Report

McAfee Threats Report: Fourth Quarter 2011

By McAfee Labs™

Table of Contents

The final quarter of 2011 was one of significant ups and downs in the global threat landscape. The quarter serves as a microcosm for the entire year: 2011 delivered some of the most noteworthy events we have seen to date. High-profile attacks such as Duqu[1] and the rise of Anonymous-centric hacktivism made 2011 a truly challenging year for the security business. The increasing attention on industrial control systems mated with growing hacktivist activities could lead to turbulent times in 2012.

Looking back at the quarter several things jumped out. Growth in almost all areas of malware and spam declined, with the exception of mobile-based malware. Mobile malware rose during the quarter and recorded its busiest year to date. Android, once again, was the clear choice for malware writers. And although the release of new malware slowed, the total malware we've captured still managed to break the 75 million mark, a figure we predicted late in 2010.

Despite spam numbers dropping around the world, with many regions reaching multiyear lows, we still observed great diversity and specificity in subject lines. Scammers are adept at understanding what lures and subjects work both globally and locally. This tactic has not changed. The odd contradiction of botnet growth, however, continued this quarter. (Botnets usually send spam; growth in botnets would suggest growth in spam, yet that was not the case.) We saw a considerable worldwide jump in botnet detections, with Grum at the top of the pack.

This quarter the United States again hosted the most malicious web content, and the growth of sites with bad reputations was up in general. The number of active malicious URLs increased, and new malware sites almost doubled this quarter. The web continues to be a dangerous place for the uninformed and unprotected.

In this Threats Report we include a review of two new areas: database and data breaches, and network-based attacks. The number of reported data breaches increased during the quarter; and remote procedure calls, SQL injection, and cross-site scripting remain the most popular forms of network assaults.

Some of the year's most dangerous hacktivist and cybercrime actions took place during the quarter; this is a portent for 2012. We saw some advances in cybercrime toolkits, as well as events that may have involved national governments. One bright spot in the threats landscape, however, was the number of successful arrests and prosecutions of cybercriminals.

As always, threats continue to evolve, and attackers continue to push the envelope. We must remain vigilant in defending against them.

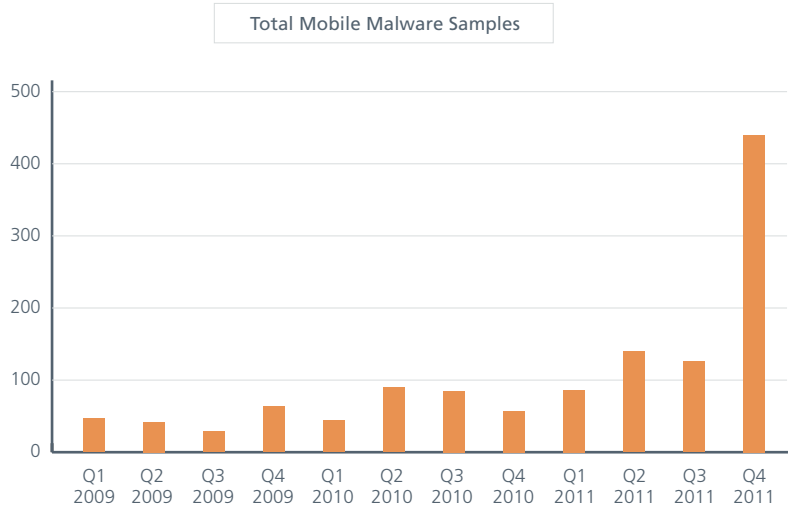
Mobile Threats

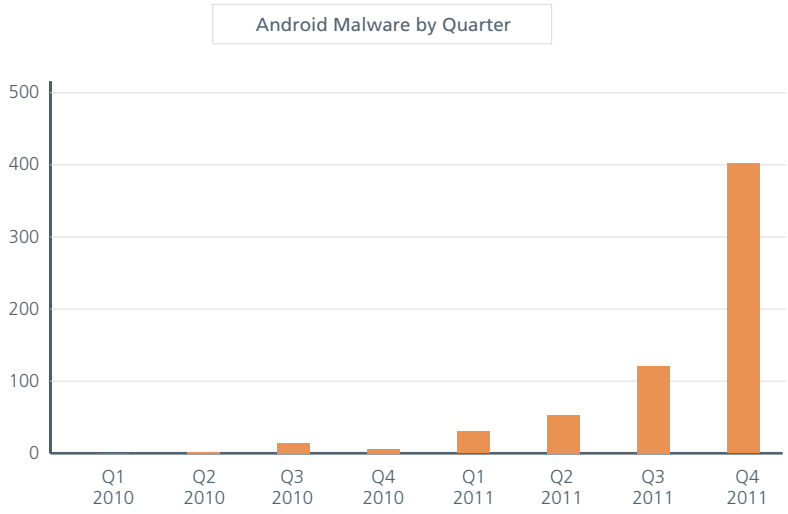
This quarter we saw Android firmly fixed as the largest target for writers of mobile malware. Like the PC, mobile platforms suffer from commercial spyware and adware. In total numbers, both 2011 and the fourth quarter were by far the busiest periods for mobile malware we have yet seen. We expect this trend to continue for quite some time.

