Report

McAfee Threats Report: Fourth Quarter 2010

By McAfee® Labs™

The past year was a transformative and evolutionary period in cybersecurity. Throughout the year we saw increases in targeted attacks, increases in sophistication, and increases in the number of attacks on the new classes of devices that seem to appear with regularity. Informing users at all levels of these threats without scaring them unnecessarily is no easy feat. At McAfee Labs our goal is to empower the use of technology in the safest manner possible. To do this we must openly analyze and explain the ramifications of what we see.

This quarter presented some of the most interesting changes of the year. In the past three months we saw the lowest spam volumes since 2007, but at the same time we identified attacks on new devices such as smartphones using the Android operating system. Mobile malware and threats have been around for years, but we must now accept them as part of the mobile landscape, both in awareness and deployment. This quarter also introduced some drastic changes in the diversity of global malware, which at the moment is very different depending upon what geography users find themselves in. The global diversity of botnets has also changed significantly since last quarter, with Cutwail no longer the world leader. The types of digital threats users face differ depending upon where people are and what they use.

It is impossible to talk about this quarter without discussing hacktivism, WikiLeaks, and the hacktivist group Anonymous. This chapter in political action may turn out to be one of 2010's defining events—with the exposure of data and activism that surrounds both sides of the issue. Regardless of a user's or business' alignment, hacktivism and the WikiLeaks phenomenon will influence the topics of data loss, data exposure, and political activism for quite some time to come. Aside from WikiLeaks itself, there were numerous other global hacktivist activities this quarter. At the same time, Eastern Europeans made some great advances in the fight against cybercrime.

By the end of 2010 malware reached its highest ever overall growth levels while maintaining considerable diversity in the classes of malware that are prevalent from quarter to quarter. We will revisit some old "favorites," such as Koobface, fake-AV, password-stealing Trojans, and AutoRun malware to check their recent activity.

McAfee Labs predicted in late 2009 that 2010 would be a very Adobe product–centric exploit year, and that has certainly turned out to be true. Adobe software far exceeds Microsoft's as the favorite of exploit writers, who commonly target both Adobe Reader and its web-based plug-ins. Vulnerability activity and SQL-injection attacks also held a surprise or two in this quarter. McAfee Labs noted some changes in search engine and term abuse as well as where some of those links actually lead.

Cyberthreats and cybercrime are evolving into new areas as fast as businesses and consumers adopt new technologies and engage more online in their daily lives. Because criminals follow the money and the data, it would be unrealistic—and unwise—to think otherwise.

Table of Contents

Mobile Threats Grow Rapidly

Threats to mobile platforms (primarily smartphones) are not new; however, cybercriminals seem to have renewed their interest for a variety of reasons. As in most crimes it's a matter of opportunity, and cybercriminals currently have a window of opportunity to exploit a variety of mobile platforms. More consumers are using mobile devices and tablets in their daily lives as well as at work. Enterprises must now support more devices than ever before, in effect extending their corporate firewalls and services to places they may not be prepared for.

During the last several years McAfee Labs has seen steady growth in the number of threats to mobile devices. The numbers cannot match the sheer volume of PC-based malware, but it is steady growth just the same.

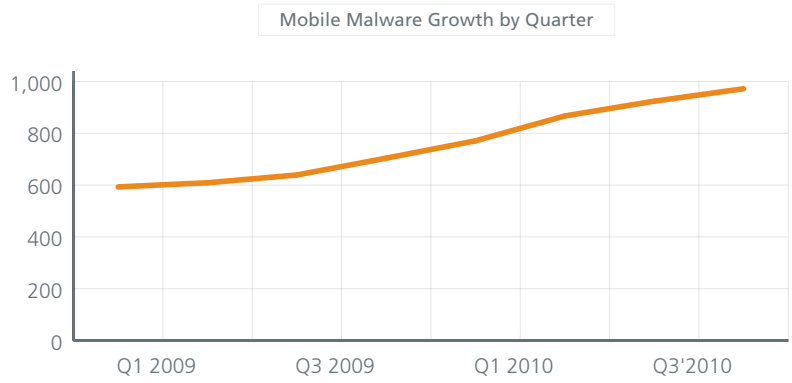


Figure 1: The number of new mobile malware in 2010 increased by 46 percent compared with 2009. The threat vector shows steady growth.

At McAfee Labs our research and analysis reveals that although most of the threats center on certain platforms, criminals can target any mobile platform they desire.

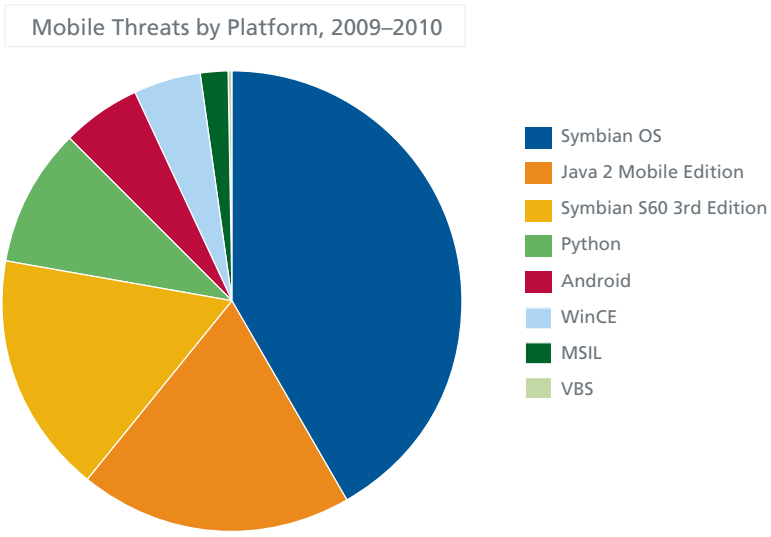


Figure 2: The Symbian OS (used by Nokia smartphones) is the most popular platform for mobile malware developers. McAfee Labs has identified 188 new threats in the last two years and 668 since 2004.

Some of the most interesting mobile threats of this quarter were SymbOS/Zitmo.A and Android/Geinimi. The former was a high-profile threat that struck early in the quarter. It looked as though the criminals behind the Zeus botnet were creating their own custom spyware to capture financial mobile transaction authentication numbers (mTANs) on mobile devices, as they already do for TANs on the PC. It turns out, however, that they just repurposed an old version of a commercial spyware package. This is a scenario we predicted and described back in 2007.

Android/Geinimi is arguably one of the most important threats of the quarter. It is a Trojan inserted into legitimate mobile applications and games (for example, MonkeyJump2 and Hardcore Dirt Bike) for the Android platform. It was found in China and is similar to other mobile malware and mobile botnets from the region (such as SymbOS/XMJTC, Yxe.A, and "sexy" worm) except that it requires users to install it on their phones.

