Report

McAfee
An Intel Company

2013 Threats Predictions

By McAfee Labs

Table of Contents

McAfee Labs collected an immense amount of data on malware, vulnerabilities, and threats to endpoints, networks, email, and the web in 2012. Using our Global Threat Intelligence, we analyzed this data to block these intrusions and reduce the danger to our customers. (For more detail, read the *McAfee Threats Report*: *Third Quarter 2012.)*[1] Next year we anticipate more of the same: Cybercriminals and hacktivists will strengthen and evolve the techniques and tools they use to assault our privacy, bank accounts, mobile devices, businesses, organizations, and homes.

McAfee Labs researchers recently debated the leading threats for the coming year. We foresee an increase in or the introduction of the following threats in 2013:

- Mobile worms on victims' machines that buy malicious apps and steal via tap-and-pay NFC
- Malware that blocks security updates to mobile phones
- Mobile phone ransomware "kits" that allow criminals without programming skills to extort payments
- Covert and persistent attacks deep within and beneath Windows
- Rapid development of ways to attack Windows 8 and HTML5
- Large-scale attacks like Stuxnet that attempt to destroy infrastructure, rather than make money
- A further narrowing of Zeus-like targeted attacks using the Citadel Trojan, making it very difficult for security products to counter
- Malware that renews a connection even after a botnet has been taken down, allowing infections to grow again
- The "snowshoe" spamming of legitimate products from many IP addresses, spreading out the sources and keeping the unwelcome messages flowing
- SMS spam from infected phones. What's your mother trying to sell you now?
- "Hacking as a Service": Anonymous sellers and buyers in underground forums exchange malware kits and development services for money
- The decline of online hacktivists Anonymous, to be replaced by more politically committed or extremist groups
- Nation states and armies will be more frequent sources and victims of cyberthreats

Mobile Threats

Malware shopping spree

Once criminals discover a profit-making technique that works, they're likely to reuse and automate it. For example, Android/Marketpay.A is a Trojan horse program that buys apps from an app store without user permission. We're likely to see crooks take this malware's app-buying payload and add it to a mobile worm.

Buying apps developed by malware authors puts money in their pockets. A mobile worm that uses exploits to propagate over numerous vulnerable phones is the perfect platform for malware that buys such apps; attackers will no longer need victims to install a piece of malware. If user interaction isn't needed, there will be nothing to prevent a mobile worm from going on a shopping spree.

NFC worms

Phones with near-field communications (NFC) enabled are becoming more common. As users are able to make "tap and pay" purchases in more locations, they'll carry their digital wallets everywhere. That flexibility will, unfortunately, also be a boon to thieves. Attackers will create mobile worms with NFC capabilities to propagate (via the "bump and infect" method) and to steal money.

Malware writers will thrive in areas with dense populations (airports, malls, theme parks, etc.). An NFC-enabled worm could run rampant through a large crowd, infecting victims and potentially stealing from their wallet accounts.

Block that update!

One of the advantages that a mobile service provider (as opposed to Microsoft, for example) has in fighting malware is that once the cell company recognizes malware it can automatically push an update to customers to clean their devices. This works on phones that have not been rooted (or unlocked) by their owners. For mobile malware to stick around for a long time, it will have to prevent updates. Putting an app on a store that does nothing more than download external malware which locks the phone from communicating with the cell provider will achieve this.

