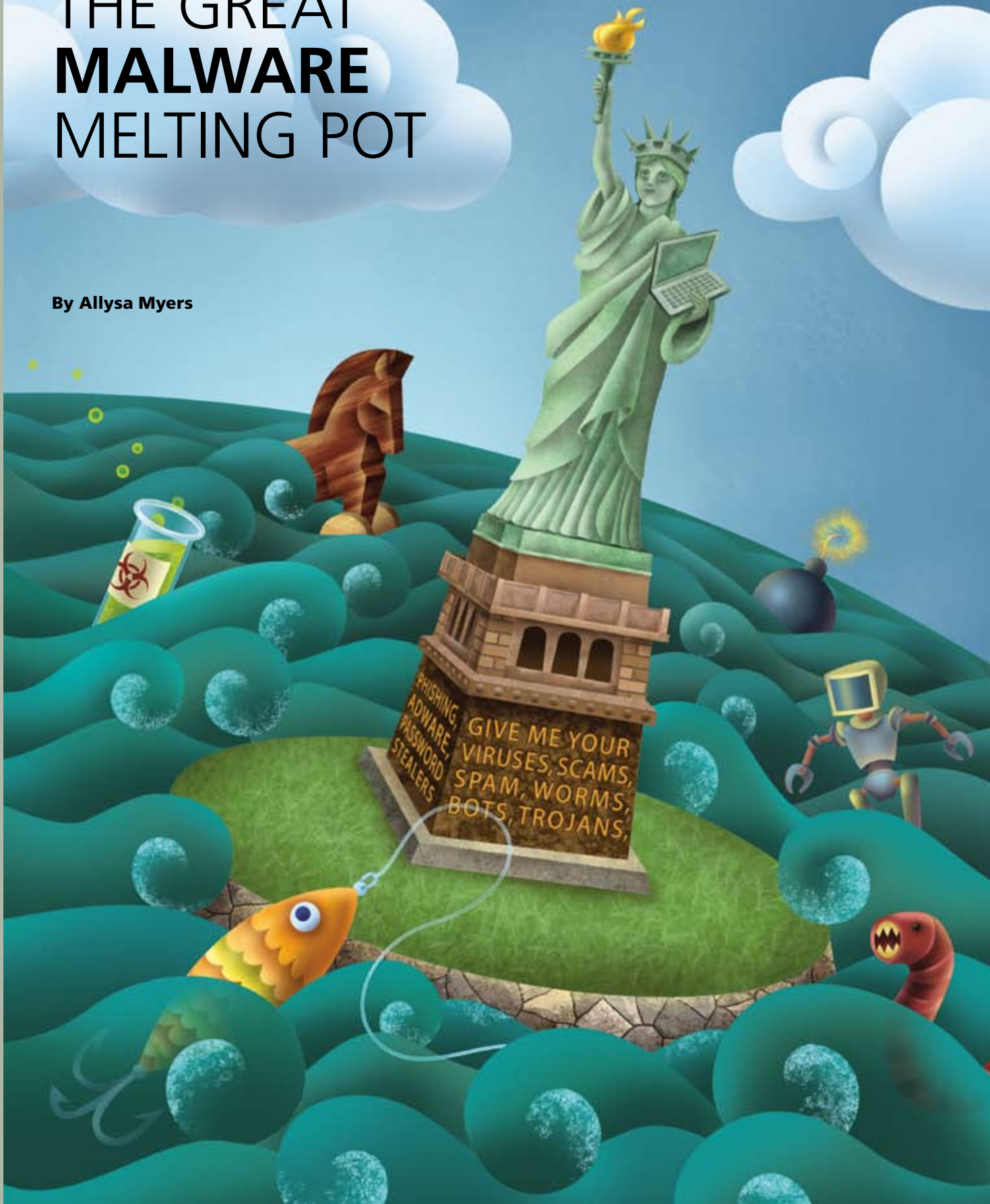


UNITED STATES:

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 the 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/newsletter7/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.

