2010 Threat Predictions

By McAfee Labs

McAfee Labs foresees an increase in threats related to social networking sites, banking security, and botnets, as well as attacks targeting users, businesses, and applications. However, in 2010 we expect to see an increase in the effectiveness of law enforcement to fight back against cybercrime.

• Social networking sites such as Facebook will face more sophisticated threats as the number of users grows.
• The explosion of applications on Facebook and other services will be an ideal vector for cybercriminals, who will take advantage of friends trusting friends to click links they might otherwise treat cautiously.
• HTML 5 will blur the line between desktop and online applications. This, along with the release of Google Chrome OS, will create another opportunity for malware writers to prey on users.
• Email attachments have delivered malware for years, yet the increasing number of attacks targeted at corporations, journalists, and individual users often fool them into downloading Trojans and other malware.
• Cybercriminals have long picked on Microsoft products due to their popularity. In 2010, we anticipate Adobe software, especially Acrobat Reader and Flash, will take the top spot.
• Banking Trojans will become more clever, sometimes interrupting a legitimate transaction to make an unauthorized withdrawal.
• Botnets are the leading infrastructure for cybercriminals, used for actions from spamming to identity theft. Recent successes in shutting down botnets will force their controllers to switch to alternate, less vulnerable methods of command, including peer-to-peer setups.
• In spite of the worldwide scope of botnets, we anticipate even more successes in the fight against all forms of cybercrime in 2010.

McAfee®

Table of Contents

McAfee®

Web Evolution Leads to Escalating Attacks

In 2009 we saw increased attacks on websites, exploit cocktails thrown at unsuspecting users, infrastructure failure via natural and unnatural causes, and "friendly fire" become a larger problem than ever. With Facebook reaching more than 350 million users, we expect that 2010 will take these trends to new heights. Criminal toolkits are evolving rapidly to use new technologies that increase the sophistication of the attack—leaving even more users blind to the risks. Malware authors love following the social networking buzz and hot spots of activity; that will continue in 2010. As Google and other providers crack down on search engine poisoning, we expect that Twitter and similar services will increase in appeal for such purposes.

Along with Twitter's success we have seen widespread adaptation of abbreviated URL services, such as bit.ly and tinyurl.com. These services now appear in all sorts of communications—making it easier than ever to mask the URLs that users are asked to click. This trick will play a more predominant role in 2010; it's the perfect avenue to direct users to websites that they would normally be wary about visiting.

As users expectations of their Web 2.0 services evolve, we expect to see many rogue services set up with the hidden purpose of capturing credentials and data. Users blindly distribute applications; with the widespread availability of stolen credentials it could become very easy to launch and share these rogue apps across a wide population. The audience is there: Facebook boasts more than 350,000 active applications[1] and Apple's App Store recently reached the 100,000 mark.[2] And that's not counting the numbers in other markets. Wherever and whenever a trusted mainstream website distributes or promotes third-party content, attackers seek to abuse the trust relationship established between the site and their users. Why? Because it works. Users often let down their guard when clicking hyperlinks sent from their friends, or when installing applications offered by well-known sites.

The preceding are the attacks and trends that the general population should expect to see—and beware of—during 2010. However, there are quite a few emerging technologies that present new risks. Although we do not expect to see widespread attacks with these technologies, we do expect to see activity and proof-of-concept attempts. So when the general population embraces the new, the cybercriminals will be ready.

With the technological advances brought on by HTML 5, the web will undergo a dramatic upgrade that will change the way web application developers and hackers are able to interact with their "target market." HTML 5 holds all the promises that today's web community seeks—primarily blurring and removing the lines between a web application and a desktop application. HTML 5–based attacks will become even more tempting once the Google Chrome Operating System is released. (It's scheduled for second half of 2010.) Google Chrome OS is intended for use with netbooks, and HTML5 enables not only a rich Internet experience, but also offline applications. Another motivation for attackers is HTML 5's anticipated cross-platform support, which will allow attackers to eventually reach users of many mainstream browsers.

Prior to the full release of Google Chrome OS, the company plans to release Google Wave, adding another new attack vector. Google Wave is designed to combine collaboration and real-time social networking capabilities into a full web-based service—while also combining all of the security risks associated with these communication vehicles into one service. At its core Google Wave uses XMPP (eXtensible Messaging and Presence Protocol), which provides Wave applications with a decentralized application-to-application control model. This arrangement will give cybercriminals another weapon to create redundancy in their networks and make them even more difficult to disrupt. With Twitter also serving as a control vehicle for botnets, the trend of botnets riding on top of commonly used applications and protocols will continue to make botnet communication traffic more difficult to detect and prevent.