Malware

Kits lead to an explosion in malware for OS X and mobile

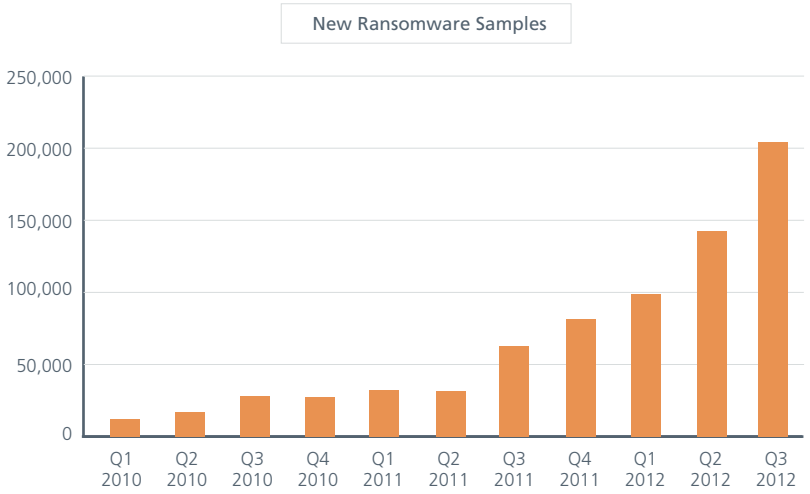
Given the popularity of mobile computing, we should perhaps be surprised that cybercriminals have taken so long to extensively exploit this field. In 2012, however, we've seen the number of mobile threats go up dramatically. As we look at them in more detail, we see the large amount of Windows-based malware owes its existence to the easy availability of malware kits in the underground market. In 2013, there is a good chance ransomware kits will take the lead from malware kits. We have already seen Android and OS X as targets of ransomware. Now the first ransomware kits are being marketed in the underground. For the moment the kits attack only Windows systems, but this may change soon.

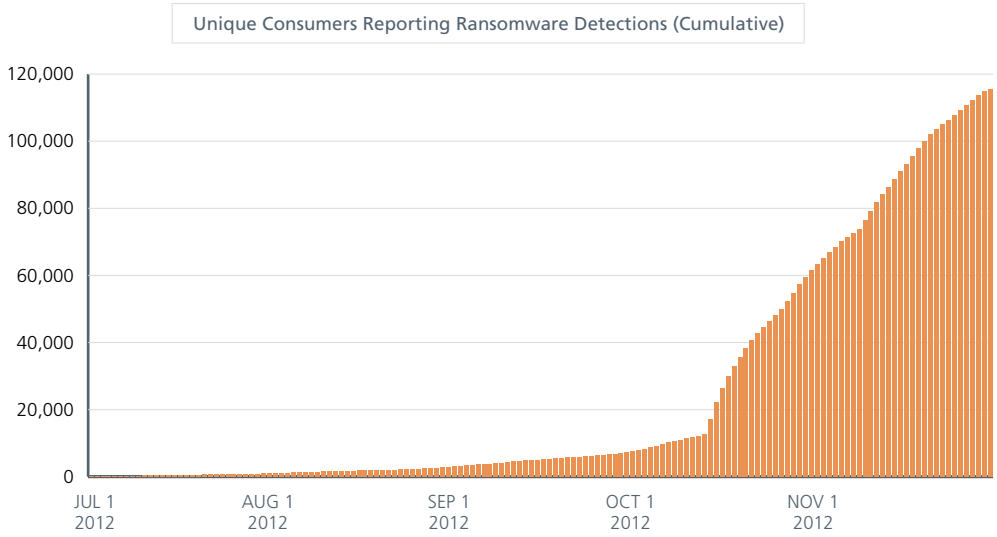
Ransomware continues to expand to mobile devices

Ransomware on Windows PCs has more than tripled during the past year. Attackers have proven that this "business model" works and are scaling up their attacks to increase profits. One way ransomware is different from other types of malware—such as backdoors, keyloggers, and password stealers—is that attackers do not rely on their victims using the infected systems for financial transactions to separate them from their money. Instead these criminals hijack the users ability to access data, communicate, or use the system at all. The victims are faced with either losing their data or paying a ransom in the hope of regaining access.

One limitation for many malware authors seeking profit from mobile devices is that more users transact business on desktop PCs rather than on tablets or phones. But this trend may not last; the convenience of portable browsers will likely lead more people do their business on the go. Attackers have already developed ransomware for mobile devices. What if the ransom demand included threats to distribute recorded calls and pictures taken with the phone?