This Trojan tries to appear as a legitimate application by using a key to sign the application. The signing, however, uses the default test certificate from a debug build with the standard Android SDK and indicates that the malware author did not go to a lot of effort. In contrast, the authors of the SymbOS/XMJTC worm family and its close cousins actually registered developer certificates to sign their malware. These certificates are both trackable (to a fake identity) and revocable (to protect uninfected users).

The manual-labor aspect might suggest that Geinimi is a first attempt on a new platform rather than a polished malware from an experienced Android developer.

Android/Geinimi has a set of hardcoded URLs encrypted within itself to reach botnet command servers. The malware has code to send information about the mobile phone, mobile carrier, and user to control servers. It contains code to update the server list and encryption key. The malware can also download software from the attacker's servers. However, currently all of the servers are inactive. It is unlikely that the malware can maintain an active botnet—at least for now.

McAfee Labs expects to see more developments in this class of threat throughout 2011.

Botnet Lead Changes Hands

Last quarter Cutwail was the clear global leader in botnet activity. This quarter Rustock was the most prevalent in many parts of the world, with Cutwail and Bobax also showing lots of activity.

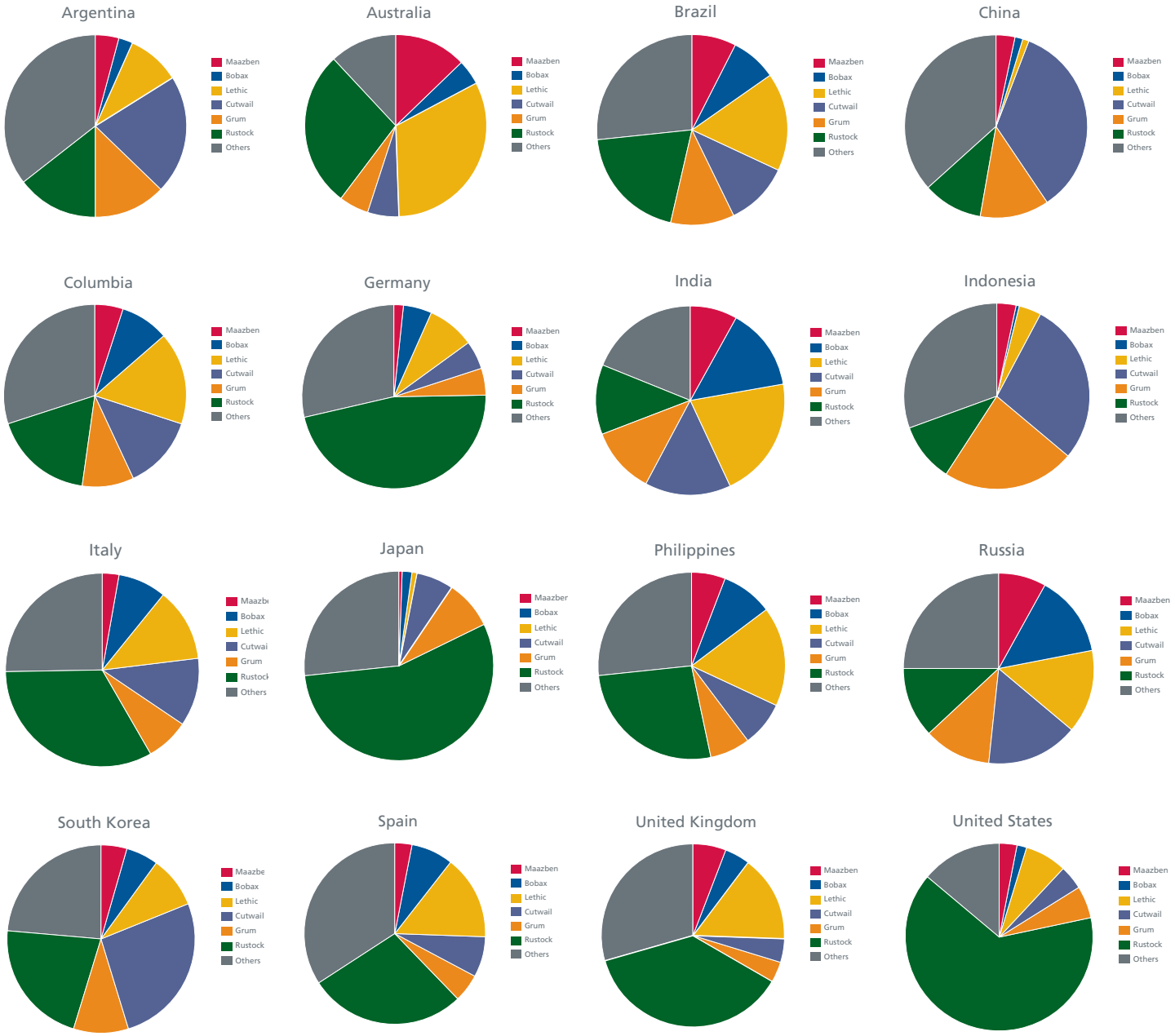


Figure 3: Botnets vary in impact among countries. Rustock was this quarter's overall world leader.

With the adoption of so many new mobile platforms, McAfee Labs expects botnet infections and distribution will target these devices. The lack of security awareness among mobile users and the relative immaturity of mobile safeguards offer cybercriminals a significant opportunity for mischief.

Malware Reaches Record Numbers

Malicious code, in its seemingly infinite forms and ever expanding targets, is the largest threat that McAfee Labs combats daily. We have seen its functionality increase every year. We have seen its sophistication increase every year. We have seen the platforms it targets evolve every year with increasingly clever ways of stealing data. In 2010 McAfee Labs identified more than 20 million new pieces of malware.

Stop. We'll repeat that figure.

More than 20 million new pieces of malware appearing last year means that we identify nearly 55,000 malware threats every day. That figure is up from 2009. That figure is up from 2008. That figure is way up from 2007. Of the almost 55 million pieces of malware McAfee Labs has identified and protected against, 36 percent of it was written in 2010!

Let's dig into some of the numbers and popular classes of malware.

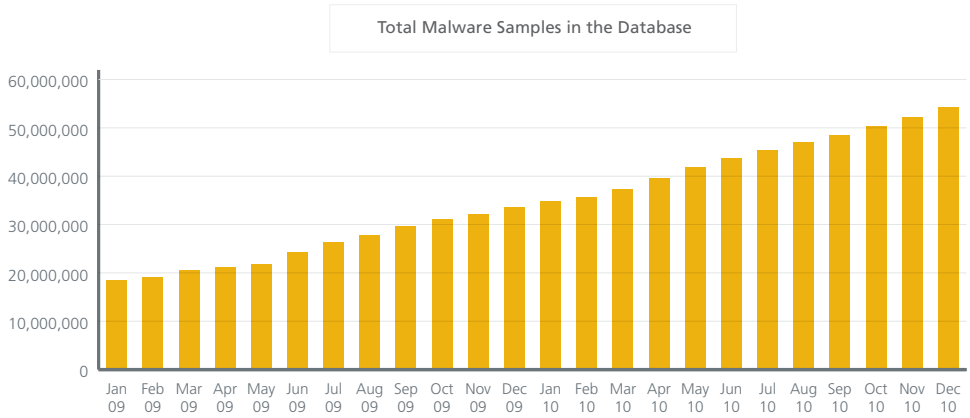


Figure 4: Total count of unique malware (including variants) in the McAfee Labs database.