1. Press Room: Statistics, Facebook. http://www.facebook.com/press/info.php?statistics
2. "Apple Announces Over 100,000 Apps Now Available on the App Store," Apple. http://www.apple.com/pr/library/2009/11/04appstore.html

McAfee®

Targeted Attacks on the Rise

Email is increasing in popularity as the preferred method for targeting attacks against individual users, corporations, and government institutions. Although such attacks were rare some years ago, we now see many reports of successful assaults, both by criminals and for espionage, in which an email with an attachment or a link to a website is the attack vector. Those emails have been specifically crafted to get the attention of a particular individual. The success of such attacks is certainly helped by vulnerabilities in a number of popular applications that process and display attached documents or media files. These security holes allow malware to install Trojans when users open files that most people expect to be benign. We anticipate that these attacks will continue to increase in 2010.

In 2009 a couple of major incidents represented the tip of the iceberg, as such incidents are rarely made public. In March, following a ten-month investigation, authorities disclosed the "GhostNet," a network of at least 1,295 compromised computers in 103 countries. The machines primarily belonged to government, aid groups, and activists. The attack was carried out by emails with subject lines related to the Dalai Lama or Tibet. The emails carried malicious attachments that connected the infected machines to systems located in China. (No evidence suggests the Chinese government was involved.)
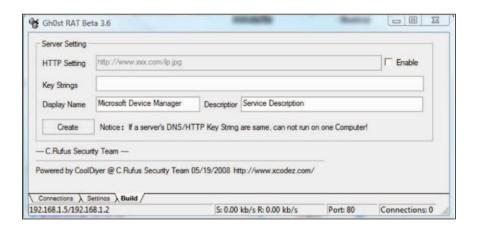

Figure 1: Gh0st RAT, a toolkit for developing Trojans, has been distributed primarily by members of the C. Rufus Security Team (CRST), through their website wolfexp.

The Swiss organization MELANI, the Reporting and Analysis Centre for Information Assurance, has reported a very targeted wave of attacks against the management of major companies. An email with an attachment referring to a wire transfer was used in this attack. When the victim opens the attachment, an .rtf file, malware installs that records all directories accessed with Windows Explorer, all websites visited, and all data entered in forms. The malware then sends this information to various servers.
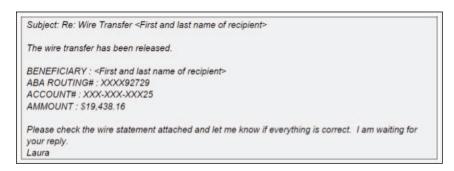

Figure 2: This wire transfer email carries a malicious attachment. (Source: MELANI)

Another example shows that not only top management or governments can be victims. Journalists have suffered, as well. An attack in September targeted journalists from various media organizations, including Agence France Press, Dow Jones, and Reuters based in China. The attacks seemed to come from an editor of the *Straits Times*, an English-language paper in Singapore, with an attachment in PDF format. Opening the attachment exploits a vulnerability in Adobe Acrobat and results in malware being installed that connects to compromised computers in Taiwan. The timing corresponds with the 60th anniversary of the founding of the People's Republic of China, but there is again no evidence of any involvement by the Chinese government. Anti-virus software detection of the attachment was very low; that's typical in targeted attacks. Before starting an assault, the attackers make sure that their Trojans will not be detected by most anti-virus products, a task made easier when websites don't forward malware samples to security companies.

From: Pam [mailto:pam.bourdon@yahoo.com]
Subject: Trip to Beijing

Please can you both confirm that you received this e-mail I sent a few days ago. Given recent e-mail problems I am worried that it has gone astray yet again.

Dear,

I am the economics editor of The Straits Times. I plan to be in Beijing October 2nd, (arriving late evening) to research the annual world economy survey.
I was suggested that you would be able to help me fix up some interviews.
I attach a list of people I would like to meet with. I would be happy with just 6-7 interviews during my stay, so don't worry if some of them are away. If a lot of my chosen economists are unavailable, I will have a few more names.
I think that they are all Chinese speakers, but please check for me as I find that discussing technical economics through a translator does not work very well.

