media works, that unfounded speculations received much wider publicity than the facts that became available once the murder case was closed.

Black market price list

Figure 1: This site offers malware for sale and even asks for visitor feedback in a small poll.

If one is looking for custom-made malware, it is not difficult to find—there are even specialized Web sites that advertise such services. We also encountered several requests for malware in some forums.

Clearly, because there are buyers and sellers, there is a market. On this same site in Figure 1 we found poll results asking visitors whether they are interested in offers of bank accounts, logs, PayPal, eBay, etc. Surprisingly 67 percent (149 votes) said "Yes." The site offers the following "specialized" markets:

- Bots
- Bruters (apparently brute-force crackers)
- Flooders
- Grabbers
- Infectables (viruses and worms)
- Keyloggers
- Sniffers
- Spam software
- Sploits (exploit demos and vulnerabilities)
- Trojans

Financial malware

Figure 2: Shopping for malware: What's available?

This site offers a total of seven entries, including the following:

- PG Universal Grabber (Power Grabber Version 1.8): supports Microsoft Internet Explorer and compatible browsers, installs itself and eliminates installation traces, bypasses firewalls, is invisible and undetected, sends logs immediately after a POST, loads external files, updates bots, blocks selected sites, self-destructs after n-th restart, encrypts URLs
- Grabber toolkit: "everything for a novice carder"—builder, key generator, provides stats through an administrative page
- Grabber Ghost Version 2.0: when activated changes URLs returned by search engines or when specific keywords are used

3 "MPack, Packed Full of Badness," Symantec Enterprise Weblog. http://www.symantec.com/enterprise/security_response/weblog/2007/05/mpack_packed_full_of_badness.html

4 "Vardan Kushnir," Wikipedia. http://en.wikipedia.org/wiki/Vardan_Kushnir

Bots and builders

Bots (Figure 3) on the market:

- WDLX Version 1.1: includes a downloader that uses a URL specified in a builder, installs itself, and waits for a live Internet connection. After a time specified by the purchaser, runs the program and removes all traces of its activity
- Xloader: fools firewalls, provides detailed statistics via php-scripting
- Multithreaded distributed denial of service (DDoS): new multifunction, multithreaded bot for Unix, Linux, and related operating systems

And their prices, in U.S. dollars:

- Bot builder with DDoS functions: $250
- Bot build: $35
- Bot: $25
- Downloader (5K–6K in size): $10
- Form grabbers: $350
- Keylogger: $20–$30
- WebMoney Trojans/builders: $60

Custom malware

This advertisement (Figure 4) was posted to multiple forums, offering the following services:

- Breaking into Web sites and forums: $50
- Guaranteed break-in into mailboxes on mail.ru and yandex.ru: $45
- Mass deployment of Trojans and spying programs: $100
- Spam distribution: $70

Spam-related services

This site (Figure 5) offers "spam services," offering collections of email addresses, at these rates:

- 400,000 companies: $55
- 1,800,000 individuals: $100
- 90,000 companies in St. Petersburg: $30
- 450,000 individuals in Ukraine: $50
- 6,000,000 Russian individuals: $150
- 4,000,000 addresses at @mail.ru: $200

The service generously offers discounts for payments made via WebMoney.

Figure 3: Bots for sale

Figure 4: Choose your exploit

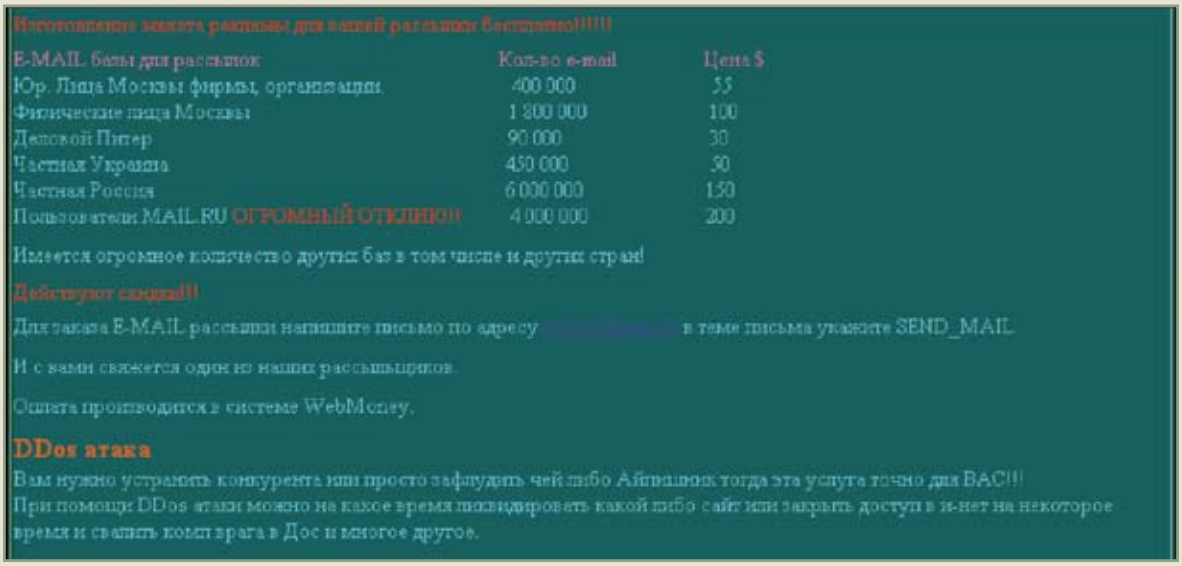


Figure 5: All the spam you could ask (and pay) for

DDoS attack on Estonia

In April and May 2007, there was a major DDoS attack targeting many government Web sites in Estonia. Investigators believe the attack was triggered by the relocation of the "Bronze Soldier," a monument that memorializes a Russian unknown soldier of the Second World War.[5] Estonian authorities had decided to move the statue from the center of Tallinn to a suburban cemetery. This caused civil unrest in Tallinn; one person was killed. Later, closer to the anniversary of the Victory in Europe Day (from the Second World War, celebrated on May 9), a DDoS attack started that lasted for several days. Many major Estonian Web sites were unavailable during this period. The prevailing opinion of the security experts is that this attack was committed by a group of individuals and was fuelled by their patriotic feelings.[6] More technical details about the attack can be found here.[7] No trace to any Russian government involvement was found nor is a link likely to be found, even if there were one.[8,9] Mutual accusations of cyberattacks followed this incident.[10]

Conclusions

At McAfee® Avert® Labs, we have a good feeling for what is fueling the creation of computer malware. All countries that combine relatively poor computer users with wide availability of the Internet and good computer skills are contributing to the problem; examples include China, Russia, Brazil, and Ukraine.

It is obvious to us that the Russian mafia and FSB are not behind the increase in malware, spam, and phishing attacks coming from former USSR. The mafia, however, must be interested in supporting computer crime—due to its extremely high return and low risk. At the same time it would be surprising if the new edition of the secret police had no department specializing in computer security and did not invest in research on computer warfare. The same should apply to the military. Nonetheless, we see economic factors as the primary cause of the development of malware in Russia and the other former Soviet republics.

Predictions

With enhancements in legislation, a strengthening economy, lower unemployment, and stronger law enforcement in Russia we expect a gradual decrease in the rate of malware production. Other former Soviet countries and even China are likely to follow the same pattern. At the same time, current trends in malware counts clearly indicate an acceleration of production in almost all regions of the world. Even if the production of malware in Russia falls to "western standards," it will still be considerable.