As the preceding chart clearly shows, the onslaught of malware, especially in the last three years, seems to have no end. How the proliferation of both handheld and IP-enabled devices will affect this growth remains to be seen, but the increase is not likely to diminish.

What of the "staples" of malware? In the following charts we can see that AutoRun malware has shown recent growth, while fake alert (fake security software) is flat and password-stealing Trojans have declined since this year's high point in May. Koobface saw a spike in activity late in this quarter, though it lags behind the numbers from the first half of the year. (For more on fake security software, read our recent report by McAfee Labs senior researcher François Paget.[1])

1. "Running Scared: Fake Security Software Rakes in Money Around the World," McAfee Labs. http://www.mcafee.com/us/resources/white-papers/wp-running-scared-fake-security-software.pdf

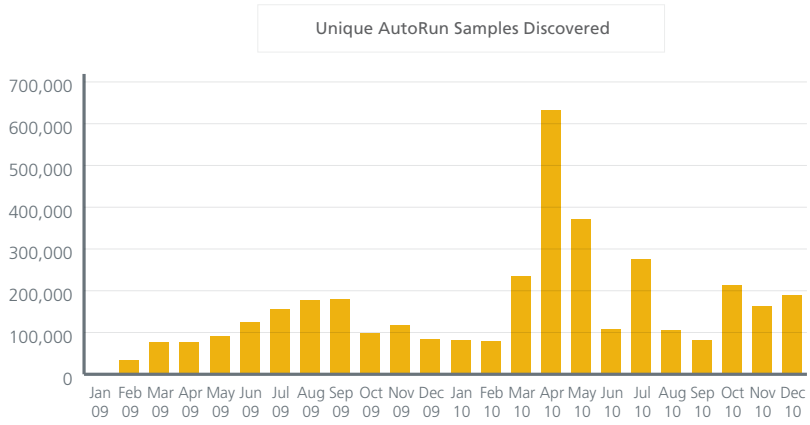


Figure 5: The number of AutoRun worms is slowly moving upward again compared with the prior quarter.

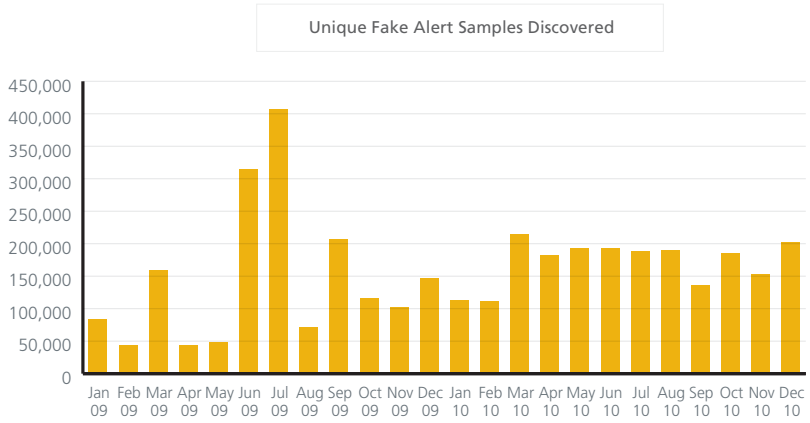


Figure 6: Fake security software samples have remained steady for most of the year.

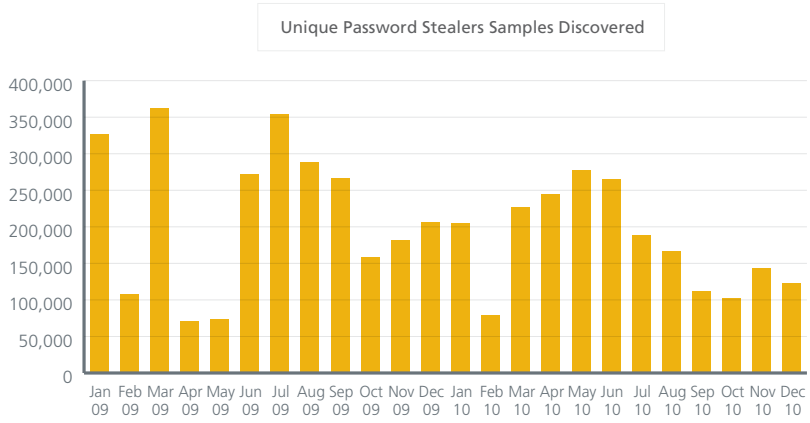


Figure 7: Password-stealing Trojans primarily target data in victims' bank accounts.

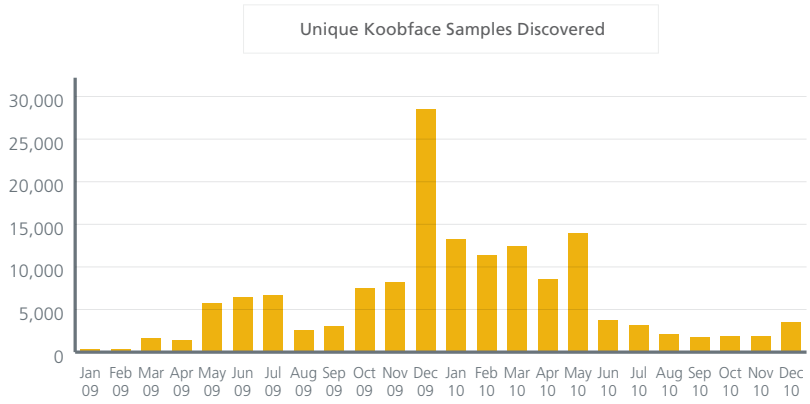


Figure 8: The count of new Koobface variants attacking Facebook users rose slightly in December after a relatively flat second half of the year.

For the last several quarters the top malware threats have been pretty much the same around the world—meaning that the top malware threats in North America were generally the same in South America or Asia. This quarter is very different in the various geographies. This difference is part of the larger trend that threats now tend to match the types of users, habits, and events that are specific to a region. This makes sense when we step back from the data and think about it: Users have likes and dislikes that are culturally and geographically specific. Cybercriminals are aware of this; thus we see very different threats in different geographies.