Much of the Android malware has been for-profit SMS-sending Trojans, which benefit cybercriminals by hijacking phones to send messages that cost their owners money. We saw one interesting variant that takes that technique and carries it into the realm of hacktivism. With Android/Arspam, instead of submitting the app to the Android Market or another venue, the authors uploaded the malware to a number of Arab-language discussion forums. (The Trojan is a modified version of a Muslim prayer-calendar app.) This version sends SMS messages relating to a key figure whose death led to the start of the uprising in Tunisia. Members of the discussion forums, instead of reformatting their phones to remove the malware, forwarded the Trojan to other like-minded individuals and spread the message.

Rooting Android devices has becoming easier with the availability of apps that combine vulnerability exploits. Users can install an app, click a button, and root their phones. This also means that attackers can do the same, by repackaging those same root exploits with malware. This technique has long been popular in the PC malware world and is a great example of transitioning what works on one platform to a new one. For this reason McAfee has added detection for a number of widely available rooting apps and their included exploits.

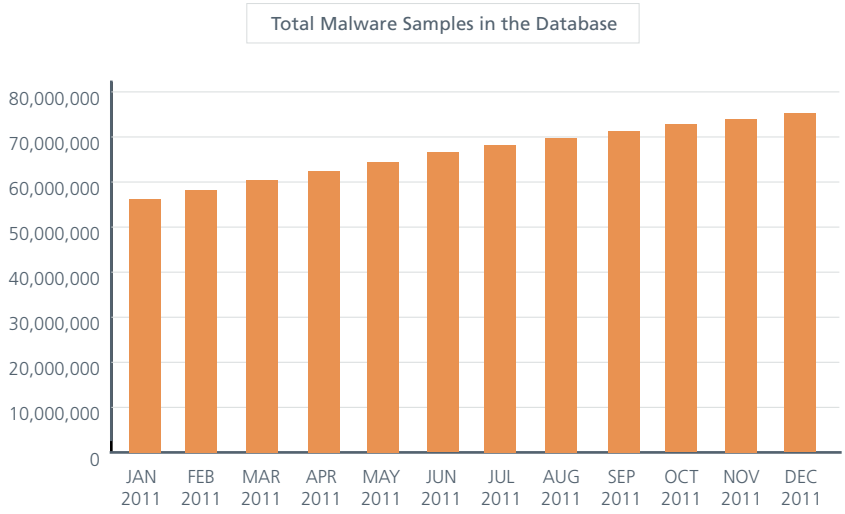
Attackers aren't the only people to use exploits. Penetration testers, professionals who test computer security, have discovered how useful mobile devices can be in their jobs. We've run across a commercial Android app that allows a penetration tester to exploit a Windows PC from a phone or tablet. Normally testers would need to carry a full-sized laptop or netbook while working; now they can avoid suspicion and still map out a client's network and perform attacks. Because attackers can also use this tool, we detect it as a potentially unwanted program named Android/AnitTool.