We are not likely to see a general decrease in malware numbers any time soon. Computer crime is too profitable and poses too few risks at the moment. And contrary to a common opinion, it is not just a technological problem—it is very much a social and economic problem. As it frequently happens, things are likely to get worse before they start to get better. We believe in the long term that major changes may occur if we can reach global agreements on using the Internet (for example, compulsory Internet ID cards). More likely change for the better will come from advances in computer security, in both hardware and software areas.

Dr. Igor Muttik is Senior Architect for McAfee Avert Labs. Dr. Muttik holds a Ph.D. in physics and mathematics. His studies of the first computer viruses led to his joining Dr. Solomon's Software, which was later acquired by McAfee, Inc. In addition to his research work on malware, Dr. Muttik is a frequent presenter at security conferences around the world.

5 "Bronze Soldier of Tallinn," Wikipedia. http://en.wikipedia.org/wiki/Bronze_Soldier_of_Tallinn

6 "Estonian DDoS—a final analysis," Heise Security. http://www.heise-security.co.uk/news/90461

7 "Estonian DDoS Attacks—a summary to date," Arbor Networks. http://asert.arbornetworks.com/2007/05/estonian-ddos-attacks-a-summary-to-date/

8 "DDoS attacks on the Estonian servers were not a cyber war," Heise Online. http://www.heise.de/english/newsticker/news/91095

9 "Massive DDoS attacks target Estonia; Russia accused," Ars Technica. http://arstechnica.com/news.ars/post/20070514-massive-ddos-attacks-target-estonia-russia-accused.html

10 "Malware Evolution: April–June 2007," Viruslist.com. http://www.viruslist.com/en/analysis?pubid=204791956

GERMANY:

MALWARE LEARNS THE LANGUAGE

By Toralv Dirro and Dirk Kollberg

The threat landscape in Germany, and all over Europe, has differed from North America's since the 1990s. The main reason for this difference is the variety of languages; in the European Union alone there are 23 official tongues. Furthermore, we've seen for a long time that a language barrier stops most malware and other attacks from succeeding.

The barrier went up when paths on the file systems differed depending on the language of the operating system. Malware often used hard-coded paths to determine where to put files or where to seek information. And it failed miserably. (We still see commercial software failing to function properly from time to time for this very reason.)

Microsoft Word macro viruses were the next class of malware to find the language barrier difficult to cross. The first macro viruses didn't work at all; many of the macro viruses we have seen since then have had some problems too. The reason for this is that in localized versions of Word the functions had been localized as well. So if a virus tried to hook the function FilePrint, for example, it would have to hook DateiDrucken in a German version of Word and FichierImprimer in a French version. This led to malware authors creating viruses that specifically targeted German Word, French Word, Spanish Word, etc. Of course it is possible to create macro viruses that do not hook any function that is translated to local languages; those have been successful in Europe.

The next wave was mailers and mass mailers, viruses that actively created emails to send themselves to other people. This was the first kind of malware that relied on social engineering to be successful. (Social engineering in this context means that the receiver must be convinced that it's worthwhile to open the email and attached file.) The problem for the attacker today is exactly the same as it was when mailers first appeared: creating a message that looks authentic and makes a user open the attachment. Using the receiver's native language for the message text is a good start. Or use little or no text at all. A long English-language message claiming that there is something very important in the attachment that I absolutely have to open, apparently sent by a friend or coworker, just won't cut it in Germany.

Some very primitive viruses were successful because they used hardly any text. Some of these were created with VBSWG, a virus construction toolkit that allowed anyone to create simple mass mailers that used Visual Basic Script. In the following example all that matters is the name of the attachment, so the language barrier makes little impact.

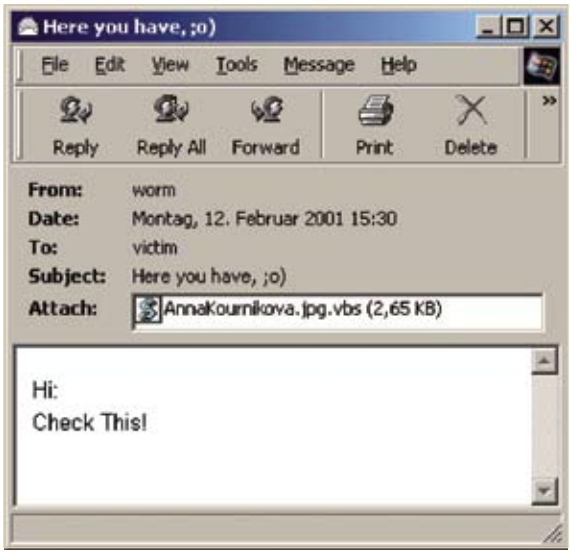


Figure 1: Social engineering is the key to this tempting file attachment.

With Windows Explorer preferences set by default to hide known file extensions, the name of this malware would appear as AnnaKournikova.jpg, and fool the user into assuming it's a picture.

Other threats used the local language for the text of an email. Although this tactic made malware successful in one region of Europe, they were hardly a threat outside that area. Thus we have seen a number of local outbreaks, in which one particular virus blankets a region, yet is hardly

seen outside it. This extreme regional focus makes it very difficult for researchers to provide an accurate assessment of the risk posed by the malware. Having local virus research labs throughout European countries proved very helpful in these cases.

Now that we've seen the big shift in the malware scene caused by the potential profits of the botnet business, data-stealing Trojan horses and phishing scams in email messages are getting more sophisticated every day. In the early days messages were composed in a crude German notation that looked like it was an English or Russian text translated by Babel Fish. That's probably what happened.

Today we read text written in perfect German, referring to current events and playing on people's hopes. During the FIFA soccer World Cup in the summer of 2006, German fans had trouble finding tickets. So we saw emails promising details in an attachment with information about buying those rare tickets. The illegal sharing of music and videos has been in the news for a long time; German authorities have proposed an online search of computers using a special "BundesTrojaner." This has been a hotly debated topic and has led to the following email:


Aktenzeichen [00133542]

File Edit View Tools Message Help

From: Kriminaldirektor
Date: Mittwoch, 9. Mai 2007 03:13
To: spammed-addresses
Subject: Aktenzeichen [00133542]
Attach: ka070507.zip (7,88 KB) ATT00044.txt (0 bytes)

Sehr geehrter Internetnutzer,

im Rahmen unserer ständigen automatisierten Überprüfung von sogenannten Tauschbörsen im Internet, wurde folgende IP-Adresse auf unserem System ermittelt.

IP: 81.112.150.144

Der Inhalt Ihres Rechners wurde als Beweismittel mittels den neuen Bundestrojaner sichergestellt.
Es wird umgehend Anzeige gegen Sie erstatten, da sich illegale Software, Filme und/oder Musikdateien auf Ihren System befinden. Durch die Nutzung sogenannter Tauschbörsen, stellen Sie diese auch anderen Nutzern zu Verfügung und verstoßen somit gegen §§ 249ff StGB.

Das vollständige Protokoll Ihrer Online-Durchsuchung finden Sie im Anhang dieser Email.

Die Strafanzeige und die Möglichkeit zur Stellungnahme wird Ihnen in den nächsten Tagen schriftlich zugestellt.

Figure 2: The text says "Your IP address has been logged while illegally sharing files with other users. Your computer has been searched using the BundesTrojaner and evidence has been secured. A criminal complaint is going to be filed; the attachment contains a protocol of the online-search conducted on your computer."

This is one example of the notorious Downloader-AAP, which is a very common threat in Germany. This malware was spammed to users with email addresses that ended with ".de"; the text was in German. For many months we have seen several spam runs each week, all with different messages in the mail body and different variants of the downloader and the password-stealing Trojan that the downloader installs.