Overall traditional viruses made a strong showing this quarter. Ramnit, with a few variants, was the overall leader. "Favorites" generic!atr (autorun malware), banking Trojans and downloaders (sometimes called PWS or generic.dx), as well as web-based exploits such as StartPage and exploit-MS04-028 were prevalent. Adware and various messenger-targeted threats also demonstrated their malicious activity.

Rank	Top 5 Global Malware
1	W32/Ramnit.a
2	Generic!atr
3	W32/Ramnit.a!htm
4	Exploit-MS04-028
5	Generic StartPage

Rank	North America
1	W32/Ramnit.a
2	Exploit-MS04-028
3	Generic!atr
4	W32/Ramnit.a!htm
5	Adware-OneStep.n

Rank	Europe
1	W32/Ramnit!htm
2	Generic!atr
3	W32/Ramnit.a
4	Adware-OneStep.n
5	Generic PWS.o

Rank	South America
1	PWS-Banker!goj
2	Generic!atr
3	Downloader-CEW
4	W32/Jahlover.worm.gen
5	MessengerPlus

Rank	Africa
1	Generic!atr
2	W32/Rontokbro.b@MM
3	Generic PWS.y!bfi
4	Generic.dx!cyf
5	W32/Rontokbro.gen@MM

Rank	Asia
1	Generic StartPage
2	Generic!atr
3	Generic.dx
4	W32/Rontokbro.gen@MM
5	W32/HLLP.Philis.remnants

Rank	Australia
1	Uploader-R
2	Generic.dx!vhp
3	VBS/FWBypass
4	Generic.dx
5	Generic VB.c

Are Criminals Growing Tired of Spam?

This quarter spam volumes reached their lowest point since the first quarter of 2007, almost four years ago. Further, spam accounted this period for only 80 percent of total email traffic, its lowest prevalence since the third quarter of 2006, when total spam traffic was starting a meteoric rise that would peak three years later. From its highest historic point, spam volumes are off by 70 percent, even lower than they were after the shutdown of McColo, a major hosting provider for spammers, in November 2008.

This quarter's volume is off by 47 percent from last quarter and by more than 62 percent since the start of 2010. A significant portion of the plummet occurred within just the last six weeks of the year.

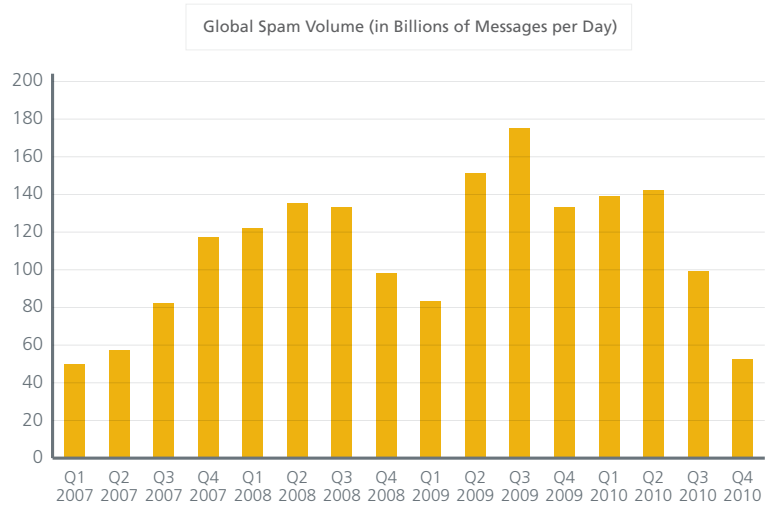


Figure 9: Spam volume, measured by average number of messages per day, has fallen precipitously in the past two quarters, reaching a level last seen in 2007.

We've seen several significant spam shutdowns over the course of the year. Spamit, a notorious spammer responsible for large volumes of "pharmacy" mail, shut its doors in September. In October we learned the Bredolab botnet had been closed along with parts of the Zeus botnet (although this network is still thriving), and in March the Mariposa botnet was shuttered.

The Christmas holiday brought users another present this year, as spam from the Rustock, Lethic, and Xarvester botnets all but disappeared. We noted a resurgence from the Waledac botnet over the New Year's holiday; it was implicated in an e-card spam campaign that briefly accounted for one in every 1,000 spam messages. Nonetheless, the Bobax and Grum botnets currently sit on the throne as spam kings.

Does this mean Bill Gates long-predicted demise of spam is finally here? Hardly! We do appear to be in a transition period, with several major botnets going dormant during a time of year when spam volumes are usually on an upward path. Typically in the first quarter spam volumes drop; but considering their relative low point now, it is hard to believe that they could fall much further. Look for a retooling and possibly some consolidation in the botnet space during the coming months that will likely result in spam volumes climbing once again.