I will be staying at the China World Hotel, No. 1 Jian Guo Men Wai Avenue .
From past experience, it would be good if meetings could be grouped to minimise getting stuck in bad traffic!

The subject I am researching is the implications for the world economy, and in particular the developed economies, of the increasing
global importance of China, India and the other emerging economies. How is the increased weight in the world of emerging economies affecting growth rates, jobs, wages, profits, commodity prices, inflation, interest rates, asset prices, capital flows and exchange rates? Who will be the winners and losers in this new economy?

Please let me know if you need any more information.
And thank you in advance for helping me arange my trip.

Best regards

Pam

Figure 3: This email from appeared to come from *The Straits Times*. It included a malicious PDF targeted at journalists. (Source: http://www.infowar-monitor.net)

We've named just a few examples of targeted attacks that occurred in 2009. Although exact numbers are often classified, a number of agencies report a major increase in such targeted attacks against the governments of various countries compared with last year. We expect this trend to continue in 2010. Home users and IT personnel should provide extra protection for computers used by any person or organization that is likely to be attacked.

McAfee

Malware Writers Love Adobe, Microsoft Products

In 2009 McAfee Labs saw an increase in attacks targeting client software.[3] The favorite vector among attackers is Adobe products, primarily Flash and Acrobat Reader. Using reliable "heap spray–like" and other exploitation techniques, malware writers have turned Adobe apps into a hot target. Further, Flash and Reader are among the most widely deployed applications in the world,[4] which provides a higher return on investment to cybercriminals. Based on the current trends, we expect that in 2010 Adobe product exploitation is likely to surpass that of Microsoft Office applications in the number of desktop PCs being attacked.

Sensors in McAfee Labs also recorded many SQL-injection assaults aimed at web servers. These attacks included some live attempts from the Danmec bot. We expect that automated SQL-injection attacks will continue, leveraging badly configured web servers. These attacks have been on the rise because "traditional" server vulnerabilities allowing mass propagation continue to decline.[3]

The holiday season continues to be a popular time for attackers to launch their assaults. During the past five years, we have seen consistent reports of zero-day exploits targeting Microsoft Internet Explorer in November and December. With so many people going online and looking for good deals, this is a "click friendly" time of year.

Zero-Day Vulnerability	Microsoft's Acknowledgement of Exploitation	Date of Patch Release
Mismatched Document Object Model Objects Memory Corruption Vulnerability—CAN-2005-1790: KB(911302)	November 21, 2005	December 13, 2005
Microsoft XML Core Services Vulnerability—CVE-2006-5745: KB(927892)	November 3, 2006	November 14, 2006
Windows URI Handling Vulnerability—CVE-2007-3896: KB(943521)	October 10, 2007	November 13, 2007
Pointer Reference Memory Corruption Vulnerability—CVE-2008-4844: KB(960714)	December 10, 2008	December 17, 2008
Vulnerability in Internet Explorer Could Allow Remote Code Execution—CVE-2009-3672: KB(977981)	November 23, 2009	December 8, 2009

Banking Trojans Grow Smarter as They Follow the Money

In 2009 criminals adapted their methods to more effectively attack online banking and get around current protections used by banks. Trojans demonstrated new tactics that went well beyond the rather simple keylogging-with-screenshots efforts that we had seen in previous years.

Most Trojans now use rootkit techniques to hide on a victim's system and disable anti-virus software or prevent signature updates. Often the victim's computer becomes part of a botnet and receives malware configuration updates.

Simple Trojans, such as those predominant in South American countries, lie dormant until the victim opens the bank's website. They then add fields for the user to fill in, asking for credit card number and ATM PIN, for example, or for a couple of indexed transaction authorization numbers (iTANs). The Trojan usually comes with a configuration file that contains information for hundreds of banks, specifying the additional fields and their layout and mimicking the bank's design. Although these Trojans, such as Torpig, are still popular today, they are far from state of the art.