In the message, the recipient gets an invoice from an attorney or a well-known German company, such as Deutsche Telekom, eBay, or GEZ, the federal service that collects fees from anyone who owns a TV or radio. These "senders" catch the reader's interest: No one likes to receive a bill, particularly if might be a case of fraud.

The Downloader-AAP example employs the fear factor, in this case due to file sharing and its associated legal problems being big news in Germany. The message says that the user was caught red-handed downloading copyright-protected files from a file-sharing network and the IP address was logged. The user's PC was already examined by the BundesTrojaner and admissible evidence was found. The Bundeskriminalamt (BKA, similar to the FBI in the United States) will report the offense.

As in all of these spam runs, the mail promised further details in the attachment, which appeared to be a bill, often named Rechnung.pdf.exe. Depending on system settings, some users may notice only the PDF extension and assume the file is safe, but it's actually a malicious executable—Downloader-AAP.

These messages scared many people, and they clicked before thinking twice. Due to a lack of evidence, however, this example does not work in other countries.

Focus on Germany

Why do the bad guys focus only on a single country?

Downloader-AAP downloads a text file that contains an encrypted URL. This file gets decrypted and the file hosted at the URL gets downloaded. It turns out to be Spy-Agent.ba, a Trojan that attempts to steal confidential account information and focuses on financial institutions. It's designed to "hijack" home-banking connections and to steal user credentials and transaction authentication numbers (TANs). These functions within the Trojan are optimized for different corporations in Germany; the Trojan injects itself into the communication between the user at home and the bank. Depending on the institution the Trojan has different ways of infiltrating communications.

On September 13, 2007, Germany's BKA announced that they had busted an international group of phishers, arresting 10 persons and seizing a number of computers and other evidence.[1] The BKA's press release claims this is a group that has been harassing the world with phishing emails containing Downloader-AAP as an attachment.

But this is unfortunately not the end of Downloader-AAP. Just a week after the arrest, McAfee® Avert® Labs received a new sample distributed in a similar way and downloading Spy-Agent.ba.

Trojans targeting financial institutions do not plague only Germany; they also occur in other European countries and they are also a big threat in Brazil.

Germans care a lot about their banking security and were very hesitant to adopt technologies such as online banking.

Phishing itself has had less impact in Germany than in many other countries. And this is not solely due to the language barrier. The Germans care a lot about their banking security and were very hesitant to adopt new technologies such as online banking. This reluctance forced banks to offer a security scheme that makes it much more difficult to take over someone's bank account. The current system requires not only an account name and PIN to log in, but every transaction also needs a TAN. The bank sends those on paper to the user. Every transaction needs to be submitted with an unused TAN. This strong security has forced criminals to pursue online banking opportunities in other countries.

Phishing for TAN

Some Trojans were written to extract the TAN list from the user's machine if those numbers were stored electronically, and, of course, we did see the occasional dumb phishing mail that tried to get those TANs.

Figure 3: This phishing request asks for 10 unused TANs, in addition to lots of personal data.

In recent months we have seen Trojans that specifically attack German banks, hooking into the user's browser and emulating the behavior of each online banking site with fake error messages to get at the TANs the attacker needs. Those Trojans are available for sale on certain web sites for would-be criminals; the authors have released videos demonstrating their features and effectiveness online. German online banking is very likely to be attacked more often in the near future.

1 "Success against internationally organized online criminals" (in German), BKA. http://bka.de/pressemitteilungen/2007/pm070913.html

W32/Sober@MM is a mass mailer that has gained a lot of attention in Germany, Austria, and Switzerland. The first variant was seen at the end of 2003, the most recent in March 2007. Like many other mass mailers, W32/Sober harvests email addresses found on the local system and sends out mails to users in different languages, depending on the top-level domain of each recipient's address.

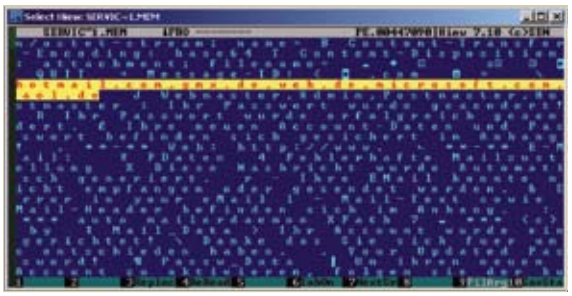


Figure 4: W32/Sober@MM can send messages in different languages. It "decides" after reading the top-level domain of the addressee.

In another popular attack, W32/Sober.p@MM sent to German users a mail stating that the recipient had won tickets to the soccer World Cup:

Subject : WM-Ticket-Auslosung
Body:
Herzlichen Glueckwunsch,

beim Run auf die begehrten Tickets für die 64 Spiele der Weltmeisterschaft 2006 in Deutschland sind Sie dabei.

Weitere Details ihrer Daten entnehmen Sie bitte dem Anhang.

Ihr "ok2006" Team
St. Rainer Gellhaus

--- FIFA-Pressekontakt:
--- Pressesprecher Jens Grittner und Gerd Graus
--- FIFA Fussball-Weltmeisterschaft 2006
--- Organisationskomitee Deutschland
--- Tel. 069 / 2006 - 2600
--- Jens.Grittner@ok2006.de
--- Gerd.Graus@ok2006.de

Figure 5: This message informs the happy receiver that soccer tickets are available.

The World Cup scam promised further details, but inside the zipped attachment was the file winzipped-text_data.txt.pif. Of course there were no details; it was just a copy of the worm.

The worm's timing was excellent: It was released when many people were waiting for a mail from the FIFA ticket lottery. Even the address and the phone number listed in the German text are accurate. In effect, the worm caused a distributed-denial-of-service attack on the FIFA office because so many users who received the worm called the number and asked for details.

For English recipients, W32/Sober sent out a different mail with a copy of itself attached:

Subject: Your Password
Body:
Account and Password Information are attached!

Visit: http://www. {*sender's domain*}

*** AntiVirus: No Virus found
*** "{*recipient's domain*}" Anti-Virus
*** http://www. {*recipient's domain*}

Figure 6: W32/Sober's English-language message used a generic appeal.

Making a local appeal

Another example of localized malware is the Zunker Trojan. It's also a password-stealing Trojan that also sends spam emails or links to malicious sites, in order to infect other people. The nasty thing with this Trojan is that it connects to a server on the Internet and, based on the victim's IP address, the Trojan receives the spam messages the user is supposed to send.

Zunker not only sends spam emails in the way you would expect. It also injects some text into the emails the users send. To do this, Zunker installs a Layered Service Provider on the compromised machine. Whenever the user sends an email, Zunker alters the text and adds a malicious link. The recipient of the mail probably knows the sender and thus might trust both the message and the link. Zunker also injects these messages into ICQ, AOL, and Yahoo instant messages.

The key localization aspect in this case is the injected message. If the IP address of the victim is registered in Italy, for example, Zunker will inject an Italian quote and the link. In Sweden, it would be a Swedish quote, and so on.

Figure 7: The Zunker Trojan can localize its messages in various languages, appealing to users in many countries.

You can see in Figure 7 where Zunker's victims are located and how it spreads out the spam. The same web interface controls the Trojans and sets up the messages they're spreading—either for all victims or separate messages for each country.

Infected web servers

Another way to distribute localized malware is via web servers. When a browser requests a file from an HTTP server, it establishes a TCP network connection. The server receives the request, loads the file from the hard drive, and sends it back. Servers that host malicious files have another feature. After they receive a request, they first look at the IP address of the connecting system, using a database to resolve its country host. With this information, the infected server can deliver localized files to each country.

With this system there's just one link to a web site. Depending on where your IP address is registered, users in the United States or United Kingdom receive an English-language Trojan, while someone from Germany or Austria receives German-language malware.