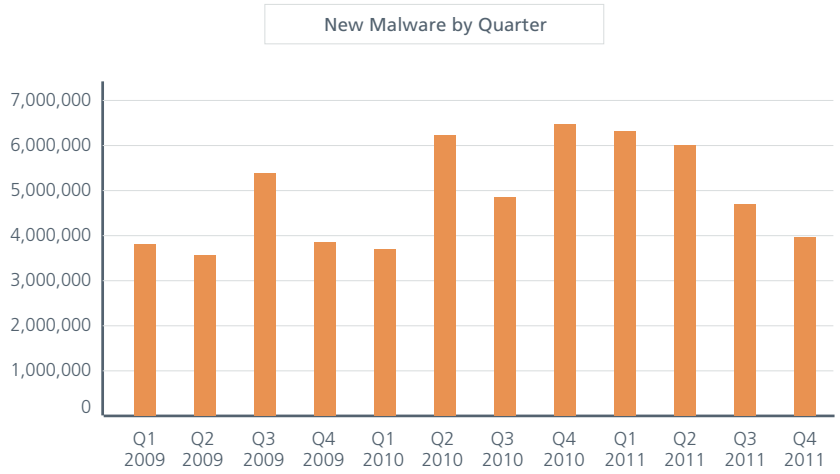




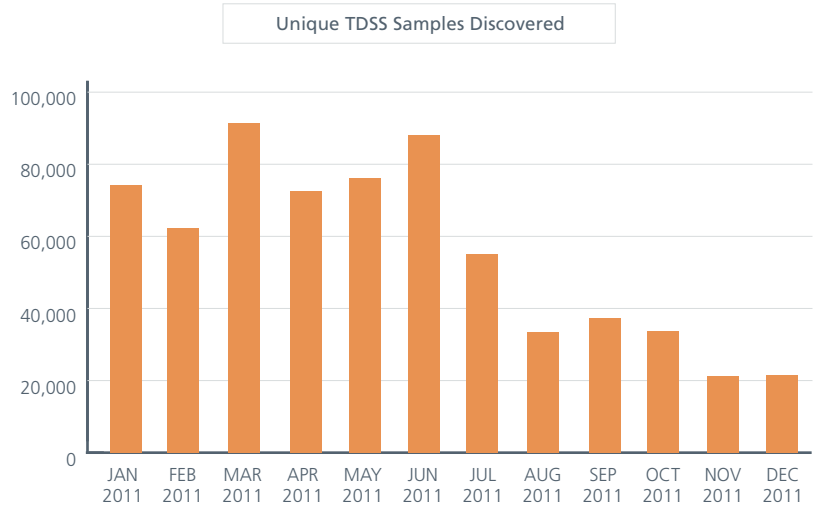
Malware

The overall growth of PC-based malware continued to decline throughout the quarter and is significantly lower than last year at this time. But don't get complacent. The cumulative number of unique malware samples in our collection still exceeds the 75 million mark, as we predicted in our last report. Has bulk malware reached a critical mass? That's not easy to answer; but as more and more of us transition to mobile computing, it is safe to assume that the threats will transition as well.

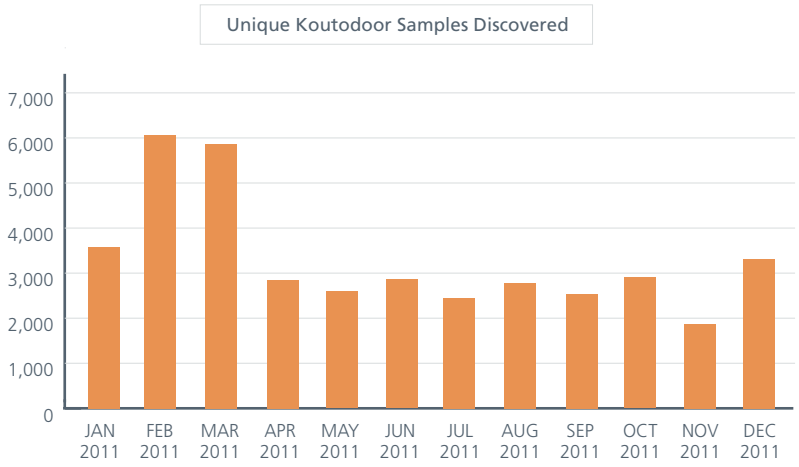


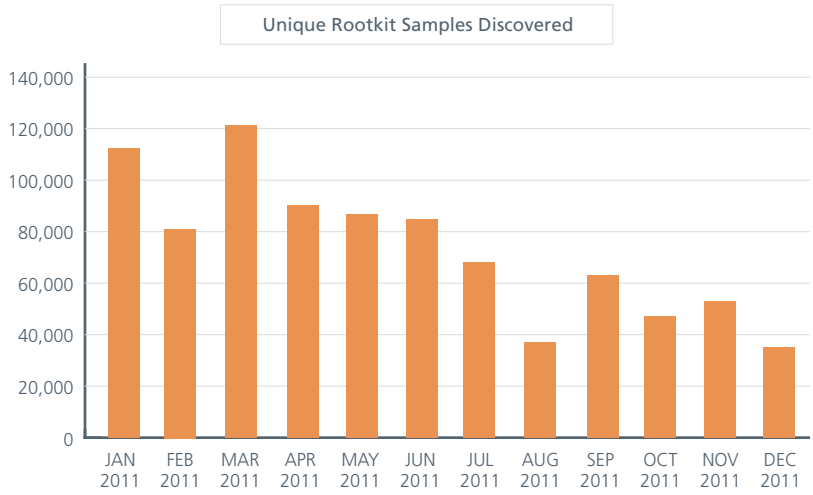


The TDSS family of rootkits, despite slowing this quarter, still represents more than half of all rootkit malware. Rootkits, or stealth malware, are one of the nastiest classifications of malware we see; they have a heavy influence on almost all other areas of malware. Rootkits are designed to evade detection and "live" on a system for a prolonged period. As we see in the graph below, the numbers of TDSS are still growing.