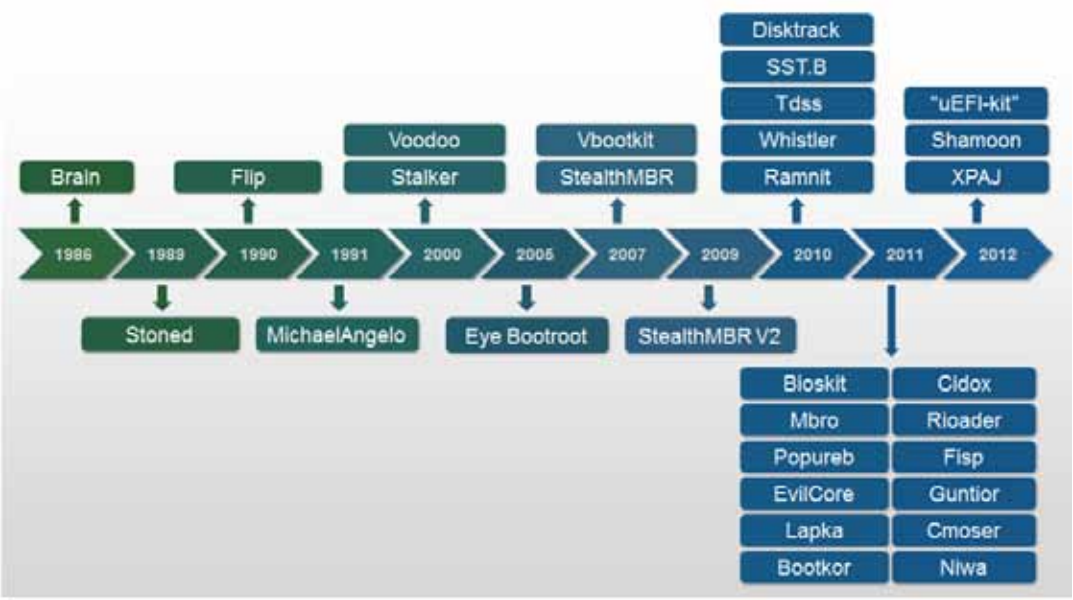
We anticipate considerably more activity in this area during 2013.


New Ransomware Samples
250,000
200,000
150,000
100,000
50,000
0
Q1 2010
Q2 2010
Q3 2010
Q4 2010
Q1 2011
Q2 2011
Q3 2011
Q4 2011
Q1 2012
Q2 2012
Q3 2012


Unique Consumers Reporting Ransomware Detections (Cumulative)
120,000
100,000
80,000
60,000
40,000
20,000
0
JUL 1 2012
AUG 1 2012
SEP 1 2012
OCT 1 2012
NOV 1 2012

Rootkits diversify, using MBR and other bootkit techniques

The evolution of computer security software and other defenses on client endpoints is driving threats into different areas of the operating system stack, especially for covert and persistent attackers. The frequency of threats attacking Microsoft Windows below the kernel are increasing. Some of the critical assets targeted include the BIOS, master boot record (MBR), volume boot record (VBR), GUID Partition Table (GPT), and NTLoader. Although the volume of these threats is unlikely to approach that of simpler attacks on Windows and applications, the impact of these complex attacks can be far more devastating. We expect to see more threats in this area during 2013.



Some notable below-the-kernel attacks, which have increased considerably in recent years.

Windows 8 the next big target

Criminals go where the money is. And if this means they have to cope with a new, more secure version of Windows, that's just what they will do. In many cases they attack the user and not the OS. Via phishing and other techniques users are tricked into revealing information or installing a malicious program. So if you upgrade, don't rely solely on Windows to protect your system: Remain vigilant and watch out for phishing scams.

Windows 8 should provide improved security against malware and exploits compared with earlier versions of Windows, at least for a while. Now that the underground market for attack and malware kits is much more competitive than three years ago, it is likely that Windows 8–specific malware will be available quicker than Windows 7–specific malware appeared. Systems running the new Unified Extensible Firmware Interface are still vulnerable to MBR-based rootkits, just as previous OS versions were, according to one research company. On the day of Windows 8's release, the firm announced for sale to its customers the availability of a zero-day vulnerability that circumvents all new security enhancements in Windows 8 and Internet Explorer 10.

In spite of any flaws, Windows 8 is a more secure OS, so upgrading is worth considering. Millions still run Windows XP, which only in fall 2012 was finally eclipsed in the number of its users by newer versions of Windows.