These infected servers are hard to monitor for anti-virus vendors, because they need to send several requests to the same URL, each from a different IP address, in order to receive all variants of the malware.

Another way to serve localized files is to look at the request the browser sends to the server:

```
000000 GET / HTTP/1.1
000010 Accept: image/gif, image/x-xbitmap, image/jpeg, image/pjpeg, application/x-
00005B shockwave-flash, */*
000071 Accept-Language: de
000086 Accept-Encoding: gzip, deflate
0000A6 User-Agent: Mozilla/4.0 (compatible; MSIE 6.0; Windows NT 5.0)
0000E6 Host: 127.0.0.1
0000F7 Connection: Keep-Alive
00010F
p00111
```

Figure 8: A Trojan could determine the nationality of this client request—and choose a local language for reply—by reading the Accept-Language line.

In Figure 8, you can see the user is from Germany (de) and uses Internet Explorer Version 6 on Windows 2000. Anti-malware researchers have little trouble dealing with these servers; it's easy to send different requests to a server from a single IP address and receive the various files the Trojan has to offer.

Conclusion

Many attackers now understand that it is important to take regional customs into account if they want to be successful. We've seen that this lesson has been well learned in Germany and the trend of localizing attacks is certain to continue. Phishing attacks are getting more sophisticated and will become harder to spot. Fraudulent job offers seeking financial agents, a thinly veiled attempt to hire innocent people for laundering money, look very professional today and are likely to adapt to local factors even more in the future. It's likely that German speakers will soon face the same level of exposure to phishing, Trojans distributed by email, and even spam as people in English-speaking countries do.

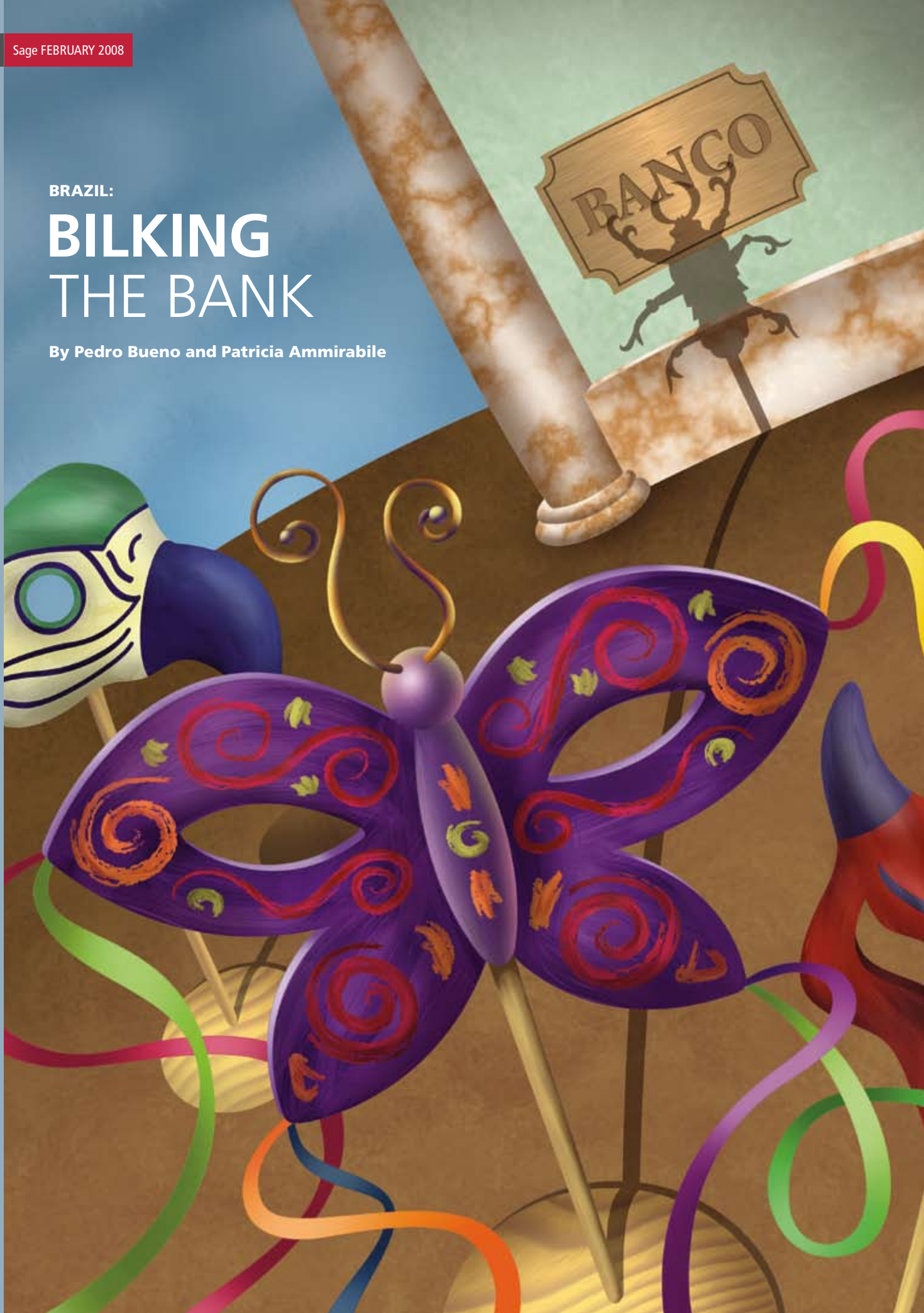
Toralv Dirro is a Security Strategist in the Hamburg office of McAfee Avert Labs. Dirro, a researcher since 1994, is a well-reputed expert on next-generation anti-virus technology and network intrusion prevention; he is a frequent speaker on those topics.

Dirk Kollberg works as Malware Research Lead in Hamburg for McAfee Avert Labs. An eight-year veteran, he analyzes worms, peer-to-peer network and service-exploiting threats, as well as Trojans, bots, and other viruses. Kollberg blames the Commodore PET for his addiction to bits and bytes.

BRAZIL:

BILKING THE BANK

By Pedro Bueno and Patricia Ammirabile



Cybercrime has a significant economic impact that varies around the world. Further, the types of cybercrime can differ significantly from country to country. In South America, Brazil has been suffering for some years from a plague of Trojans called PWS-Bankers. The PWS stands for password stealers, so this malware specifically targets bank account passwords.

The Trojans invade via phishing scams. These fake e-mails turn thousands of users into victims in Brazil, and abroad, year after year, by displaying fake login pages and playing mind games with the victims. One trick is to exploit a victim's willingness to help others by appealing for help after disasters such as hurricanes, air crashes, and more.

In Brazil, the finance industry—by a wide margin—is the preferred target of cybercrime. In 2005 alone, Febraban (the Brazilian Banks Federation) estimated the losses at R$300 million (reais, about US$165 million) due to virtual fraud in Brazil.

In this paper we will look at how Brazilian banks are organized, how the password stealers work, and the efforts of Brazilian federal police.

The State of Online Banking

According to Febraban, "Brazilian banks are concerned with this new fraud/hacking scenario, but they are aware that the technology innovation has gone past the point of no return, either due to the evident benefits to customers—who gain time and convenience for transactions anywhere, anytime—or to the sheer efficiency gains provided by the new channels to the Brazilian financial system. That's why so much is invested to enhance banking technology: R$4.2 billion [US$2.3 billion] in 2003 and R$6 billion [US$3.3 billion] in 2006."[1]

As result of these actions, Brazil today has one of the most efficient and secure online banking systems. Almost 100 percent of Internet banking sites use HTTPS and two PINs (one to log into the system and the other to confirm an operation). Some banks are using "paper token" and OTP (one-time password) tokens to provide another layer of security.