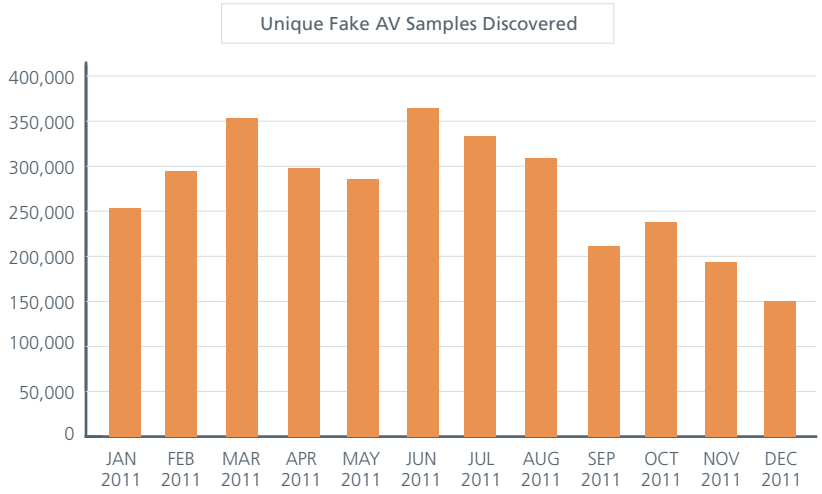


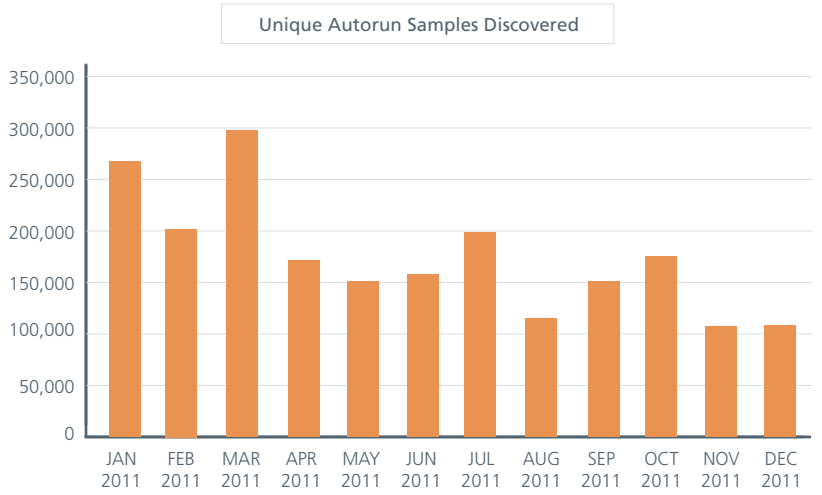
Elsewhere we see flat growth, as with Koutodoor, and a decline in the rate that all rootkits appear. Nonetheless, please stay vigilant.

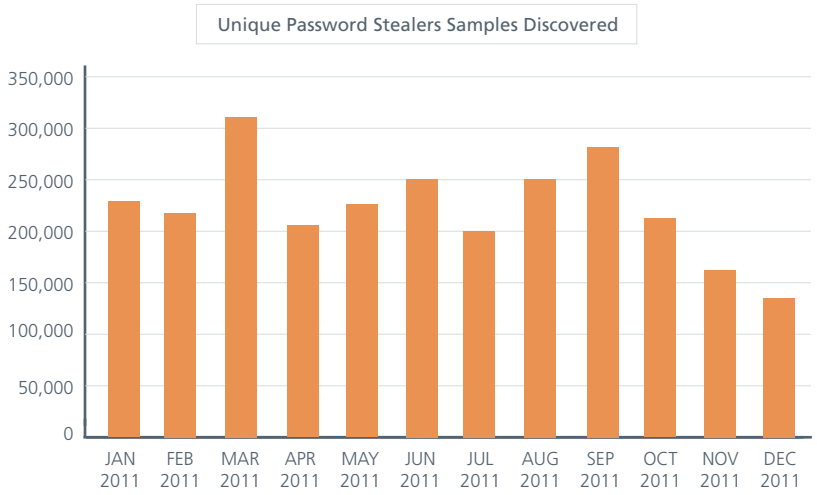




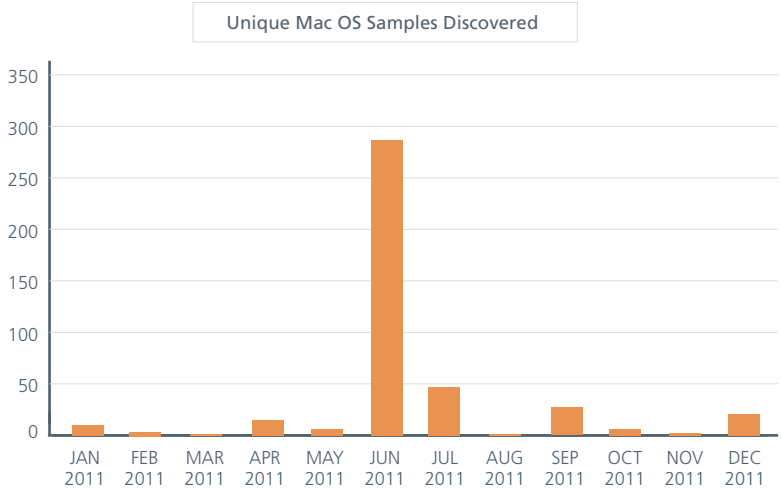
Each quarter we also track fake antivirus (or fake alert or rogue security software) and AutoRun software, along with password-stealing Trojans. Fake AV has dropped considerably from the prior quarter but it's still one of the most popular forms of malware. AutoRun and password-stealing banking Trojan malware show modest declines.



