

# 2011 Threats Predictions

By McAfee® Labs™

The threats landscape has changed considerably in the past year. McAfee Labs has seen marked increases in malware sophistication and targeting as well as a continued increase in the overall volume of daily malware threats. We have also begun to see some very significant changes in the types of threats that aim at Apple iPhones and other mobile devices. But there is good news, too, primarily a significant decrease in the daily amounts of email spam we combat. These ups and downs lead us to wonder how threats are evolving.

As we have done for the past several years, McAfee Labs is ready to dust off our crystal ball and offer our fearless predictions of the threats of the upcoming year and beyond. We urge you to consider these ideas to prepare for the ever-evolving threats of the future.

## Table of Contents

Exploiting Social Media	4
Mobile	4
Apple	5
Applications	5
Sophistication Mimics Legitimacy	5
Botnet Survival	6
Hactivism	6
Advanced Persistent Threats	6
About the Authors	7
About McAfee Labs™	7
About McAfee, Inc.	7

*“Social media connections will eventually replace email as the primary vector for distributing malicious code and links.”*

### Exploiting Social Media

In 2010 we saw some significant changes in how both malicious code and malicious links are distributed. This year ended with some of the lowest global email spam levels in years, as more and more users transition from “slower” legacy communications such as email in favor of more immediate methods such as instant messaging and Twitter. This shift will completely alter the threat landscape in 2011.

As both consumer and business users continue to flock to social media and networking sites for immediate communications and data sharing, we expect to see increasingly more targeted abuses of personal identity and data. Social media connections will eventually replace email as the primary vector for distributing malicious code and links. The massive amount of personal information online coupled with the lack of user knowledge of how to secure this data will make it far easier for cybercriminals to engage in identity theft and user profiling than ever before. Spear phishing—targeted phishing attacks—will move to Twitter and like technologies because choosing users and groups to exploit through these channels is simple.

Two related areas of social media will also attract attention next year: short URLs and locative technologies.

*Short URL Service Abuse:* Short URLs make sense when used in social media as well as in other forms. Short links are easier to paste or type. The trouble—and abuse—follows because users do not know where these shortened links actually lead until they click them. This is a huge opportunity for abuse. Spammers have already latched onto short URLs to evade traditional filters. McAfee Labs expects to see short URL abuse invade all other forms of Internet communications. We currently track and analyze—through multiple social media applications and all URL shortening services—more than 3,000 shortened URLs per minute. We see a growing number of these used for spam, scamming, and other malicious purposes. This nominal convenience will have a tremendous impact on the success of cybercriminals and scammers as they leverage the immediacy of social media over email for even greater success.

*Locative Service Abuse:* More Internet users at all levels are adding global positioning system (GPS) information to their social media updates so their friends and colleagues can see where they are. Many locative services also offer users badges and rewards to increase their popularity. There’s no trick to imagining how cybercriminals and scammers can potentially leverage this information: With locative services such as foursquare, Gowalla, and Facebook Places you can easily search, track, and plot the whereabouts of friends and strangers. Use Bing’s mapping functionality, for example, and plot all the GPS-enabled tweets in an area. It is easy to correlate these by topic or area of interest. In just a few clicks cybercriminals can see in real time who is tweeting and where, what they are saying, what their interests are, and the operating systems and applications they are using. It then becomes child’s play to craft a targeted attack based upon what the bad guys have just learned from these services.

The fact that these services allow anyone to see and track individuals and groups—including their likes and dislikes, affiliations and interests—and then act on them in Internet time will make this topic a huge focus for cybercriminals and scammers in 2011 and beyond.

### Mobile

Threats to mobile devices have been a hot topic within the security community for several years; we expect attacks to erupt at any time, yet they never quite seem to happen. Nonetheless, McAfee Labs predicts that 2011 will be a turning point for threats to mobile devices. This year we saw many new, but low-prevalence, threats to mobile devices: rootkits for the Android platform, remote “jailbreaking” exploits for the iPhone, and the arrival of Zeus (a well-known banking Trojan/botnet). The widespread adoption of mobile devices into business environments combined with these and other attacks is likely to bring about the explosion we’ve long anticipated. Given our historically fragile cellular infrastructure and slow strides toward encryption, user and corporate data may face serious risks.