To understand how the PWS-Bankers manage to work around this security, we must first understand how the Internet banking system works.

Here are the basic steps to log into a Brazilian bank:

- User goes to the HTTP bank site
- Inserts the branch office and account numbers
- User is redirected to HTTPS site
- User enters the Internet PIN (or token number)
- User starts a transaction, such as a money transfer
- User enters the bank PIN/token number to confirm

How do PWS-Bankers work?

One of the factors that has led to the increase in the number of online scams is the sophistication of the messages sent to users. These are very different from the early days of phishing messages, which often contained grammatical mistakes and typos, as well as inappropriate language. The latest scams lure users by showing a legitimate look and high-quality images; phishers also send near-perfect copies of texts used by respected companies. Attack tools are even available from the online underground market, allowing "lamers" (hackers with only basic technical skills) to participate in online fraud.[2]

Phishing emails arrive at a victim's mailbox with one of a variety of subjects:

- Fake orders from well-known Brazilian online stores
- Fake greeting cards
- Fake sex pictures/videos of celebrities
- Fake tax software
- Fake election reports
- Fake pictures of car/airplane crashes

1 "Segurança" (in Portuguese), Febraban.
http://www.febraban.org.br/seguranca_site/seg_compromisso_de_todos.asp
http://www.febraban.org.br/seguranca_site/seg_investimento_seguranca_2007.asp

2 "Lamer," Wikipedia. http://en.wikipedia.org/wiki/Lamers

The emails contain links that lead victims to download PWS-Bankers.dldr, which are the downloaders of PWS-Bankers. The malware writers cleverly use these small downloaders, which are around 45KB or less, to prevent users from becoming suspicious. Once aboard, the small applications quietly download the real PWS-Banker, which is about 1MB–4MB, in the background.

Once PWS-Banker is installed, it sends a background email to its author to confirm that another machine has been infected. The hacker gains the following information:

Computer Name: MACHINE-SVR
Computer User: Administrator
IP: 192.168.241.100
Date: 9/6/2007 Hour: 7:19:03 AM
Windows: Microsoft Windows XP (Version 5.1)
Mac Address: 00-0C-29-3C-C7-A1
IE-Version: 6.0IE-Version: 6.0.2600.0000
Windows Key: xxxxx-xxxxx-xxxxx-xxxxx-xxxxx

PWS-Banker will remain resident in the memory, monitoring the web sites the user visits. The malware usually has a list of five to eight banks to target. When PWS-Banker notices the user request the URL of one of these banks, it will pop up a fake window that mimics the bank's site.

Most banks in Brazil ask for account number, branch office number, and Internet PIN to allow the user to log in. The Trojan will ask for some additional information: the bank PIN, and credit card number, verification code, and expiration date, among other data.

Once the malware has this information, it will display an error message and redirect the user to the bank's true Internet page, while sending an email to the hacker with all the information:

- Account name
- Account number
- Internet PIN
- Bank PIN
- Pass phrase
- Account owner's name
- Credit card number
- Credit card PIN
- Credit card date
- Credit card expiration date
- Father's name (for positive authentication)

These examples illustrate the differences:

Figure 1: A real bank's online screen. A genuine bank asks only for user name and Internet PIN.

Figure 2: Fake screen used by the PWS-Banker Trojan. This form digs a little deeper, asking the user for branch office number, account number, and bank PIN.

Quick Update by PWS-Bankers

On June 16, 2007, the major corporation Banco do Brasil released a new Internet banking web site, updating everything in its design. Banco do Brasil is one of the most targeted banks in the country, and most PWS-Bankers already had a copy of the bank's old web design inside their databases of fake banks.

With a few days we discovered a source-code repository of PWS-Bankers, and found plenty of files that targeted Brazilian banks. One file in particular caught my attention; it was called "New Banco do Brasil Screen.jpg." This file had the date June 21 and had the brand new password screen of the new Banco do Brasil web site! Assuming that the dates are accurate, in fewer than five days the miscreants had a functional PWS-Banker Trojan that was ready to pose as the new bank site.

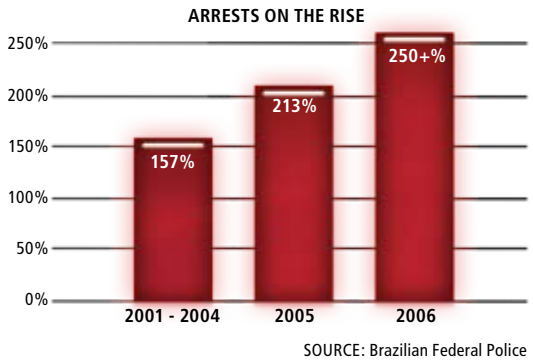


Figure 3: The Brazilian police arrested more malware writers in 2005 than in the four previous years combined. Arrest figures in 2006 continued that increase.

The federal police are enjoying some success in their contest with hackers. In the period from July to September 2007, police arrested almost 100 persons involved with bank-account password stealers.

In July the police operation Nerds II led to the capture of 29 persons alleged to be responsible for the deviation of more than R$10 million (US$5.5 million) in less than one year.

Conclusion

In spite of the increase in phishing and password-stealing Trojans, Brazilians enjoy reasonably strong security for online banking. Nonetheless, the struggle against malware is ongoing.

We can recommend a number of best practices for both consumers and corporations. The business methods include establishing policies for email, web browsing, and effective security software. Consumers should employ software to block spam, spyware, and outbound data to malicious sites. And it pays to be suspicious: If you aren't sure whether an email is legitimate, call the apparent sending institution to verify its authenticity.[3]

The coordinated efforts of financial institutions, federal police, security software companies and end-user education are making progress in containing and diminishing the current large volume of criminal activities that target online banking.

Pedro Bueno is a Virus Research Engineer at McAfee® Avert® Labs in Brasília. He has worked more than 10 years in the security arena, managing incidents for large telecom companies and serving as a volunteer handler at the SANS Internet Storm Center.