Big-Scale Attacks

Destructive payloads in malware have become rare because attackers prefer to take control of their victims' computers for financial gain or to steal intellectual property. Recently, however, we have seen several attacks—some apparently targeted, others implemented as worms—in which the only goal was to cause as much damage as possible. We expect this malicious behavior to grow in 2013.

Whether this is hacktivism taken to a new level, as some claim, or just malicious intent is impossible to say, but the worrying fact is that companies appear to be rather vulnerable to such attacks. As with distributed denial of service (DDoS) attacks, the technical bar for the hackers to hurdle is rather low. If attackers can install destructive malware on a large number of machines, then the result can be devastating.

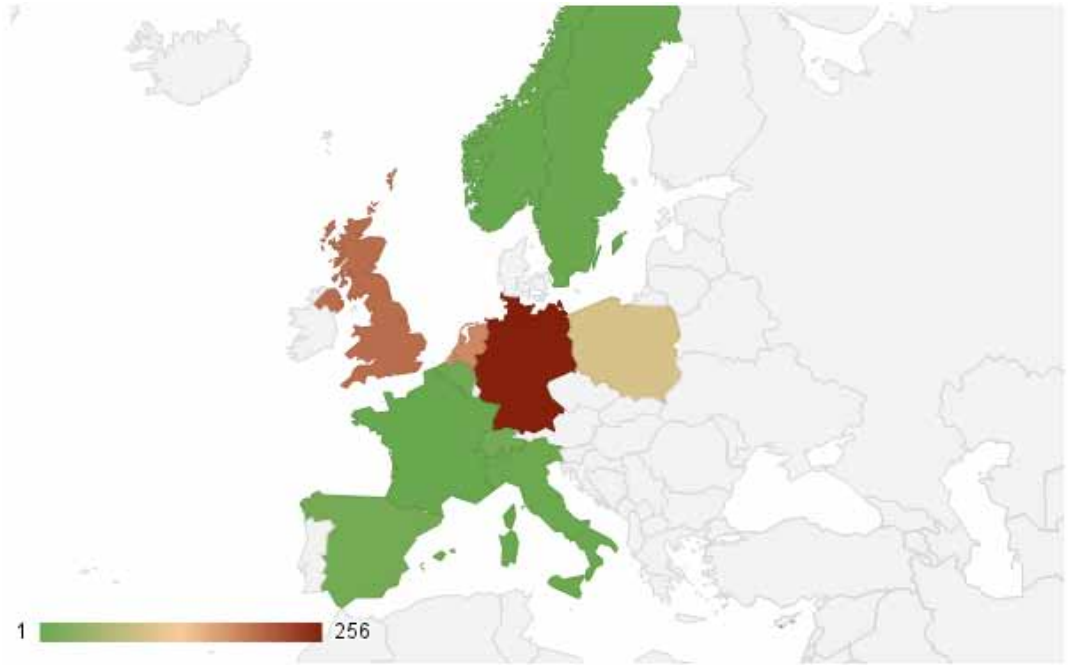
How can we prepare for such an incident and, more important, how can we mitigate or prevent some of the damage? It may be necessary to plan for the worst: An inside or outside attacker who has elevated privileges on the network for a long time could time-bomb many systems on multiple sites. This effect is likely worse than what is covered in many disaster recovery plans, so the IT staff may have to make some updates. The priority is to keep the business running, which is best achieved by having production networks, SCADA systems, etc. completely separated from the normal network, preventing them from getting hit in the first place. Then there will be a massive loss of data to deal with because users just love to store their data on their local machines. One challenge will be to reinstall thousands of machines while ensuring that the time bomb doesn't resurface. Technologies that may prove useful include remote management features that are independent of the state of the PC and its OS, but these features will need to be tested before an incident happens.

All measures to detect and block these persistent threats should also be effective against the preliminary steps of such attacks, while the attacker tries to gain and elevate access. Remote application control would prevent servers and key systems from being affected—unless an attacker has already taken full control of the update process, which can be determined by carefully monitoring who does what on the management systems. To keep the loss of data to a minimum, a reliable network backup (and restore) process needs to be in place, as well as backing up local data and blocking attackers from shredding data on shared drives and folders on the network.