More troublesome is the Silentbanker family. These Trojans can silently change the details a user enters to transfer the money to the attacker during a transaction. The user is not aware that anything is amiss until the next account statement arrives. Bebloh, also known as URLZone, takes this deception even

3. "The Changing Face of Vulnerabilities," *McAfee Security Journal*, Fall 2008. http://www.mcafee.com/us/local_content/misc/threat_center/msj_changing_face_vulnerabilities.pdf
4. "Flash Player penetration," Adobe. http://www.adobe.com/products/player_census/flashplayer/
"Adobe Flash Player PC Penetration," Adobe. http://www.adobe.com/products/player_census/flashplayer/PC.html

further. This Trojan not only changes the transaction details to suit the attacker but it will also check the user's account and transaction limits and stay just below them to avoid alerting the bank. Bebloh also keeps track of the transactions the user originally made and changes the account statement to display these instead of the real transactions. Of course, the account balance is modified as well.

The latest, and perhaps most worrisome, development comes from the Zeus family. These Trojans are frequently updated with new versions and are sold on underground forums to anyone interested in starting a career in crime. Zeus comes with a command and control server and is extremely flexible in its configuration, allowing easy adjustments to a criminal's specific needs. Now there is a man-in-the-middle console that allows an attacker to operate in real time. The attack could occur like this: When the victim logs into an online banking account the user sees a maintenance bar that moves slowly until it is full, and then must answer additional security questions, with everything in the bank's website design. These steps help buy time for the attacker. The moment the victim logs in, the attacker is notified and initiates a transaction while the victim is waiting. In the next step the victim is asked to register his or her mobile phone number and to confirm this with a specific iTAN. The attacker uses this iTAN, which the bank requests, to complete the illicit transaction. Once the victim enters the iTAN, the attacker completes the transaction and the victim gets to see a message saying the phone registration was successful but that online banking is closed for maintenance.

One variant of Zeus is JabberZeus, which has a complex structure for providing near real-time stolen information to an attacker. This version is most often used to steal one-time passwords, which certain banks require to add another layer of protection for large transactions. With this variant, an attacker uses the Jabber protocol as an instant message system to gather the stolen data. The attacker then selects which information is most (financially) important.

Given the widespread use of the Zeus kit we anticipate many more similar attacks in 2010, and not only against banking sites. This variation allows attackers to circumvent all types of two-factor authentication on websites.

Botnet Warfare in the Trenches

During the last six years, botnets have become the biggest thorn in the side of cybersecurity professionals. Botnets have become the essential infrastructure used by cybercriminals and nation-states for launching nearly every type of cyberattack: from data exfiltration and espionage to spam and distributed denial of service. By using an extremely cheap-to-acquire and seemingly infinite supply of stolen computing power and bandwidth across the globe, attackers can not only amplify the impact of their attacks but also hide their true identities and locations behind numerous hops of compromised machines in their service.

To combat this growing menace, security researchers and key infrastructure partners from telecommunications and domain-registration communities have begun to strategically target and shut down the control infrastructure of most threatening botnets. The goal is to deny this essential capability to the criminals and reduce the threat traffic traversing the Internet. In many cases the targets in the crosshairs of the security community have been illicit ISPs that provided "abuse complaint–resistant" hosting for numerous cybercriminal operations. These services have not been quickly shut down in spite of complaints of criminal conduct emanating from that hosting space. ISPs and domain registrars such as Russian Business Network, McColo, Atrivo, 3FN, UkrTelegroup, and EstDomains have long been favorite places to park control servers through which the botnet owners would issue commands and updates to their global networks of zombies.

As a result of aggressive efforts to take offline these service providers that cater predominantly to the cybercriminal element, as well as of direct targeting of specific botnet control channels, numerous botnet operations have been severely disrupted in recent years. Successes include the temporary shutdown in 2008 of the Rustock, Srizbi, and Mega-D spam botnets, whose control servers had been hosted at the McColo ISP. For a few months the shutdown resulted in a 60 percent to 70 percent worldwide reduction in global spam volumes—until the criminals recovered and moved their servers to

other locations. Earlier this year, a consortium of security companies and domain registries and registrars in coordination with ICANN was able to hijack the domain-based control method used by the Conficker botnet and effectively deny the villains the use of nearly seven million compromised machines. In recent weeks, we have again seen the temporary shutdown of the Mega-D spam botnet by unrelenting security researchers. Although in nearly every case the success has been short-lived—with criminals able to restore control or recreate their botnets in a few months or even weeks—there is evidence that this type of tactical response to threats has caused great irritation and loss of business to cybercriminals.