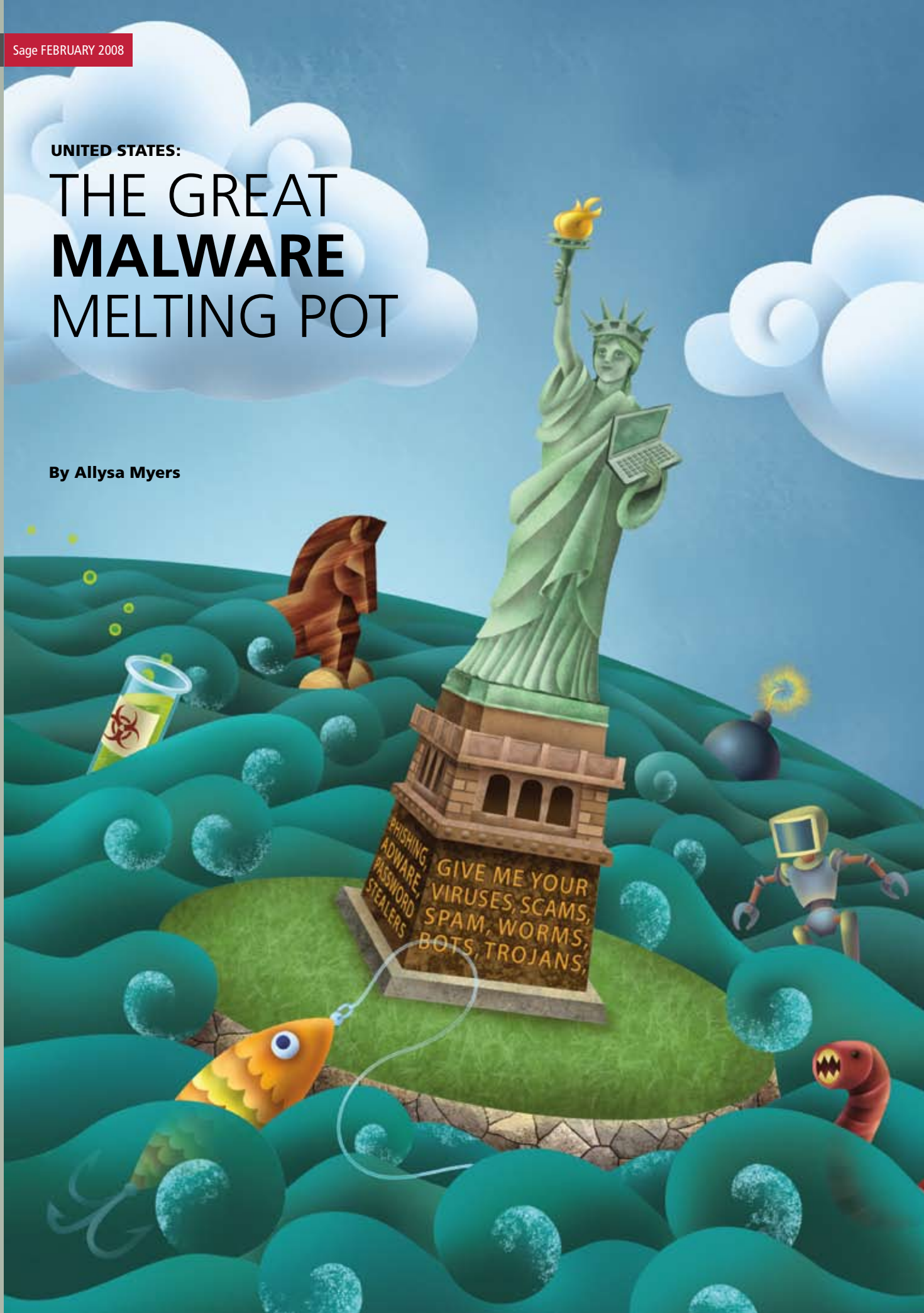
Patricia Ammirabile is a Virus Research Analyst with McAfee Avert Labs in São Paulo. She has worked at McAfee for 12 years; her duties have included offering high-level technical support to both corporate and home users, providing multilingual and translation services, and analyzing malware.

3 "Anti-Phishing: Best Practices for Institutions and Consumers," McAfee. http://www.mcafee.com/us/local_content/white_papers/wp_anti_phishing.pdf

UNITED STATES:

THE GREAT **MALWARE** MELTING POT

By Allysa Myers



In the United States, the presence of malware has become part of the background noise of the Internet. Things like spam, phishing, and scam emails are something every email user has seen at one time or another, whether or not they fell for the ruse. Viruses and Trojans are present in email, come from seemingly innocuous web sites, arrive as links in instant messages, and creep in through vulnerabilities in the operating system or popular applications.

With all these ways of entering our machines to make illegitimate monetary gains, no one genre of malware stands out as uniquely American or especially prevalent in the United States compared with other countries in the world. In this article, we will discuss how the United States has influenced the development of the Internet, and how this has affected the global malware environment.

U.S. malware: the 'new black'

In many ways, the United States has ceased to be unique in the malware realm. Because it was the first country in which both home and corporate users enjoyed widespread Internet use, it helped set the standards and expectations of what the web experience would be for the rest of the world's users. In effect, the frame for people's view of the Internet has been crafted by the Americans who created and popularized it.

Because the Internet has existed for such a (relatively) long time in the United States, it became a part of life very early for many American students and government workers. As users saw the utility of this nascent technology, a large percentage of people quickly gained access to the Web or email.

Even before money became the major malware-development motivator, hackers realized that to spread their malware widely they needed to set it loose in the United States. As other countries have gained a commercial presence on the Internet, they've begun to share the burden of being targeted by malware.

Having a single language as the de facto standard has been exceedingly helpful in international business, including the malware business. Most people in the business world have at least a passing understanding of English, which means the odds of success for social engineering written in English are significantly higher than for deceptions written in any other language. This common language simplifies carrying out targeted attacks of business executives; it obviates the need for additional intelligence on what language the targets speak, as it's almost a given that they'll speak or at least read English.

On the other hand, the unique cultures in other countries have led to a fertile ground for particular kinds of malware, as we've seen elsewhere in this publication. Although the actual infection rate in those countries may be lower than in the States, those nations have specific genres of malware that stand out as peculiar to those areas.

Many threat trends, including malware and potentially unwanted programs such as adware, started in the States. Several others started elsewhere and then moved here once virus writers realized there was more money in making international campaigns. Bank-account and online-game password stealers, for example, were common in other countries long before they appeared in significant numbers in the United States.

Virtually borderless Internet

The Internet makes it easy to cross borders. Technological advances such as proxies have made it easier to obfuscate a person's location, and Web 2.0 has made content "viral" so that it can be spread worldwide in a matter of hours.

Almost all the most popular Web 2.0 and e-commerce sites started in America, but at this point each of them has a large number of users in other countries. Online auction sites and online payment providers are common phishing targets, and are available to and popular with users outside the States. Google, Yahoo, Blogger.com, MySpace, Wikipedia, YouTube, and Facebook rate in the top 15 web sites of almost every country in the world, according to Alexa.com.[1]

The most notable security issue regarding Web 2.0 sites is the speed with which content can spread. Phishing, spam, malware, and adware have all been found on the most popular Web 2.0 sites. Malware authors have repeatedly demonstrated an ability to take advantage of technology trends as they occur.

Another trend that has caught they eye of malware authors is proxies. These were initially popularized as anonymizers, to keep people from being able to filter or track web-surfing behavior.

1 "Top Sites," Alexa.com. http://www.alexa.com/site/ds/top_500

The malware community has used this feature to make physical location meaningless for those serving up malicious code. These proxies are typically used for tunneling and anonymizing purposes and to make it more difficult to trace the initial connection—either by removing identifiable information or by adding more "hops" in a traceroute.

Proxies are most commonly used by bots, whose purpose is to "own" a large number of remote machines. Once they have remote control of the machines, bot masters can upload a wide variety of tools after the initial infection. Internet Relay Chat (IRC) bots are a truly borderless type of malware, and the one that makes the most frequent use of proxies. These bots don't rely on social engineering to spread. Instead they exploit software vulnerabilities, which are ignorant of what country you're in. Bots will happily infect a vulnerable Windows machine in Zambia, Korea, or Liechtenstein as readily as one in America.

Riches and ruffians

The United States employed 5.8 million people in the technology industry in 2006, and the average tech worker made US$75,500 per year, which is 86 percent more than the average income of people outside of the industry. Unemployment rates in the tech industry are also quite low, at around 2 percent, which means there is a shortage of qualified people to fill these jobs.

These figures are not a significant change from the past—the total number of tech jobs grew 2.6 percent from 2005 to 2006, and the average income in 2000 was actually US$78,691.[2] This means that there are a large number of people in the country who are well connected at work and at home, and who are well paid. These people make a lot of money, so they're likely to have more powerful machines that could be used surreptitiously; however, if they're employable, they stand a decent chance of getting one of these legitimate tech jobs.