Citadel Trojan Zeros In

Citadel is likely to become the Trojan of choice among cybercriminals who want the rich functionality of Zeus along with dedicated support. With the recent release of Citadel Rain, the Trojan can now dynamically retrieve configuration files, enabling a fraudster to send a targeted payload to a single victim or a selection of victims. This allows thieves to compromise accounts on a one-off basis depending on their criteria and wage attacks in a very targeted manner. Detection will become much harder because the footprint is minimal on the endpoint until the attack occurs. Typically Zeus attacks have been relatively widespread. We will likely see that change in 2013 as more cybercriminals adopt Citadel Rain and its future variants and focus on narrowly targeted attacks seeking the greatest possible gain.

Most Citadel infections are concentrated in just a few populations in Europe, but we expect that number to increase in 2013. The following map shows Germany is the prime location, with more than 200 infections to date.



The Trojan Citadel is most prevalent in Western Europe, especially in Germany. We expect attacks from this malware to increase in 2013.

HTML5

HTML5 is the next version of the standard language of Internet browsers. It provides language improvements, capabilities to remove the need for plug-ins, new layout rendering options, and new powerful APIs that support local data storage, device access, 2D/3D rendering, web-socket communication, and many other features. Today 74 percent of users in North America, 72 percent in Asia, and 83 percent in Europe use browsers that support the majority of HTML5 features.[2] Websites are quickly adopting HTML5 for its richer user experience. HTML5 continues the move to the browser, and away from the operating systems, as the platform to run applications. HTML5-based applications are increasing in number, with major players taking advantage of freedom from app stores and improved cross-browser and cross-device compatibility.

Browsers have long been one of the primary vectors for security threats, and HTML5 won't change that. With HTML5 the threats landscape will shift and broaden. We will see a reduction in exploits focused on plug-ins as browsers provide this functionally via their new media capabilities and APIs. However, HTML5 will offer other opportunities for attackers because the additional functionality will create a larger attack surface. Powerful JavaScript APIs that allow device access will expose the browser as websites gain direct access to hardware.

One example is WebGL, which provides 3D rendering. Prior to WebGL, HTML content not based on plug-ins was interpreted and rendered by the browser. This provided a layer of technology between the untrusted data on the Internet and the operating system. WebGL browsers, however, expose the graphics driver stack and hardware, significantly increasing the attack vectors. Researchers have already demonstrated graphics memory theft—allowing the web application to steal screenshots from the desktop—and denial of service attacks using all popular browsers supporting WebGL and popular graphics driver stack providers.[3]

One of the primary separations between a native application and an HTML application has been the ability of the former to perform arbitrary network connections on the client. HTML5 increases the attack surface for every user, as its features do not require extensive policy or access controls. Thus they allow a page served from the Internet to exploit WebSocket functionality and poke around the user's local network. In the past, this opportunity for attackers was limited because any malicious use was thwarted by the same-origin policy, which has been the cornerstone of security in HTML-based products. With HTML5, however, Cross Origin Resource Sharing will let scripts from one domain make network requests, post data, and access data served from the target domain, thereby allowing HTML pages to perform reconnaissance and limited operations on the user's network.

In 2013 we will see browsers expand on HTML5 features and improve HTML5 compatibility. HTML5-based applications and websites will continue to grow. We're certain that attackers will turn their attention to finding holes in HTML5 security in 2013. The question is how quickly they'll succeed.

Botnets and Spam

Botnets call home

The biggest threat to botmasters is the unrecoverable loss of their botnets. International cooperation in policing spam, malware, child exploitation, and illegal pills has made that loss a reality for many major botnets over the past few years, and will continue to threaten the proliferation of botnets. When the largest botnets get taken down, then the next largest botnets become the new targets. Botmasters have already reacted to this activity by subdividing botnets and increasing the costs associated with activities that are easily detectable (such as DDoS and spam). It is only a matter of time before botmasters implement fail-safes to reestablish command of a botnet that has lost all of the control servers it usually reports to.