In 2010, we expect to see a significant trend toward a more distributed and resilient botnet infrastructure that relies much more on peer-to-peer technologies rather than on the centralized hosting model that is prevalent today. Although we have seen some experimentation with this approach as far back as 2006 with the Storm and Nugache botnets, peer-to-peer control has not become the preferred method of operation among the majority of botnets. Why? It's due to the previous lack of incentive for the implementation and support of this more costly and sophisticated technology. We expect 2010 to be a significant year for the adoption of peer-to-peer control as the benefits finally outweigh the costs—due to the security community's increasingly aggressive attempts to shut down and deny access to these botnets.

Cybercrime: a Good Year for Law Enforcement

International law enforcement began to recognize the scope and the threat of the cybercrime problem nearly 10 years ago, as the widespread potential for economic damage and disruption was demonstrated very vividly by the crippling MafiaBoy attacks on Yahoo, Amazon, eBay, and other high-profile ecommerce sites in February 2000. By fall 2002, the FBI had formed a Cyber Division and shortly afterwards deployed Cyber Squads in all of its 56 field offices across the United States to focus on this emerging threat. At the same time, the U.S. Secret Service, Australian Federal Police, Royal Canadian Mounted Police, U.K. National Crime Squad, and law enforcement organizations in other parts of the world were reorganizing themselves to create high-tech crime centers dedicated to investigations of cybercrime. A few years later, we began to witness the first successes of this new focus, culminating in the conclusion of Operation Firewall in October 2004. Firewall was the first large and global multinational cybercrime investigation. It resulted in nearly three dozen arrests in seven countries and the shutdown of Shadowserver and Carderplanet forums that provided the infrastructure, training, and recruiting to facilitate cybercrime operations around phishing, spamming, malware distribution, and identity theft.

The worlds of law enforcement and justice have had about a decade to deal with highly organized and financially motivated cybercriminals. We finally have nearly universal recognition among global governments of the severity of this problem, and we can see significant progress from these years of relationship building, education, and training among international law enforcement organizations. This progress has been slow in coming but we now see clearly demonstrated to criminals that engaging in cybercrime has become an activity with a rapidly increasing risk of incarceration, regardless of their country of residence.

A few recent cases illustrate that the tide may finally be turning. In November 2009 the U.S. Department of Justice indicted nine individuals from Russia, Moldova, and Estonia who were allegedly responsible for US$9 million in customer payroll data compromises at RBS WorldPay. This action demonstrates the increasing level of cooperation and coordination between law enforcement agencies of countries of the former Soviet Union—the birthplace of financially motivated cybercrime and from which the majority of it continues to emanate—and Western law enforcement. In the same month we saw the conviction of the infamous "Godfather of Spam," Alan Ralsky of Michigan, and his criminal syndicate, which was responsible for generating a significant portion of the world's unsolicited email and virtually all of the stock pump-and-dump manipulation spam. This type of spam decreased from a near 20 percent market share of all spam in 2007 to near 0 percent after the January 2008 arrests of Ralsky's cybercrime gang.

These recent developments are just a few examples of numerous law enforcement successes in tracking, identifying, and ultimately arresting individuals engaging in cybercrime on a global scale. Virtually all of the arrests have been a result of difficult, years-long work to build up relationships, institutions, and

trained personnel capable of dealing with this sophisticated and transnational threat. McAfee believes that in 2010 we'll see many more successes in the pursuit of organized cybercriminals. The cooperation among international cybercrime-fighting agencies is now tighter than ever, and the cybercrime Elliott Nesses of today have the computer and network sophistication that their predecessors could not dream of just 10 years ago. We look forward to seeing more cybercriminals around the world arrested and placed behind bars in the coming months!

About the Authors

This report was written by Dmitri Alperovitch, Toralv Dirro, Paula Greve, Rahul Kashyap, David Marcus, Sam Masiello, François Paget, and Craig Schmugar of McAfee Labs.

About McAfee Labs

McAfee Labs is the global research team of McAfee, Inc. With the only research organization devoted to all threat vectors— malware, web, email, network, and vulnerabilities—McAfee Labs gathers intelligence from its millions of sensors and its cloud-based reputation technologies such as Artemis and TrustedSource. McAfee Labs' 350 multidisciplinary researchers in 30 countries follow the complete range of threats in real time, identifying application vulnerabilities, analyzing and correlating risks, and enabling instant remediation to protect enterprises and the public.

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. www.mcafee.com.