The United States has always had its fair share of young people involved in the virus-writing scene. There is no shortage of script kiddies getting a piece of the malware pie. As prosecution efforts have resulted thus far in few arrests of bot masters, many see spreading malware and adware as a low-risk way to make a significant amount of money.[3]

The States has had a relatively stable economy since the beginning of the Internet, and computer-related jobs are reasonably accessible and lucrative. Although there may be a desire to wreak havoc when computer-savvy kids are too young to be legally employed, once they're old enough they usually move into a legitimate job in the computer industry.

Canned spam and roasted bots

A number of laws have been enacted that deal with malware, spam, and adware; the oldest and most widely used of these is U.S. Code Title 18, section 1030.[4] There have also been several high-profile efforts to nab those engaged in cybercrime—Bot Roast is the most recent—to increase arrests of bot masters.[5] A number of successful suits have been brought against spam purveyors, bot masters, and adware companies, though this has had little effect on their presence or continued prevalence.

Law enforcement agents in the United States, as in much of the world, often bemoan the state of international law dealing with computer crimes.[6] Computer crime laws differ from one country to the next, so what is illegal in the States may not be so elsewhere. Extradition treaties also differ, which can affect the ability to prosecute cybercriminals.[7] Even if these two problems are not an issue in a particular case, bureaucracy may cause trouble. Frequently law enforcement officers will spend months tracking down a virus author, only to be stymied by the lack of timely cooperation from the authorities in other countries. In the time it takes to get the necessary information or reach important people in a case, a trail can go completely cold.

21st-century grifters

Where malware is concerned, social engineering tends to fall under two categories: fear and titillation. There are many universal subjects in both categories, and are limited only by one's understanding of the language that the message is delivered in. The topics of sex, curiosity, or embarrassment (for example, naked pictures—either of oneself or others) transcend culture. The primary consideration is whether the subject is of sufficient interest to the victim of the social engineering.

The appeal of American pop-culture does not stop at its borders. Although the average person in any given country may or may not know the name of the hottest stars from Bollywood, Europe, or China, most people know of celebrities such as Britney Spears or Angelina Jolie. A computer user's likelihood of falling for social engineering pertaining to these celebrities has more to do with their ability to read the language of the emails or IM messages.

2 "Number of U.S. tech jobs rises despite fears of outsourcing," USA Today. http://www.usatoday.com/tech/techinvestor/industry/2007-04-24-techjobs_N.htm

3 "Alleged Botnet Crimes Trigger Arrests on Two Continents," PC World. http://www.pcworld.com/article/id,123436-page,1/article.html

4 "Fraud and Related Activity in Connection with Computers," U.S. Dept. of Justice. http://www.usdoj.gov/criminal/cybercrime/1030_new.html

5 "Over 1 Million Potential Victims of Botnet Cyber Crime," FBI. http://www.fbi.gov/pressrel/pressrel07/botnet061307.htm

6 "Prosecuting Perpetrators of Malicious Software (Malware)," Continuing Education of the Bar. http://ceb.ucop.edu/newsletterv7/criminal_Law.htm

7 "Impediments to the successful investigation of transnational high tech crime," Computer Crime Research Center. http://www.crime-research.org/articles/trends-and-issues-in-criminal-justice/

On the other hand, due to the size of the country and the insular attitude of many of its people, the United States has an unusual tendency to show little interest in international politics or culture. Social engineering that involves news of exciting events in another country is likely to be ignored, while most other countries of the world would be interested in hearing news of the death of U.S. leaders (as W32/Nuwar@MM used for its initial email).

On the fear side of these deceptions we see bounce messages and other error notifications. Bounce messages specifically are a universal phenomenon—any ISP of a decent size will notify users when an email does not reach its goal. As long as the sender sees what looks like a real bounced message, this exploit could attack a user in any country.

In at least one case social engineering requires a country-specific approach: when spoofing messages from government agencies. Anyone in the United States might be concerned by an email that appears to be from the IRS, but this tactic won't work in other countries. This type of social engineering is certainly common, but it's rare for this to be the only trick in a virus writer's arsenal. Most mass-mailing viruses contain a variety of possible email bodies, and this will be just one of many variations. W32/Sober@ MM!M681 is a perfect example: It includes emails supposedly from the CIA and FBI, messages about Paris Hilton and Nicole Richie, three emails in German, and a handful of others using a variety of tactics.

Fixing a hole where the malware gets in

When malware writers don't want to go to the trouble of crafting effective social engineering exploits, they can always fall back on attacking vulnerabilities—a growing target. Each level of double-clicking that is removed from the malware-execution process increases its likelihood of success. This has played a huge part in the success of IRC bots in particular.

When attacking vulnerabilities, the most common targets are operating systems and popular software programs. It rarely makes sense for a virus writer to create a new, malicious exploit unless it's for an application that owns the lion's share of its market. And when that's the case, the odds are high that the application will be used by people in many countries.

There are few leading applications in the United States that are not used in other countries. In fact, most popular applications offer versions in a wide variety of languages. The same cannot be said of popular applications in other countries, especially from Asian nations. There are many games, peer-to-peer clients, and IM clients that are popular (and thus popular targets) in China, Japan, and Korea. These apps, plus a number of adware programs, are confined almost exclusively to those countries.

Conclusion

America has always been a "melting pot" of different societies, so the country's uniqueness lies in its lack of a truly homogenous culture. This multifaceted environment speaks to the rest of the world in the form of "pop" culture, through the Internet, movies, television, and music.

Phishing, spam, adware, password stealers, and bots are all increasingly common here, just as elsewhere in the world. Malware continues to use both social engineering and vulnerabilities to spread themselves. Teams of malware developers are working together to find better ways to stay ahead of security developers, with remarkable success.

Malware is an enormous international enterprise. It's unlikely, as miscreants continue to realize significant gains in income, that this problem will go away soon. The lesson for us is that regardless of where in the world we find ourselves, we must remain vigilant and deploy layered defenses against malware.

Allysa Myers is a Virus Research Lead for McAfee Avert® Labs. Her primary responsibilities are coordinating researchers and tracking global malware trends. She also discusses these new threats and trends with the press and on the Avert Labs blog. Myers especially enjoys having the opportunity to express her snarky sense of humor on the blog; she has found no better forum for discussing the security ramifications of spicy ham products and clover stolons.

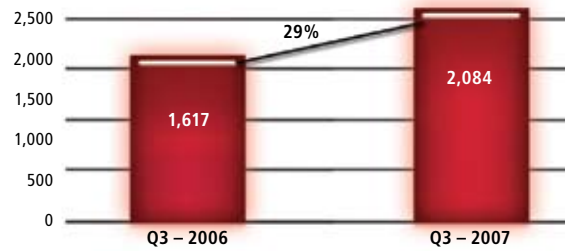
By the Numbers:

A GLOBAL VIEW OF THREATS

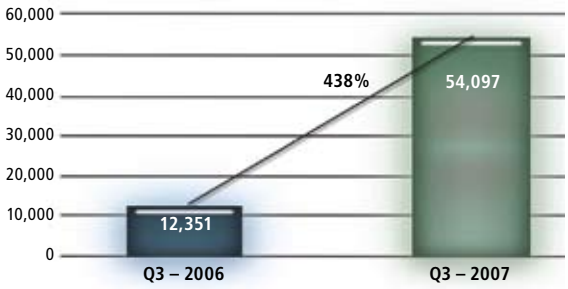
The worldwide threat landscape

The growth rate in vulnerabilities and malware has doubled in 2007 compared with 2006, according to Avert Labs data. The National Institute of Standards and Technology and the Computer Emergency Response Team Coordination Center have seen a rapid increase in vulnerabilities in recent years.