### Apple

Any security professional who cruises online InfoSec forums or attends conferences will know that the Mac OS X platform is a favorite target of the whitehat and blackhat communities. Whitehats have been poking at the Mac for a long time looking for vulnerabilities. Although historically not a frequently targeted platform by malicious attackers, the Mac operating system is very widely deployed. McAfee Labs saw malware of increasing sophistication that targets Mac this year; we expect this trend to increase in 2011. The popularity of iPads and iPhones in business environments and the easy portability of malicious code between them could put many users and businesses at risk next year and beyond. We anticipate threats of data and identity exposure will become more pronounced. The lack of user understanding regarding exposure on these platforms and the lack of deployed security solutions make a fertile landscape for cybercriminals. McAfee Labs expects to see botnets and Trojans move from a rare encounter to a more common occurrence on Apple platforms in 2011.

### Applications

Regardless of our choices of platform or device, we live in an application-centric world. The drawback to that world lies in the portability of our apps among mobile devices and the coming Internet TV platforms, which combined will make threats from vulnerable and malicious apps a major concern for 2011. In addition to malicious code, McAfee Labs expects to see apps that target or expose privacy and identity data. This danger will eventually lead to data exposure and threats through new media platforms such as Google TV.

As home-, work-, and device-controlling apps become more popular, they will increasingly become targets. These tools have historically weak coding and security practices, and will allow cybercriminals to manipulate a variety of physical devices through compromised or controlled apps. This assault will raise the effectiveness of botnets to a new level.

In 2011 McAfee Labs expects to see increasing numbers of both suspicious and malicious apps for the most widely deployed mobile platforms and operating systems. Apps that are poorly developed have already exposed identity data. We expect developers and marketers to succumb to “rush to market” thinking as these apps become more commonplace. Platforms that have undersupervised models of app development and distribution are particularly at risk. This haste to sell insecure products will eventually lead to more app-centric privacy and data attacks in 2011.

McAfee Labs has already seen the move toward application-controlled botnets this year in Twitter and LinkedIn; we expect this to become the norm in 2011 and beyond, as application deployment and use becomes more ubiquitous. Will this be the year of mobile botnets controlled via a downloaded app?

### Sophistication Mimics Legitimacy

This year we saw an increase in the sophistication of some threats. “Signed” malware that imitates legitimate files will become more prevalent in 2011. This will cause an increase in stolen keys as well as the techniques and tools to forge fake keys to use in these types of attacks.

“Friendly fire”—in which threats appear to come from your friends—from social media such as Koobface and VBMania will continue to grow. This will go hand-in-hand with the increased abuse of social networks, which will eventually overtake email as a leading attack vector.

We also expect to see an increase in “smart bomb” attacks, those designed to trigger under certain conditions but not others. These threats require victims to follow the designated attack path—thwarting honeypots, crawlers, and security researchers—while greatly impacting designated and vulnerable targets. Such threats will create an even greater need for Global Threat Intelligence to defend against attacks observed under specific circumstances.

Personalized attacks are about to get a whole lot more personal.

*“The haste to sell insecure products will lead to more application-centric privacy and data attacks in 2011.”*

### Botnet Survival

As we mentioned in the discussion of applications, botnets continue to be one of the greatest and most sophisticated threats McAfee Labs faces. In the coming years, we expect to see more data exfiltration capabilities. Through this year we have seen cybercriminals engage in a growing number of targeted attacks; we anticipate a greater focus on botnets removing data from targeted machines and companies, rather than the common use of sending spam. Botnets will also engage in advanced data-gathering functionality as well as focus more on targeting and abusing social networking.