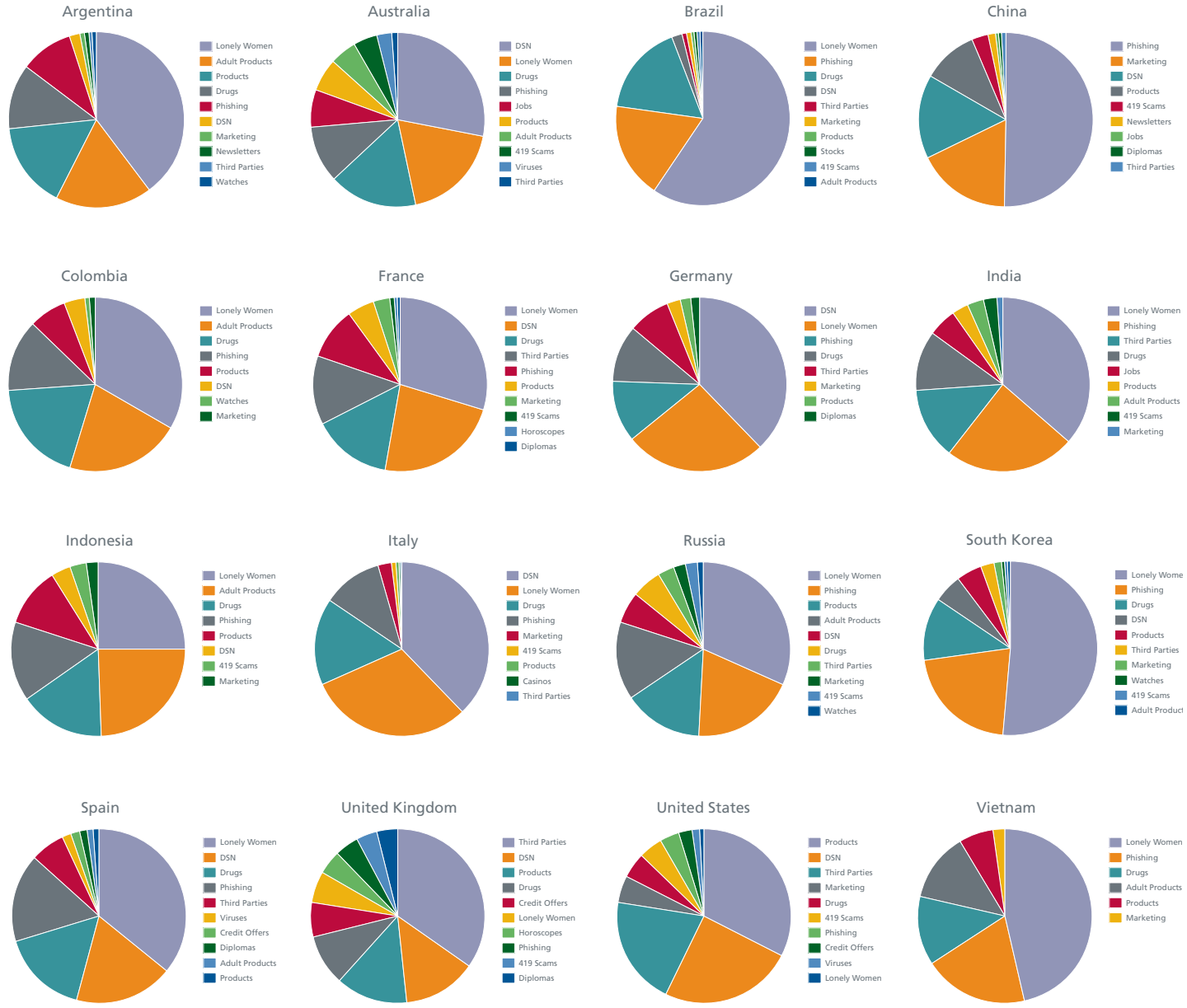


Figure 10: Spam subjects vary considerably among countries. These charts show the relative frequency of the leading topics originating within each nation. These subjects do not represent all spam traffic, only the most popular. DSN stands for Delivery Status Notification, bogus messages that claim your email has failed to reach its destination.

Web Threats

A number of new exploits appeared on the web this quarter. We continue to see a trend of malware following a Conficker-like pattern of accessing a wide range of random domains—legitimate domains that are just pinged, malicious domains waiting for the malware to "phone home," and the vast majority of domains not available. The malware's tactic is to hide the real phone-home domains like a needle in a haystack. The number of potentially malicious domains grew at a rapid pace this quarter, as did the number of malicious URLs—hosting activities such as "phone home" downloading and data-theft tools, a beacon, an anonymizer used only for malicious purposes, or a redirection URL to divert a victim to a payload, for example. In contrast, McAfee Labs observed that the overall monthly summary of URLs that were active (such as serving browser exploits or hosting malicious downloads) reflected a more modest rate of growth. Some of the most active threats from last quarter, including Zeus-Murofet, Conficker, and Koobface, resurfaced along with a number of drive-by exploit sites.

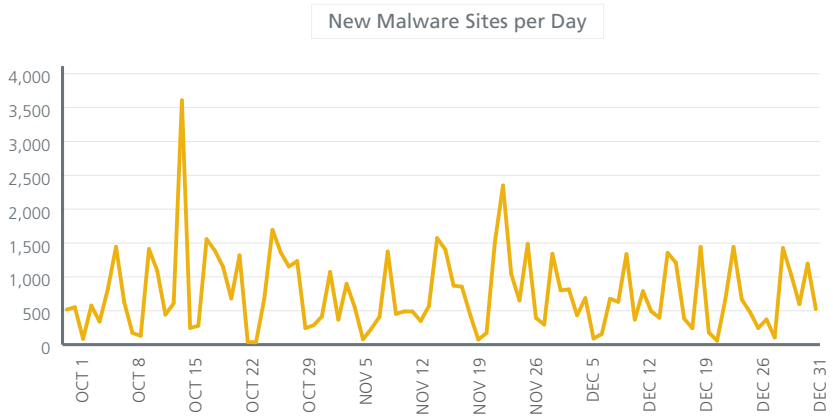


Figure 11: Conficker, Koobface, and Zeus—oh, my! Tracking the different malware families as they evolved and the reverse engineering of possible "phone home" locations led to a set of new malicious URLs.

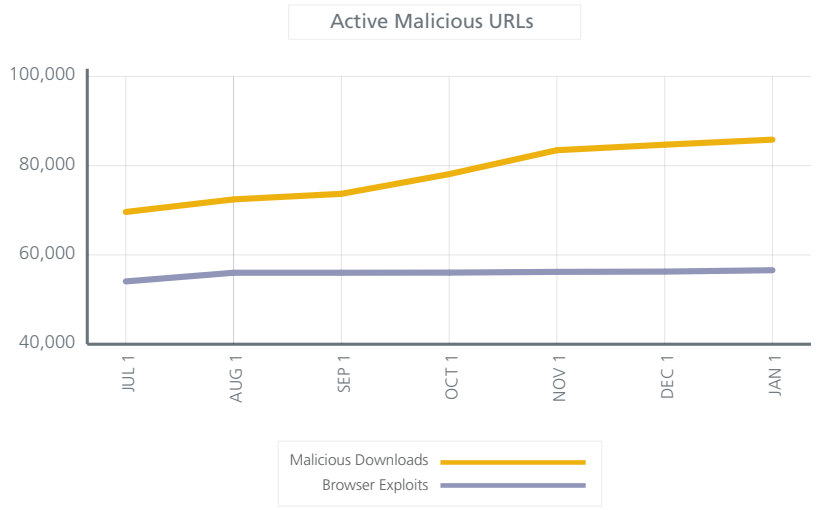


Figure 12: Among active URLs, we saw noticeable growth in sites hosting malicious payloads, while growth in sites hosting browser exploits was flat.

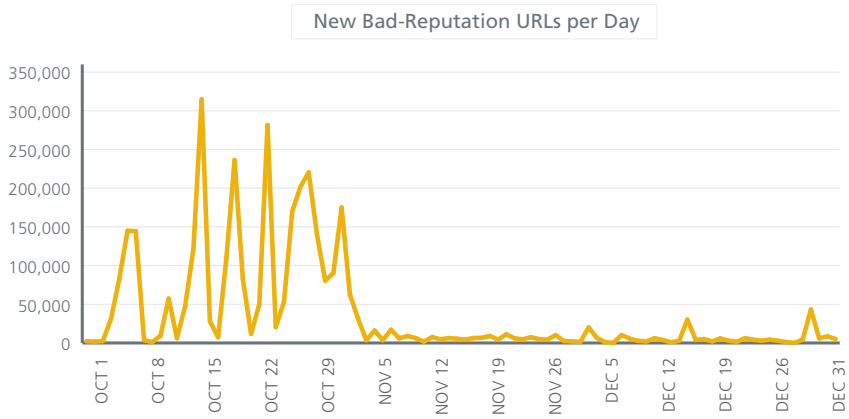


Figure 13: In October we observed a significant number of domains, IP addresses, and URLs that were reserved for possible malicious communications. The small spike at the end of December occurred due to fast-flux usage and other crawling trends.