In many cases botnets are temporarily hijacked by whitehat security researchers. Due to possible negative side effects, however, these takeovers do not lead to new commands reaching the infected hosts. There is a massive liability issue associated with the unauthorized remote operation of systems, even with the best of intentions. Pushing new commands to an old Windows machine serving a hospital could turn the PC into a brick and lead to incorrect care or even the death of a patient. Botmasters will take advantage of this reluctance by the good guys to meddle by hardwiring their botnets to reestablish control after a takedown.

"Snowshoe" spam will continue to increase

When a shady marketing company approaches your marketing people and tells them that they have a list of email addresses that have already opted into receiving whatever advertising you want to send them, it should set off alarm bells. Unfortunately those bells don't ring often enough. Well-known companies selling products from cell phones to cigars to language-learning software to satellite TV to medical supplies have all signed on with these shady advertisers. The shady companies blast out millions and millions of blatantly illegal spam messages every day from newly rented hosts in hosting companies until they get evicted from their subnets or move on—after they've turned those addresses, and sometimes the subnets, into permanently blacklisted wastelands. (By sending from many IPs, they spread out the load, thus the snowshoe metaphor.) Recipients have their inboxes bombarded with these spam messages and are unable to opt out of them.

Because this sort of activity is not as malicious as the most newsworthy hacks and malware, this area has been mostly ignored by the authorities. Nonetheless, this practice of snowshoe spamming has exploded during the past two years and is currently one of the biggest problems in the spam world. Attempts by researchers to expose this sort of activity have resulted in threats of defamation lawsuits by the companies using these shady marketers. In that environment (combined with an economy in which marketing budgets are thin or nonexistent), this sort of activity will only continue to increase at the breakneck pace that we've seen.

SMS spam from infected phones

Cell phone providers are working to prevent SMS spam. Their primary method of receiving reports from consumers is for the latter to forward messages to SPAM (7726) on their phones and report the messages so that they can be blocked. An infected phone can also send spammy text messages; then the victims face the problem of having their accounts closed by the providers. We expect to see pill advertising or phishing lures delivered by SMS in 2013.

Crimeware

Hacking as a Service

For a long time, cybercriminals have attended public forums to discuss and make business deals with other criminals. In these meetings, they not only offer software for sale but also services. Highly professional cybercrooks, however, see these forums as a waste of time (they are full of "newbies"), a loss of confidentiality (each deal needs direct contact with the client, who could be an undercover agent), and a loss of money (as the purchaser attempts to negotiate a lower price). For these reasons, the number of invitation-only criminal forums requiring registration fees and/or guarantors (vouchers) has increased.

This trend will continue, but to improve anonymity without discouraging buyers, online sales sites modeled on legal trade activities will grow in 2013. On these sites, buyers can make their choices at the click of a mouse, use an anonymous online payment method (such as Liberty Reserve), and receive their purchases without any negotiations or direct contact with the seller.

The shopping cart of a buyer looking for crimeware.

More secure and anonymous, these offers will be easier to find on the Internet. They will also be more diversified. We have already started to see high-level audit services and offers for project development for cybercriminals.[4]

The number of suspicious outfits claiming to sell zero-day attacks or the sale of spying services reserved for the sole use of governments or secret services will grow. It will be difficult to separate the wheat from the chaff, or to ascertain real activities and real customers.

An advertisement for "hacking as a service."

Hacktivism

The decline of Anonymous

Sympathizers of Anonymous are suffering. Too many uncoordinated and unclear operations have been detrimental to its reputation. Added to this, the disinformation, false claims, and pure hacking actions will lead to the movement's being less politically visible than in the past. Because Anonymous' level of technical sophistication has stagnated and its tactics are better understood by its potential victims, the group's level of success will decline. However, we could easily imagine some short-lived spectacular actions due to convergence between hacktivists and antiglobalization supporters, or hacktivists and ecoterrorists.

Anonymous is just one aspect of hacktivism. Another more powerful force is people with strong political motivation and high availability over a long term. An excellent example of this was the support for the uprising in Libya, as explained in the story "Power People 2.0," published in April 2012 by MIT Technology Review.[5] And to support the actions of these activists, the Telecomix group, not to be confused with Anonymous, contributed its high-level hacking techniques. Thanks to all of these people, their actions were significant. Actions like these should be more visible in the future whenever a people will promote a cause that hacktivists consider just.