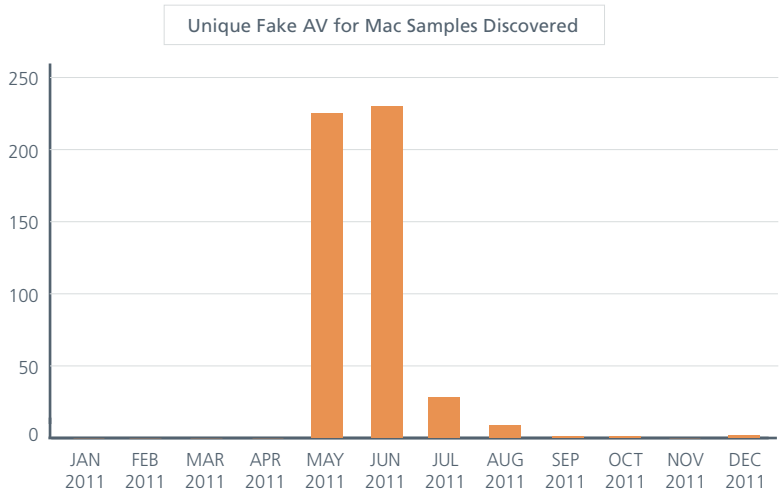




Mac malware had a big spike in the second quarter but has remained quiet since then. As always, comparing overall malware growth for the Mac with that for PCs makes the Mac threat look rather tame, but it's always wise to protect your system, even if it's a MacBook Air.



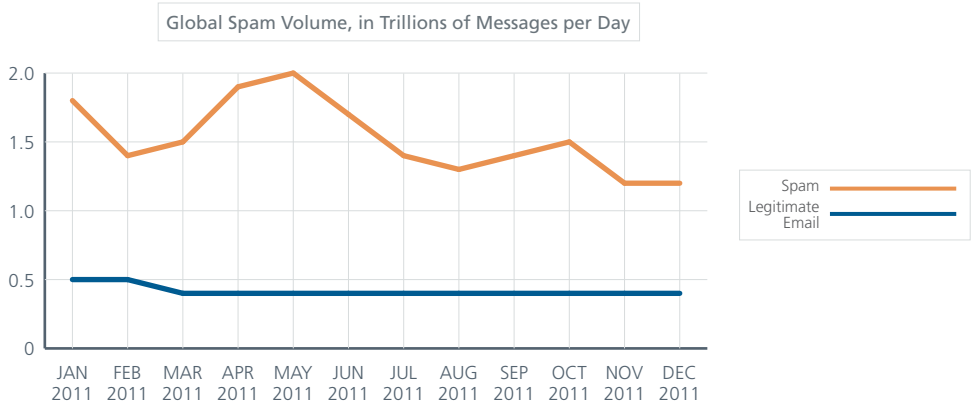
In contrast to the second-quarter spike, fake AV on the Mac is once again practically nonexistent.



Although we saw very little end-of-year activity against Macs, any OS can be a target.