Although phishing URLs decreased this quarter compared with the prior three months, they still remained very high compared with a year ago. We saw the beginnings of various IRS attacks as well as continued expansion into the profitable areas of gift cards, rewards accounts, and social networking accounts.

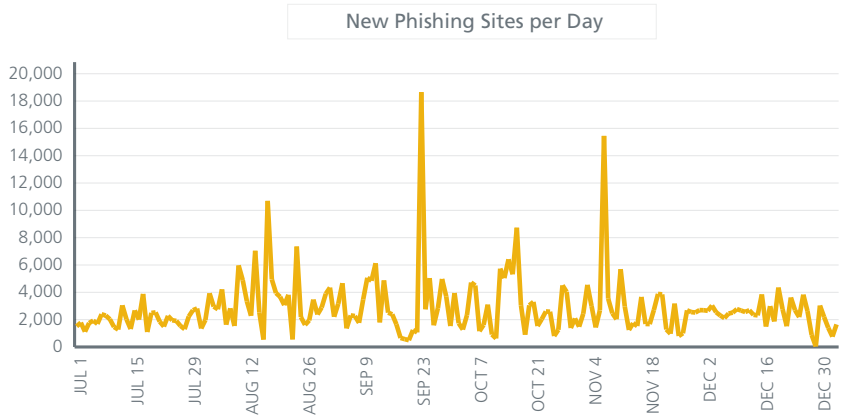


Figure 14: The appearance of new phishing URLs increased dramatically in 2010. The most recent quarter saw a small decrease from the prior quarter.

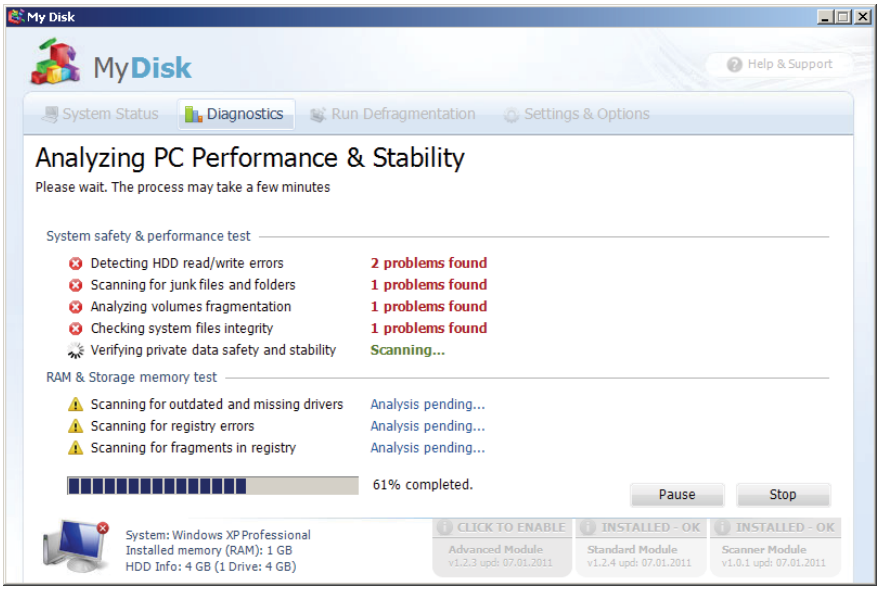
As more users access the Internet from an ever-expanding pool of devices, these types of web-based threats will continue to grow in size and sophistication. No matter what hardware users choose for surfing—computer, tablet, smartphone, or InternetTV devices—they all lead to the same Internet.

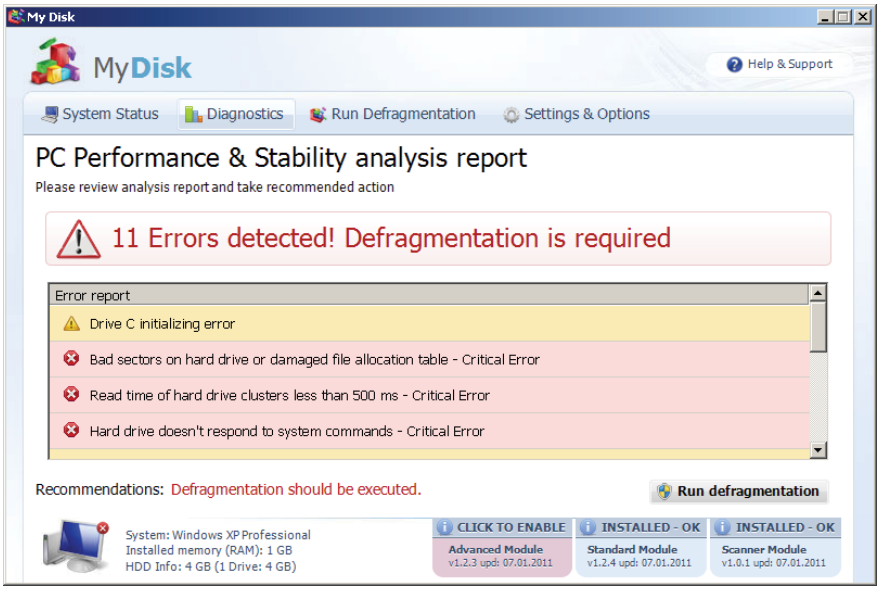
Search Engine, Terms, and New Rogues

Cybercriminals and scammers continue to abuse cloud services. Search terms and trends have long posed an easily exploitable lure for a variety of attacks. Every quarter varies in which terms, trends, and keywords are abused and poisoned; this quarter, sports terms topped the list, with celebrities and weather terms also among the most poisoned. The following cloud snapshot shows the Top 100 poisoned search terms of the quarter:

We found that within the top 100 results 51 percent of the daily top search terms led to malicious sites, and on average each of these poisoned-results pages contained more than five malicious links. Of those poisoned, almost 5 percent had a malicious link in the top 10 results alone. Clearly the cloud remains a popular method of leading users of all types to bad sites. This trend will certainly continue as more users adopt non-Windows and non-traditional devices such as InternetTV. McAfee Labs expects attacks using the techniques of search-engine abuse and trend abuse to focus more specifically on these types of users and devices in the new year.

During our analysis of this quarter's data we discovered a change in where many of these malicious links lead. Cybercriminals and scammers have long used fake security products—known as fake or rogue AV—to scam users out of their money. After infecting machines, these programs present bogus results of fake "security scans" to con victims into buying the products. We have noticed a newly developing trend, however. Rogue applications are shifting from security products toward system and disk utilities. As you can see from the following screenshots, the methodology is the same: Present victims with fake, horrific results to get them to buy products that promise to solve problems that don't really exist:





We'll see whether fake system and disk utility programs replace fake-AV as one of the prime sources of cybercriminals cash flow. In any case, McAfee Labs will certainly focus on combating this new trend.