Meanwhile, patriot groups self-organized into cyberarmies and spreading their extremist views will flourish. Up to now their efforts have had little impact (generally defacement of websites or DDoS for a very short period), but their actions will improve in sophistication and aggressiveness. They will fight among themselves, certainly, but their favorite targets will be our democratic societies each time we denounce the extremist governments they support.

Nation states and armies will be more frequent actors and victims of cyberthreats

Many of the world's military units are on the front line of social networks. They communicate more and more frequently. Professional forums such as CompanyCommand and professional wikis involve the development of online collaborative work.[6] Furthermore, military operations use the Internet for emailing, social networking and, unfortunately, visiting dubious websites. All of these elements will increase the possibilities of infiltration and unintentional information leakage.

Experts are no longer reluctant to predict national responsibility in military and industrial espionage or precision attacks that cause physical damage, as in the case of Stuxnet or Shamoon. State-related threats will increase and make the headlines. Suspicions about government-sponsored attacks will grow. Using zero-day vulnerabilities and sophistical malware, some of these attacks may be considered advanced persistent threats, while others will involve conventional malware.

In January 2012, the Atlantic Council of the United States published a spectrum to help analysts in assigning responsibility for a particular attack or campaign of attacks.[7] Using ten categories based on whether a nation ignores, abets, or conducts an attack, this spectrum starts from a very passive up to very active responsibility. We predict this measurement tool will be effective in 2013 to judge the actions of nations ranging from employing insecure systems that lead to an attack to nations that plan and execute one.

Even if they have never launched a cyberattack against noncombatant targets, some terrorists are also Internet fans. They use the web to communicate, recruit, disseminate propaganda, seek funding, search for information on people and targets, and prepare their assaults. We can read of numerous examples in various reports, among them "The Use of the Internet for Terrorist Purposes," published by the United Nations Office on Drugs and Crime.[8] The next step could be a combination cyber-physical attack: an online attack carried out in conjunction with a physical attack. If a group can remotely disrupt a critical infrastructure, such as a defense or communications system, a conventional attack could more easily cause more damage. We have no evidence that such a terrorist event will occur in 2013, but today our fears of one are not just fantasy.

About the Authors

This report was prepared and written by Xiao Chen, Toralv Dirro, Paula Greve, Prashant Gupta, Haifei Li, William McEwan, François Paget, Craig Schmugar, Jimmy Shah, Ryan Sherstobitoff, Dan Sommer, Bing Sun, Peter Szor, and Adam Wosotowsky of McAfee Labs.

About McAfee Labs

McAfee Labs is the global research team of McAfee. 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 500 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. http://www.mcafee.com/labs

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled global threat intelligence, 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. McAfee is relentlessly focused on constantly finding new ways to keep our customers safe. http://www.mcafee.com

[1] http://www.mcafee.com/us/resources/reports/rp-quarterly-threat-q3-2012.pdf
[2] http://arstechnica.com/information-technology/2012/08/forrester-report-urges-html5-adoption-says-most-browsers-can-support-it/ http://www.forrester.com/The+Coming+Of+HTML5/fulltext/-/E-RES70341
[3] http://www.contextis.com/research/blog/webgl-new-dimension-browser-exploitation/
[4] http://blog.xmco.fr/index.php?/page/2
[5] http://www.technologyreview.com/featuredstory/427640/people-power-20/
[6] http://companycommand.army.mil/index.htm
[7] http://www.acus.org/files/publication_pdfs/403/022212_ACUS_NatlResponsibilityCyber.PDF
[8] http://www.unodc.org/documents/frontpage/Use_of_Internet_for_Terrorist_Purposes.pdf

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

The information in this document is provided only for educational purposes and for the convenience of McAfee customers. The information contained herein is subject to change without notice, and is provided "as is," without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.
McAfee, the McAfee logo, and McAfee Global Threat Intelligence are registered trademarks or trademarks of McAfee, Inc. or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2012 McAfee, Inc.
57500rpt_threat-predictions_1212_fnl_ETMG