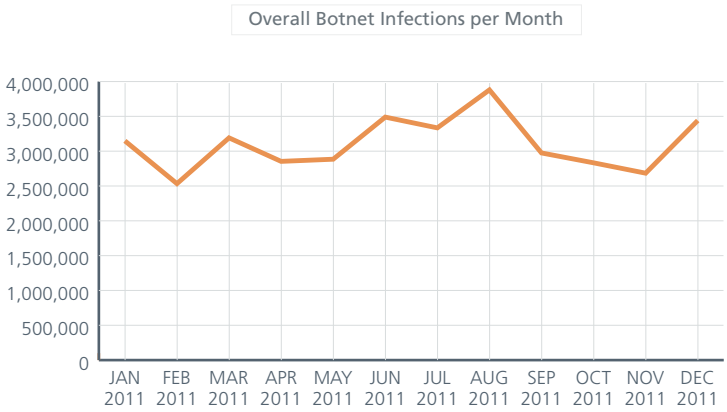
Messaging Threats

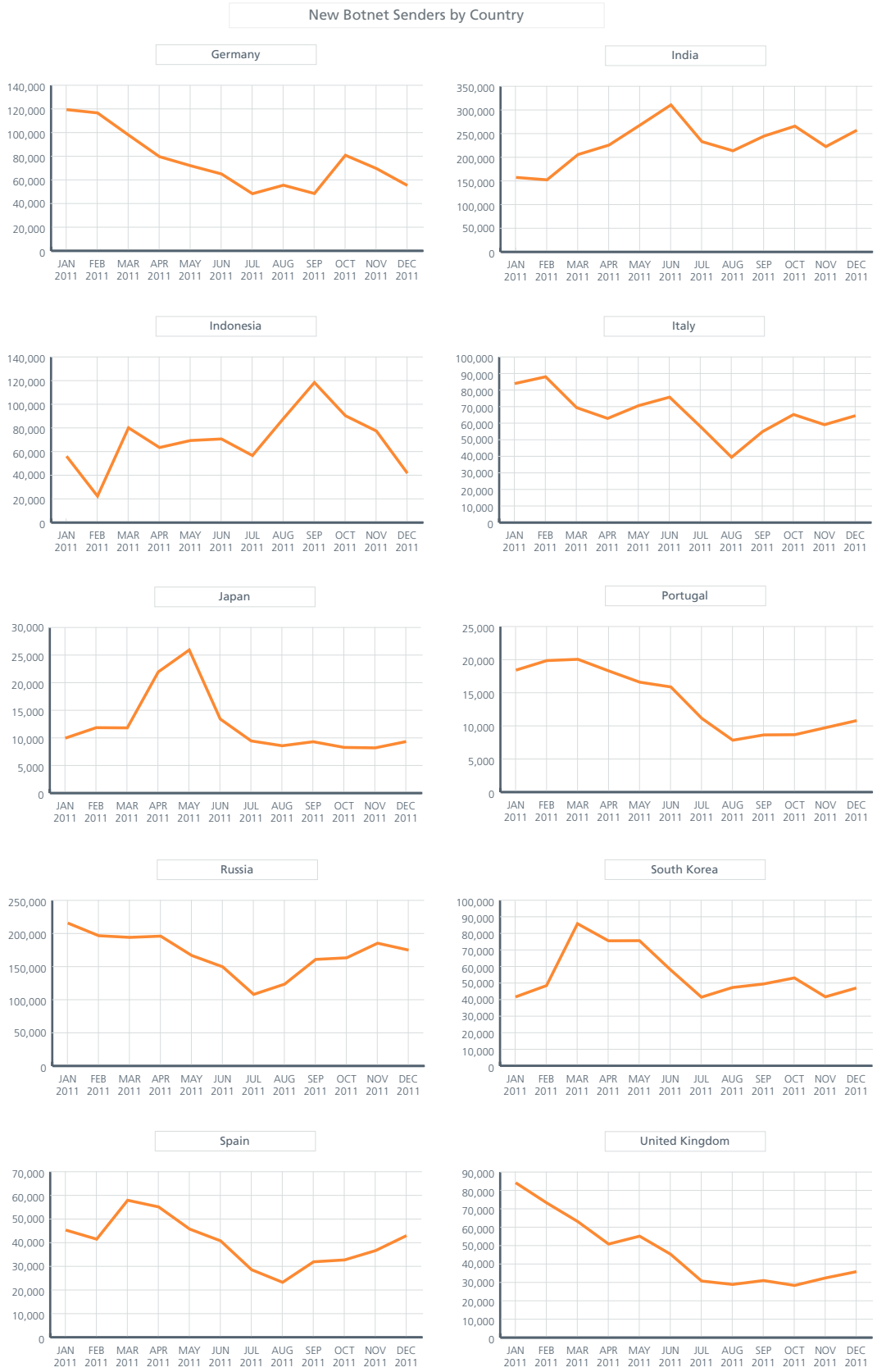
At the end of 2011, global spam reached its lowest point in years. This phenomenon is reflected in countries such as Brazil, Argentina, the United Kingdom, Turkey, and South Korea, all of which are at their lowest points since 2007. Meanwhile the United States and Germany, to name two, experienced slight increases. Despite the drop in global levels, spearphishing and spam are as dangerous as ever. Remember that although the numbers are declining, the threat level and sophistication remains high. Spammers several years ago sent mail to many random addresses, but today's address lists are much more accurate.

