



M86 Security Labs: Threat Predictions 2011

Introduction

A year makes a big difference when it comes to Web and email security. In 2010, scareware has become more nefarious, mimicking Microsoft's Security Essentials, Windows Automatic Updates and even browser-based attack warnings used by Mozilla Firefox and Google Chrome. Malware such as GootKit and Asprox have been used to compromise websites in mass through stolen FTP credentials and vulnerabilities in ASP pages. Furthermore, cybercriminals used shortened URLs to obscure malicious links in spam messages, tweets and Facebook status updates.

As 2011 approaches, we look to the future to determine what's in store for tomorrow's threat landscape. Below are eight of the top trends we expect to see in the next year.

1. Malware Will Increasingly Use Stolen Digital Certificates to Bypass Whitelisting and Code Signing Requirements

Though nothing new, this issue gained notoriety following the discovery of the Stuxnet malware, which was intended to target a specific set of industrial systems and reprogram them. In analyzing Stuxnet, it was observed that the malware was digitally signed (certified) with two legitimate certificates. Soon thereafter, a variant of the Zeus Trojan was discovered to be digitally signed using a certificate from antivirus vendor Kaspersky.

This trend is alarming because Windows Vista, Windows 7 and many other products check the validity of digital signatures and warn or deny users when a certain type of software is not digitally signed. When cybercriminals use stolen certificates to digitally sign their malware, they bypass this protection with ease.

We expect this trend to increase in the coming year as cybercriminals continue to experiment with different ways to avoid detection and lower victims' suspicion levels.

2. Exploding Smartphone Market and Growing Tablet Demand Lead to More Mobile Malware

Since the introduction of the iPhone, the smartphone market has grown over the last several years. And the introduction of tablet devices such as the Apple iPad, HP Slate and Android-based tablets signals a potential shift in which cybercriminals target end users via mobile platforms. As with other platforms, the attackers will go where the most users are, and where these users are the least protected.

Top Smartphone Platforms Sep. 2009 to Aug. 2010		Share (%) of Smartphone Subscribers				
		Sep 2009	Dec 2009	May 2010	Aug 2010	Point Change
Total Smartphone Subscribers	100%	100%	100%	100%	N/A	
RIM	42.6%	41.6%	41.7%	37.6%	- 5.0	
Apple	24.1%	25.3%	24.4%	24.2%	- 0.1	
Microsoft	19.0%	18.0%	13.2%	10.8%	- 8.2	
Palm	8.3%	6.1%	4.8%	4.6%	- 3.7	
Google	2.5%	5.2%	13.0%	19.6%	17.1	

Total U.S. Smartphone Subscribers Ages 13+
Source: comScore MobiLens

A recent discovery found that a new variant of the Zeus malware was released with the intention of targeting users of Nokia phones which run the Symbian OS. This malware was used to defeat online banking two-factor authentication, monitoring the SMS messages sent by banking institutions to their customers for fraud protection.

Google's mobile operating system, Android, has increased from a [2.5% market share](#) in September 2009 to [19.6% in August 2010](#). The mobile operating system is also slated to be included in numerous tablet devices in the coming months.

Apple's iOS platform is a closed system, and the application approval process for its Application Store is restrictive. Despite this, multiple vulnerabilities have been discovered for the iPhone, including the [vulnerability](#) that was exploited to "jailbreak" (remove the restriction on which applications can be installed) the iPhone.

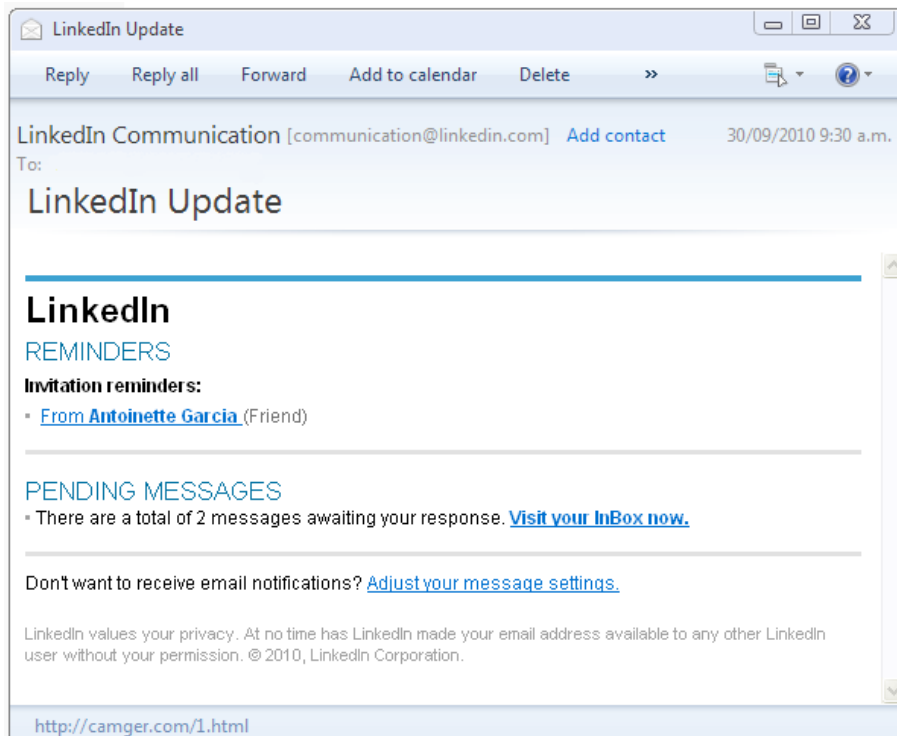
Google's Android platform is open source, and its application approval process is less restrictive, allowing most applications to be submitted and approved. Additionally, users of Android-based phones have a setting that allows users to install applications from outside Google's App Store.