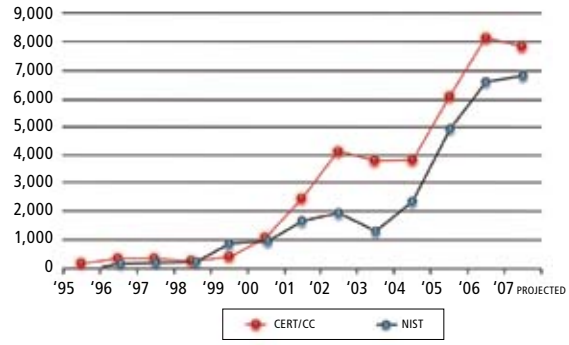
VULNERABILITIES IN NATIONAL VULNERABILITY DATABASE



NUMBER OF VIRUSES AND TROJANS



REPORTED VULNERABILITIES



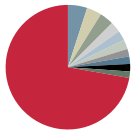
Avert Labs fun facts:

NUMBER	FACT
353,760	Total threats identified by McAfee Avert Labs (all-time total)
131,800	Threats identified by Avert Labs solely in 2007
50,000+	Samples analyzed daily by Avert Labs
325	Unique malware identified daily by Avert Labs
53,567	Unique pieces of new malware in 2006
131,862	Unique pieces of new malware in 2007
246%	Growth in malware from 2006 to 2007

Pieces of pie: Top 10 malware and spam by language

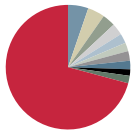
In a single day in November 2007, Avert Labs sampled malware in each of six countries. These charts show the leading malware by percentage. You might have already guessed that most spam is written in English, but how much appears in other languages? Our final pie chart shows their average popularity during the second half of 2007 in the five other tongues covered in this issue.

Japan



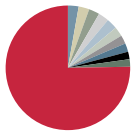
71.9%	Others	2.3%	Exploit-ByteVerify
5.0%	VBS/Psyme	2.0%	Exploit-MIME.gen.c
4.1%	JS/Exploit-BO.gen	3.0%	Exploit-ANIfile.c
3.4%	JS/Wonka	1.9%	JS/Downloader-AUD
2.9%	Winfixer	1.8%	W32/Antinny.gen!p2
2.6%	Exploit-MS06-014		

China



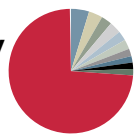
70.7%	Others	2.4%	New Malware.j
5.4%	Exploit-ANIfile.c	2.3%	New Malware.z
4.6%	VBS/Psyme	2.2%	Tool-Evid
3.2%	W32/HLLP.Philis.ini	1.9%	PWS-QQPass
3.0%	Exploit-MS06-014	1.9%	Exploit-ObscuredHtml
2.5%	ObfuscatedHtml		

Russia



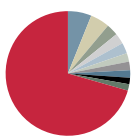
75.2%	Others	2.4%	Exploit-IEPageSpoof
2.9%	W32/Wukill.worm.gen	2.3%	JS/Downloader-AUD
2.9%	New Malware.n	2.3%	JS/Exploit-ActXComp
2.8%	New Win32	2.0%	Tool-TPatch
2.7%	VBS/Psyme	1.8%	Keygen-XPStyle
2.7%	W32/Jeefo		

Germany



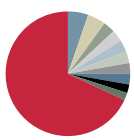
73.9%	Others	2.5%	JS/Exploit-BO.gen
4.8%	IE Window Popper	2.0%	Exploit-ByteVerify
3.6%	VBS/Psyme	1.8%	New Malware.j
3.0%	JS/Downloader-AUD	1.6%	Winfixer
2.8%	JS/Wonka	1.6%	New Malware.n
2.5%	Downloader-AAP		

Brazil



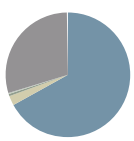
70.2%	Others	2.2%	Exploit-ANIfile.c
6.3%	VBS/Psyme	2.1%	PWS-Banker.dldr
5.0%	Exploit-MS06-014	2.1%	JS/Wonka
2.9%	New Malware.j	1.7%	JS/Downloader-AUD
2.9%	JS/Exploit-BO.gen	1.6%	New Malware.n
2.7%	PWS-Banker.gen.i		

USA



67.9%	Others	3.0%	Exploit-MS06-014
5.5%	VBS/Psyme	2.7%	Exploit-ANIfile.c
4.5%	JS/Exploit-BO.gen	2.7%	WinFixer
3.2%	JS/Wonka	2.4%	Exploit-ByteVerify
3.1%	RemAdm-PSKill	1.9%	Puper
3.1%	JS/Downloader-AUD		

Spam



67.0%	English	.13%	Japanese
29.7%	Others	.06%	Spanish
2.5%	German	.05%	Chinese
.60%	Russian		

THE LAST WORD

By Christopher Bolin

Looking back at the past year, it's apparent that the global security landscape has undergone dramatic changes. Rapidly evolving malware has grown in complexity and sophistication.

We've seen a number of new developments, including an escalation in the scope and severity of cybercrime activities. We've also witnessed a surge in data breaches that have had far-reaching consequences for individuals and even for highly reputable organizations. And, we've observed the emergence of government-sponsored cyberespionage, which has the potential to put entire nations at risk. This has created new security challenges that strain the capabilities of traditional anti-virus technologies. Clearly, the days of fighting cybercrime and data loss simply with anti-virus solutions across hosts, network perimeters, and servers are over.

In recognition of this challenge, the best defense is a holistic approach through the concept of security risk management (SRM), which marries risk and compliance. Defending multiple layers of infrastructure from ever-changing threats and exploits is one facet of SRM, but equally critical is compliance. Mandatory disclosure laws and regulatory compliance obligations have turned security into a boardroom issue.

Today integration is the watchword. The best way to counter current threats is by offering multiple technologies that interoperate and communicate through a centralized management system that automates compliance-reporting processes to respond to audits.

McAfee® Avert® Labs is also waving the banner of integration. Thanks to the tireless efforts of Jeff Green, senior vice president of product development and Avert Labs, our group has undergone a transformation that reinforces our position as one of the world's leading threat-research organizations. Jeff has been the chief architect of many positive changes. Under his leadership, we've had the lowest attrition rate ever, and we've brought in new talent with solid industry experience. We've also integrated our specialized research teams for optimized operational efficiency and the fastest possible response, and we've implemented an unprecedented level of automation that gives us detection and blocking capabilities we've never had before. Because many threats are using common technologies, we are now seeing cooperation and the sharing of information among the research groups that are working on network- and host-intrusion prevention, enveloping, shielding, and protecting host systems with behavioral rules. All of this expands our knowledge base and allows us to provide up-to-the-minute threat data to our customers.

We also publish an annual report of predictions that discusses trends and the types of threats we'll see in the coming year. In 2007, we had a phenomenal year, achieving higher-than-ever accuracy in our predictions. This level of accuracy has been the driving force in our development efforts and recent acquisitions. Our research team is also making sure that our customers know about the latest threats and trends as soon as we do by publishing more white papers, articles, and blogs. Our output in this area has increased by a factor of 10. And, of course, our major thrust is embedding this knowledge into our products.

Our reason for being has always been and will always be to enable our customers to make easier and faster security decisions, so they can set policies as quickly as possible, protect valuable assets and data, and conduct their daily operations with confidence. We look forward to continually improving our ability to help you protect what you value.

Christopher Bolin is Executive Vice President and Chief Technology Officer of McAfee, Inc. He is responsible for the worldwide development of all McAfee products. Prior to joining McAfee (then Network Associates) in 1998, Bolin was engineering director of Cyber Media, co-developed consumer anti-virus products with Trend Micro, and served as QA director at Symantec Corp.

McAfee, Inc. 3965 Freedom Circle Santa Clara, CA 95054 888.847.8766 www.mcafee.com

12-avert-sage-rpt-003-0108