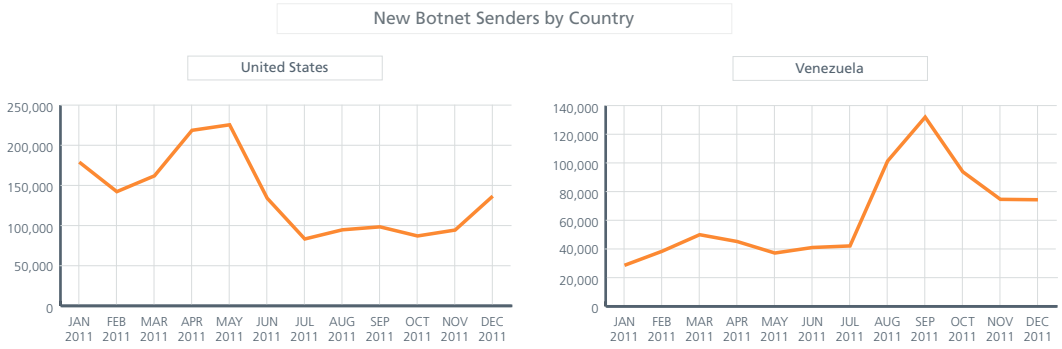


Botnet breakdowns

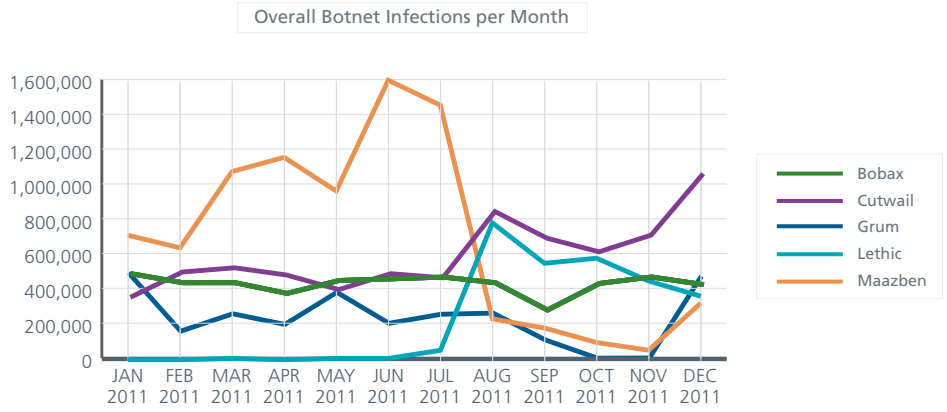
Overall botnet growth rebounded in November and December after falling since August. Brazil, Columbia, India, Spain, and the United States saw significant increases. Germany, Indonesia, and Russia, on the other hand, declined.




New Botnet Senders by Country
Germany
140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
India
350,000
300,000
250,000
200,000
150,000
100,000
50,000
0
Indonesia
140,000
120,000
100,000
80,000
60,000
40,000
20,000
0
Italy
100,000
90,000
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
Japan
30,000
25,000
20,000
15,000
10,000
5,000
0
Portugal
25,000
20,000
15,000
10,000
5,000
0
Russia
250,000
200,000
150,000
100,000
50,000
0
South Korea
100,000
90,000
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
Spain
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
United Kingdom
90,000
80,000
70,000
60,000
50,000
40,000
30,000
20,000
10,000
0
JAN 2011
FEB 2011
MAR 2011
APR 2011
MAY 2011
JUN 2011
JUL 2011
AUG 2011
SEP 2011
OCT 2011
NOV 2011
DEC 2011



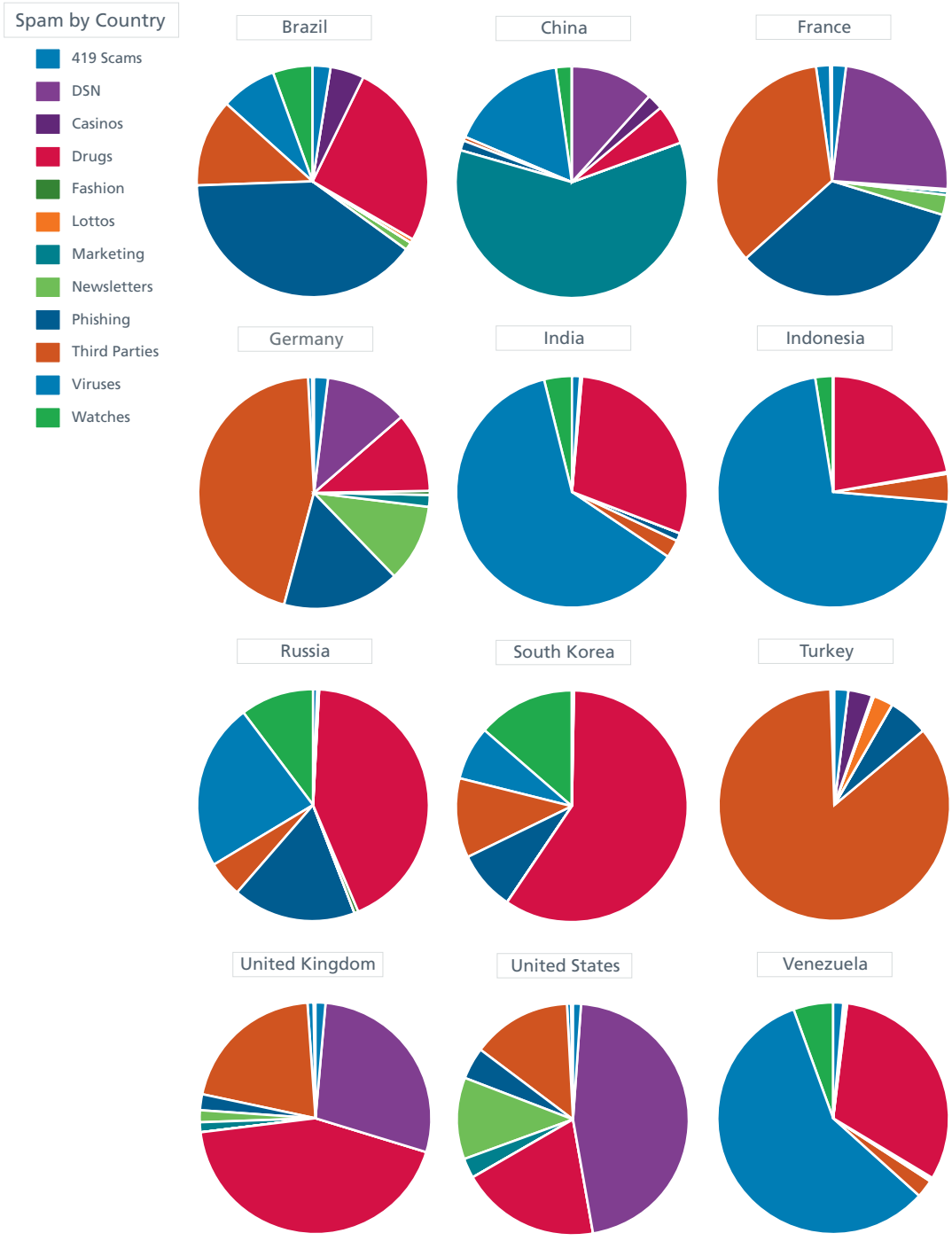
Among botnets, the usual suspects remained on the scene. Bobax rose in October and November before dipping in December. Lethic continued to fall following its peak last quarter. Cutwail and Maazben climbed significantly in December, but the real "standout" of the quarter was Grum, which after a long decline recovered its position of a year ago.