So far, Android has seen rogue applications such as a "Movie Player," which secretly sends SMS messages to a premium rate number, costing the end user several dollars per message. Other applications have harvested information such as a user's SIM card number and voicemail password, sending it to a server in another country.

This is just the beginning. As smartphone adoption grows and new devices are released (Windows 7 phones and tablet devices), and the focus shifts towards the tablet platform, we anticipate malware targeting all mobile platforms to increase in 2011.

3. Spam Campaigns Will Increasingly Mimic Legitimate Mail from Popular Websites

While we have seen messages like these before, we've noticed that they now look more legitimate than in the past. Examples of this include spammers who targeted [Amazon/Flixster/GoDaddy names](#) and a [FedEx campaign](#). In the case of [LinkedIn spam messages](#), we observed that the headers and body templates were taken from actual LinkedIn messages. Therefore, it's nearly impossible for the average user to distinguish between the legitimate LinkedIn messages and the nefarious ones.



E-commerce sites like Amazon.com and logistic services companies like FedEx are used by millions of people worldwide who are accustomed to receiving receipts and shipping confirmations from them. Therefore, they are ideal targets for spammers who want to mimic these types of messages to trick users into downloading malware or clicking on a link that leads to a malicious payload.

Whether it's Facebook notifications, LinkedIn updates or bank statements, we expect this trend to increase. Spammers will continue to perfect the faux spam templates they use to convey a sense of legitimacy when targeting end users, making it difficult for users to differentiate between good mail and potentially malicious spam.

4. Data-stealing Trojans Will Become More Sophisticated

The name Zeus is synonymous with cybercrime. This data-stealing malware has been used over the last three years to perpetrate hundreds of thousands of eBanking fraud cases against consumers. Aided by money mules, it has also been used to siphon large amounts of money from businesses and school districts.

Trojans such as Zeus have become more sophisticated, inserting forms onto legitimate banking websites, spoofing bank statements and even moving into man-in-the-browser attacks which take over users' banking sessions after they login. They present users with phony Web pages, showing funds and transactions that look normal, while pilfering money behind the scenes.

Zeus received intense media scrutiny after M86 Security Labs discovered an attack on customers of a major UK financial institution, spurring arrest warrants for those who were responsible. As a result, pressure is mounting against Zeus, driving the advancement and creation of other Trojans such as Carberp, Bugat and SpyEye, and malware authors are finding new ways to evade detection and keep the money flowing. One option is for them to move beyond Internet banking and financial institutions—perhaps to take over a user's Amazon.com account and ship goods to drop points via goods mules.

With the [recent news of a SpyEye and Zeus merger](#), the potential for more sophisticated banking Trojans is even higher.

5. On Social Networks, More Users and More Integration Lead to More Problems

It's no surprise that Facebook recorded its 500 millionth user this year. The service has become the de-facto social network used today. Additionally, Twitter, which has seen its popularity soar in the last few years, is on pace to reach 200 million users by the end of 2010. When you add these two up, you have a pool of 700 million users that cybercriminals can target.

From recent cross-site scripting (XSS) and cross-site request forgery attacks to the "likejacking" attacks, increase in spam and sensationalized headline applications on Facebook, cybercriminals are constantly tooling and retooling, finding ways to exploit the social networks. This is because there is more success and payoff in assuming the identity of someone a user knows than in pretending to be a Nigerian Prince.

The major problem is that the users of these services have a more lax approach when it comes to security. The networks themselves have made strides to try to combat the threats their users face. However, as the platforms grow and integrations happen (Skype and Facebook), cybercriminals continue to find new and interesting ways to target the users of these services.