Vulnerabilities and Network Attacks

McAfee Labs predicted in 2009 that vulnerabilities in Adobe products would become the clear choice of malware authors and cybercriminals for distributing malware and compromising systems and networks. This prediction has come true. Throughout 2010 malware developers have heavily exploited weaknesses in both Flash and especially PDF technologies. Our malware database reveals that malicious Adobe PDFs topped the number of unique samples by a wide margin, making them the favorite targets of client-side exploitation.

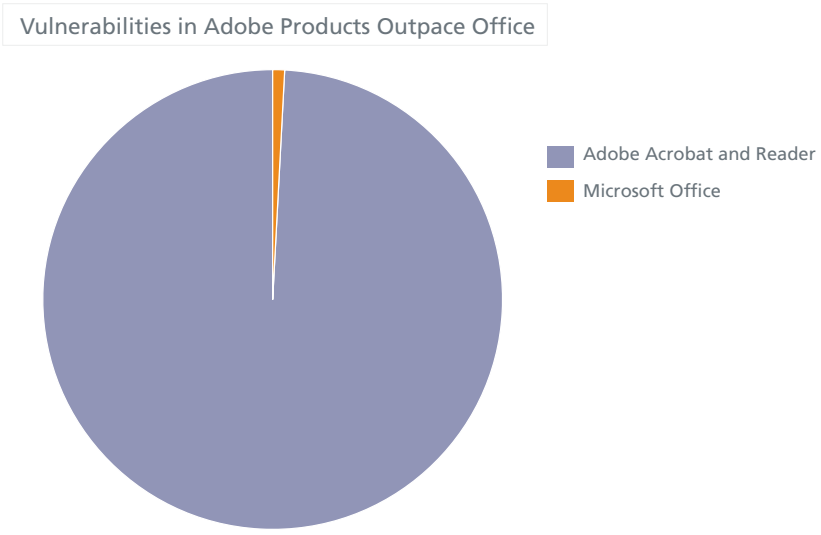


Figure 15: In 2010 McAfee Labs counted 214,992 pieces of malware aimed at vulnerabilities in Adobe Acrobat and Reader. In contrast, only 2,227 malware attacked vulnerabilities in Microsoft Office products.

McAfee Labs is certain that the "Adobe" trend will continue this year, as more mobile devices and non-Microsoft operating systems support various Adobe technologies.

Here's a short list of notable vulnerabilities that appeared this quarter:

- CVE-2010-3962. Uninitialized Memory Corruption Vulnerability: This zero-day vulnerability was discovered being exploited by malware in the wild. The vulnerability affects Internet Explorer Versions 6, 7, and 8 and can be reliably exploited. Enabling memory-protection schemes such as data execution prevention can mitigate this exploit.
- CVE-2010-3971. Microsoft Internet Explorer CSS Parsing Remote Code Execution Vulnerability: This vulnerability was discovered and posted in a Chinese vulnerability discussion board. It was initially listed as a denial of service vulnerability, but was later shown to be exploitable with publically available information. Since then, McAfee Labs has tracked some instances of exploitation of this issue in the wild. This vulnerability remained unpatched when we wrote this report. Attacks using this issue are prevalent; we urge all users to keep their security software updated to block this vulnerability.
- CVE-2010-3654. Adobe Acrobat, Reader and Flash Player Remote code execution vulnerability: Another zero-day vulnerability being exploited in the wild, this time multiple Adobe products were vulnerable on Windows, Mac OS X, Solaris, Android, and Linux.[2] McAfee Labs urges all affected users to immediately deploy the relevant patches.

SQL-Injection Attacks

China and the United States continue to be the primary sources for SQL-injection attacks. This quarter again sees China as the number one source of attacks, with the United States second and Iran jumping to third place—a tenfold increase. Primarily used to access databases of various types, SQL-injection attacks usually represent a sophisticated class of attacks with a determined aggressor.

2. More details and patch information is available at http://www.adobe.com/support/security/advisories/apsa10-05.html

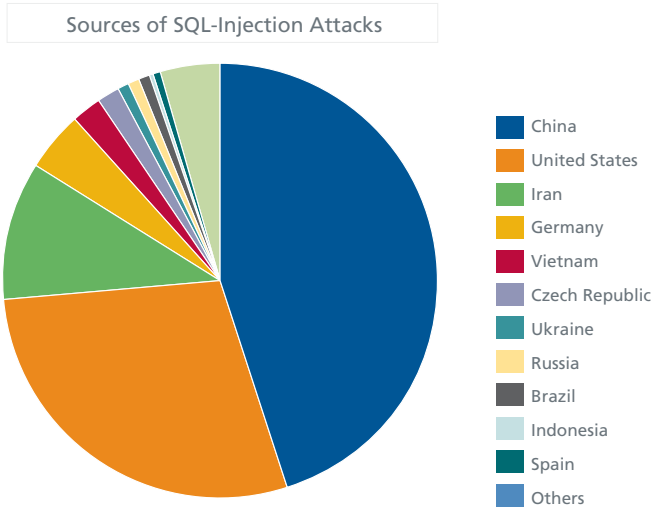


Figure 16: China and the United States are followed in the top 10 this quarter by surprising Iran, which leaped up several places from last quarter.

Cybercrime

Abuse of social networks can take many forms. With user counts in the hundreds of millions, they are a logical target for cybercriminal activities. Social network accounts can be abused in a variety of ways. Creating accounts in forums, for example, helps in sponsoring or spamming. These accounts can be used to send spam, phishing links, links to fake products or services, or even malicious downloads. Prices for providing bogus accounts vary depending on the account quality. The most expensive accounts are usually verified (after a phone text or SMS acknowledgement).

Account Offers	Number of Accounts and Prices in US Dollars		
Facebook	Basic: 100/$15 250/$35 500/$65 1,000/$120	Multiple Pictures: 100/$22 250/$55 500/$100 1,000/$190	Verified: 20/$40 50/$100 100/$200 250/$500
YouTube	Basic: 100/$12 250/$30 500/$60 1,000/$120		Verified: 100/$45 250/$100 500/$190 1,000/$350
Yahoo	100/$3 500/$8 1,000/$15		5,000/$50 10,000/$100
Gmail	Basic: 100/$20 250/$40 500/$65 1,000/$120		Verified: 100/$30 250/$75 500/$115 1,000/$190
Hotmail	Basic: 500/$10 1,000/$15 5,000/$65 10,000/$120		Verified: 500/$15 1,000/$20 5,000/$80 10,000/$150
Twitter MySpace	100/$15 250/$35		500/$65 1,000/$100
Hushmail AOL	500/$10 1,000/$20		5,000/$90 10,000/$160

Services are also provided should users need to increase the size of their fan clubs or friends list:

Offers	Prices
Facebook likes/fans for a fan page	1,000 worldwide fans: $50
YouTube subscribers and ratings	100 subscribers and ratings: $7 200 subscribers and ratings: $16 300 subscribers and ratings: $23 500 subscribers and ratings: $38

This quarter, three "crimeware" exploit kits made the headlines. These toolkits can be used to create botnet networks via sets of precompiled exploits to take advantage of software vulnerabilities.