Botnets are suffering losses, too. Global law enforcement has recently taken down Mariposa, Bredolab, and some Zeus botnets. However, botnets continue to evolve. We predict that the recent merger of Zeus with SpyEye will produce more sophisticated bots due to improvements in bypassing security mechanisms and law enforcement monitoring. Mergers and acquisitions have finally made their way to the malware world.

Botnets that employ FaceBook and Twitter will expand their scope to include popular social networking sites such as foursquare, Xing, Bebo, Friendster, and others. The growing populations and business use of these sites is something that cybercriminals simply cannot ignore. McAfee Labs also expects to see more integration of location-based functions within botnets as GPS features continue to become more widespread.

### Hacktivism

Attacks motivated by politics are not new, but we encounter them more and more regularly. And they will be far more numerous in 2011. In addition to defacement (the primary activity of hacktivists) and distributed denial of service (DDoS, the latest “fashionable” activity), new kinds of sophisticated attacks will appear. Information theft, stolen and then disclosed to discredit political opponents, will certainly increase. More groups will repeat the Wikileaks example, as hacktivism is conducted by people claiming to be independent of any particular government or movement. Whether governments drive these manipulations and activities covertly is open to debate, but it is likely enough that states will adopt a privateer model. Hacktivism as a diversion could be the first step in cyberwarfare. Everyone within information security—from journalists to researchers—will have to be vigilant to recognize the difference between hacktivism and the beginning of a cyberwar.

We expect that social networks will be used more often to bring hacktivism into play next year. Just as cybercrime has moved from isolated individuals (able to create a piece of malware) to unstructured groups (able to launch a DDoS), we expect to see much more and stronger organization and structure within hacktivist groups in 2011.

Hacktivism will become the new way to demonstrate your political position in 2011 and beyond. Transitioning from the streets, political organizers will move to the Internet to launch attacks and send messages in broad daylight or Internet time. And as in the physical world, we expect that hacktivist attacks will inspire and foment riots and other real-world demonstrations.

### Advanced Persistent Threats

The news in January of the Operation Aurora/Google incident gave birth to the new category of advanced persistent threat (APT), which has been a hot topic of discussion in the industry and press for much of the year. However, there is much confusion about the true nature of these attacks.

The generally accepted definition of an APT is one that describes a targeted cyberespionage or cybersabotage attack that is carried out under the sponsorship or direction of a nation-state for something other than a pure financial/criminal reason or political protest. Not all APT attacks are highly advanced and sophisticated, just as not every highly complex and well-executed targeted attack is an APT. The motive of the adversary, not the level of sophistication or impact, is the primary differentiator of an APT attack from a cybercriminal or hacktivist one.

*“Hacktivism will become the new way to demonstrate your political position in 2011.”*

For instance, the RBS WorldPay hack that resulted in the theft of US\$9 million by an Eastern European cybercriminal gang was not an APT, despite its high level of sophistication and coordination. APTs also are not launched by a single adversary. There are numerous APT attack teams located around the world, all with varying degrees of capabilities and expertise. Just as there are A teams and B teams in the organized cybercriminal hierarchy, the same holds true for APTs. Some have access to massive amounts of resources (hardware, software, and human) and even traditional intelligence, surveillance, and reconnaissance capabilities. Others borrow, steal, or purchase ready-made tools offered and frequently used by established cybercriminal gangs and conduct themselves in a similar manner to gangs, except for the type of data they try to exfiltrate from their targets. Companies of all sizes that have any involvement in national security or major global economic activities (even peripherally, such as a law firm advising a corporate conglomerate starting business in another country) should expect to come under pervasive and continuous APT attacks that go after email archives, document stores, intellectual property repositories, and other databases.

#### About the Authors

This report was written by Dmitri Alperovitch, Toralv Dirro, Paula Greve, Rahul Kashyap, David Marcus, Sam Masiello, François Paget, and Craig Schmutgar 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 service McAfee Global Threat Intelligence. The McAfee Labs team of 350 multidisciplinary researchers in 30 countries follows 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](http://www.mcafee.com)