The reason for the lax security posture is that there is an inherent trust placed in the service. The people that are a part of the "social network" are friends — people users trust. When a trusted person posts a link, the people in this user's social network are more likely to click on it.

We expect this trust to continue to be exploited, as cybercriminals will pursue this huge target among the various social networks.

6. As a New Standard, HTML5 Will Become the New Target for cybercriminals

When it comes to new platforms and standards, a phase of experimentation takes place for legitimate use cases. HTML5 is a cross-platform standard for Web browsing, and to meet the need of this new standard, support has already started shipping for it in newer versions of popular Web browsers such as Internet Explorer 9. Apple has already positioned HTML5 in the latest release of its Safari browser, which is used on its Mac devices as well as its mobile platform devices like the iPhone, iPod Touch and iPad.

While developers are experimenting with HTML5 for legitimate purposes, cybercriminals are finding ways to exploit the standard for malicious reasons.

Browser usage is split more than ever before, with Internet Explorer no longer holding its dominant share of the market. Therefore, it would be beneficial for cybercriminals to target HTML5, as its appeal lies in the fact that it will have cross-platform support. HTML5 features support for scripting APIs (application programming interfaces) which could easily be used by cybercriminals.

As browser support grows and Web application developers implement HTML5, we expect cybercriminals to find ways to exploit this new technology in the coming year.

7. Malware-as-a-Service (MaaS) Offerings Will Increase as an Alternative to Malware Applications

Exploit kits, also known as “attack toolkits,” have become popular with cybercriminals over the last couple of years. Used as “Command Control” for cyber attacks, exploit kits have lowered the entry level to cybercrime and given birth to a new ecosystem with different players and roles.

Our research indicates that a shift is occurring whereby exploit kit developers have started to provide services (instead of/in addition to) classical application offerings. For example, the NeoSploit and Phoenix exploit kits offer different malware services to their customers. With the NeoSploit kit, customers can purchase a specific Web server configuration that redirects victims’ requests to a Neosploit back-end server, which is apparently handled by the NeoSploit team.

Different “suppliers” can be used to provide active vulnerabilities and the exploits that use them, or to get help in driving traffic past infected websites. In the same way the commercial world is embracing cloud-delivered services, cybercriminals will also become better organized, offering a complete suite of services in one place.

While we do not anticipate a decline in the usage of exploit kits, we do believe there will be more service offerings for cybercriminals instead of just application offerings.

8. Botnets Will Thwart Future Takedowns; Smaller Botnets Will Become More Prevalent

In 2010, we’ve seen a number of takedown attempts against various botnets. At the beginning of the year, the Lethic spambot was taken down briefly, only to return soon after. In August, attempts were made to takedown the Pushdo botnet. Unfortunately, these efforts were short-lived. Like Lethic, Pushdo returned not long after. Microsoft used legal action to shut down the Waledac botnet, and there was another effort made to bring down the Mariposa botnet. Most recently, the operator of the Bredolab botnet was arrested, and Dutch authorities seized the servers controlling the Bredolab botnet.

With these takedowns, a message has been delivered to botnet operators around the globe that efforts are being made by law enforcement and security researchers to bring them down. Therefore, it’s clear that botnet operators will need to reevaluate their operations going forward in order to thwart future takedown attempts. We expect to see the command and control architectures become more and more layered and complex, making it difficult for security researchers and authorities to bring down the entire bot networks.

In addition to these stories, we’ll discuss the many security issues noted in the second half of 2010 in the upcoming recap report from M86 Security Labs.

ABOUT M86 SECURITY

M86 Security is the global expert in real-time threat protection and the industry’s leading Secure Web Gateway provider. The company’s appliance, software, and Software as a Service (SaaS) solutions for Web and email security protect more than 25,000 customers and 26 million users worldwide. M86 products use patented real-time code analysis and behavior-based malware detection technologies as well as threat intelligence from M86 Security Labs to protect networks against new and advanced threats, secure confidential information, and ensure regulatory compliance. The company is based in Orange, California with international headquarters in London and development centers in California, Israel, and New Zealand.

TRY BEFORE YOU BUY

M86 Security offers free product trials and evaluations. Simply contact us or visit www.m86security.com/downloads



Corporate Headquarters
828 West Taft Avenue
Orange, CA 92865
United States
Phone: +1 (714) 282-6111
Fax: +1 (714) 282-6116

International Headquarters
Renaissance 2200
Basing View, Basingstoke
Hampshire RG21 4EQ
United Kingdom
Phone: +44 (0) 1256 848 080
Fax: +44 (0) 1256 848 060

Asia-Pacific
Suite 3, Level 7, 100 Walker St.
North Sydney NSW 2060
Australia
Phone: +61 (0)2 9466 5800
Fax: +61 (0)2 9466 5899

Version 11/14/10