Crimeware Name	Prices	Description
Blackhole v1.0.0 beta	License Annual: $1,500 Half-year: $1,000 3 months: $700	New exploit kit developed in Russia with built-in Traffic Direct System, self-defensive module, and advanced statistics widgets
Phoenix v2.4		The Phoenix Exploit's Kit first appeared in 2007 and has been regularly updated. Among about 16 exploits, eight are from 2010: • Adobe Reader LibTiff: CVE-2010-0188 • IE iepeers: CVE-2010-0806 • Java getValue: CVE-2010-0840 • Java SMB/JDT: CVE-2010-0886 • Adobe PDF SWF: CVE-2010-1297 • QuickTime: CVE-2010-1818 • Windows Help Center: CVE-2010-1885 • PDF Font: CVE-2010-2883
Eleonore v1.6 and v1.6.2	$2,000 (with possible new year's discounts)	A new version was announced in 2010. Six of 10 exploits are from 2010: • IE iepeers: CVE-2010-0806 • Java getValue: CVE-2010-0840 • Java SMB/JDT: CVE-2010-0886 • JDT: CVE-2010-1423 • Windows Help Center: CVE-2010-1885 • PDF Font: CVE-2010-2883

Hacktivism

The main actor in the political field this quarter was the "Anonymous" activist group. Its members engaged in various cyberdemonstrations against copyright protection groups early in the quarter and against WikiLeaks censors and detractors later in the quarter. Many other notable events occurred during this period, as well. In some of these examples we might assume some level of assistance from the geographies or countries where the hacktivist activities originate. The boundary between hacktivism and cyberwarfare continues to blur.

Country/Target	Date	Description
Worldwide	October– November	The Anonymous activist group launched several major distributed denial of service (DDoS) attacks against websites of copyright protection societies and adult film industries: • SGAE (Spanish agency)[3] • Hadopi (French government agency) • Hustler (leader in porn video)[4] • Recording Industry Association of America[5]
Survival International (defends indigenous tribes)	October	A DDoS attack came one week after Survival reported a shocking video of Indonesian soldiers torturing Papuan tribal people, and four weeks after calling for tourists to boycott Botswana over the long-running persecution of the Kalahari Bushmen
Vietnamese dissidents	October	While in Vietnam, a police crackdown struck bloggers critical of the government, with more than 15,000 infected computers involved in various DDoS attacks against their sites[6]
China/South Korea	October	The South Korean National Intelligence Service announced that Chinese hackers had successfully stolen confidential information from the foreign service and security officials through emails that purport to be from the Blue House or diplomats abroad[7]
Myanmar (Burma)	November	Just before holding its first real elections in more than 20 years, Myanmar's primary Internet services were hit with a massive DDoS attack that disrupted service all over the country.[8] Motivation for the attack is unknown, but many accuse the Myanmar government of wishing to isolate the country before the November 7 elections.
Tibetan diaspora	November	Phayul.com, a leading news portal of the Tibetan diaspora, was victimized—perhaps by Chinese hackers—by a DDoS attack that rendered the website slow or inaccessible
WikiLeaks	November– December	The WikiLeaks disclosure of more than 250,000 U.S. State Department diplomatic cables upset many people. WikiLeaks as well as its supporters and detractors were victims of numerous DDoS attacks from people supporting one of the two camps.

Actions Against Cybercriminals

In spite of Eastern European countries often being criticized for their laxity, the Russian Ministry of Interior decided to take action against several cybercriminal organizations:

Country	Description
Russia	• Police dismantled an international criminal group of at least 50 suspects (Russians, Ukrainians, and Armenians) alleged to have stolen more than 20 million rubles from 17 Russian banks between January and June 2010 • Criminal case filed against Igor Gusev, a businessman listed as the world's biggest spammer. He is accused of driving the Glavmed/Spamit affiliation websites, which paid spammers to promote online pharmacies and sexual performance enhancers[9] • Arrested members of a criminal group responsible for infecting ATMs with a computer virus. The leader of the gang sought the services of a hacker through an international Internet forum to customize the malware. The job cost the gang 100,000 rubles (about US$3,200)[10]
Netherlands, Armenia	The High Tech Crime Team of the Dutch National Crime Squad took down the Bredolab botnet, containing at least 30 million computer systems worldwide infected since July 2009. Armenian authorities arrested a 27-year-old man on suspicion of running and renting the botnet.
United States	• Operation In Our Sites 2.0: The National Intellectual Property Rights Center seized 82 domains selling counterfeit goods • Lin Mun Poo, a Malaysian citizen, was arrested after meeting with a "carder" (an undercover U.S. Secret Service agent) who had offered him US$1,000 cash for 30 active credit and debit card numbers. Poo was in possession of 400,000 stolen credit and debit card numbers at the time of his arrest.[11] • A young Russian man was arrested in Las Vegas. According to an FBI affidavit, he operated the Mega-D botnet, which was used in spamming campaigns.[12]

3. http://www.infosecurity-magazine.com/view/13056/anonymous-cyberprotest-group-stages-ddos-attack-on-spains-copyright-society/
4. http://www.myce.com/news/anonymous-calls-off-hadopi-attack-targets-hustler-35675/
5. http://www.app.com/article/20101102/NEWS06/101102049/Cyber-group-hacks-recording-industry-group-s-site-in-response-to-LimeWire-shutdown
6. http://www.whec.com/article/stories/S1812949.shtml?cat=10077
7. http://joongangdaily.joins.com/article/view.asp?aid=2927242
8. http://www.mmtimes.com/2010/news/547/news54716.html
9. http://www.nytimes.com/2010/10/27/business/27spam.html
10. http://news.hostexploit.com/cybercrime-news/4686-russian-gang-used-customized-virus-bought-from-hacker-forum-on-atms.html
11. http://garwarner.blogspot.com/2010/11/lin-mun-poo-hacker-of-federal-reserve.html
12. http://www.v3.co.uk/v3/news/2273647/fbi-botnet-spam-nikolaenko

About the Authors

This report was prepared and written by Pedro Bueno, Toralv Dirro, Paula Greve, Rahul Kashyap, David Marcus, Sam Masiello, François Paget, Craig Schmugar, Jimmy Shah, 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 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

McAfee, headquartered in Santa Clara, California, 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 secures your digital world. www.mcafee.com

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

20000rpt_quarterly-threat-q1_0111_ETMG