A drop in new infection rates does not mean that a botnet is losing steam. As can be seen from our breakdown by country, many of these botnets are still quite active. Each pie piece represents the percentage of activity for that botnet in that country. Pie pieces are not comparable among countries because the total number of detections by country varies considerably.

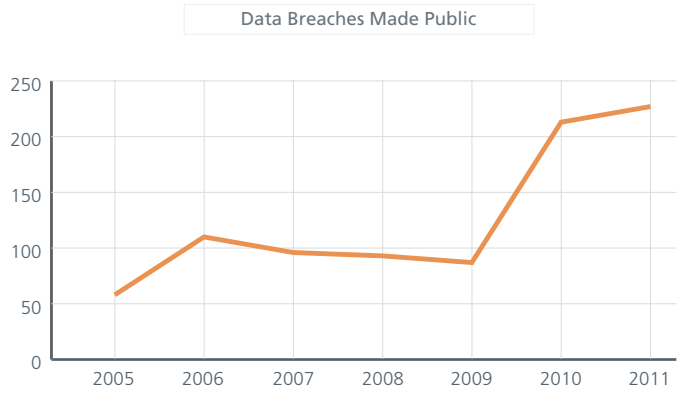
Social engineering around the world

As always, social engineering lures and spam subject lines vary greatly depending on the part of the world in which we find them. Messaging subjects still show great global diversity and specificity. Lures vary by month or season, often taking advantage of holidays and sporting events. In Brazil phishing was the most popular form of spam, while marketing-centric spam was most prevalent in China. Germany saw mostly third-party spam, while in France both third-party and phishing were popular. In contrast, drug spam was tops in the United Kingdom, and virus warnings predominated in India and Indonesia. Different lures appeal to different cultures.



Data Breaches and Network Attacks

We observed several trends during this quarter and the past year in database attacks. First we can see distinctly that the wave of reported data breaches that began several years ago has risen rapidly during the past two years. The number of reports of data breaches via hacking, malware, fraud, and insiders has more than doubled since 2009, according to privacyrights.org.



In this quarter alone we saw more than 40 breaches publically reported. Although the last three months are not the record holder in this area, data breach events continue to increase.

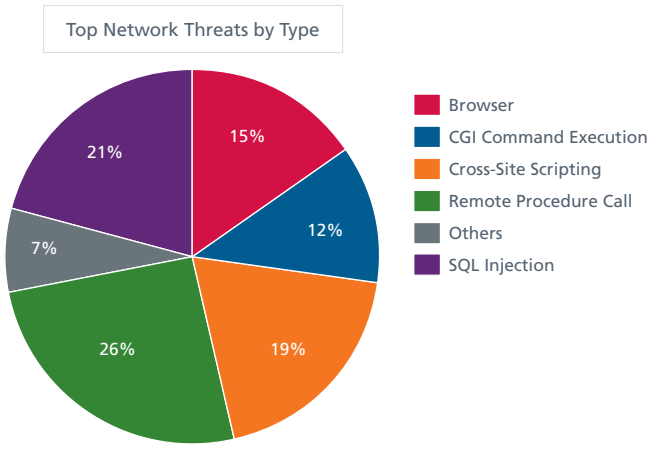
The second trend is dependent on the first. IT and security personnel are now far more aware of database intrusions. Given the increase in the volume of breaches, it's a good thing that awareness is on the rise.

A recent survey of Oracle users demonstrates this awareness:

"More than 25 percent of respondents answered that over the next 12 months data breaches are 'inevitable' or 'somewhat likely.' More than one-third of respondents who are responsible for database security in their organizations took steps to prevent SQL-injection attacks and have monitoring systems on production databases. These statistics are very encouraging, especially taking into consideration that database security solutions always historically were a most rarely found security product for years."[2]

Although the situation is far from ideal, we can see significant improvement in database security awareness. It's a pity that the impetus was an unprecedented wave of painful data breaches.

The data and analysis for our second new area, network-based attacks, comes from McAfee Global Threat Intelligence™ network.

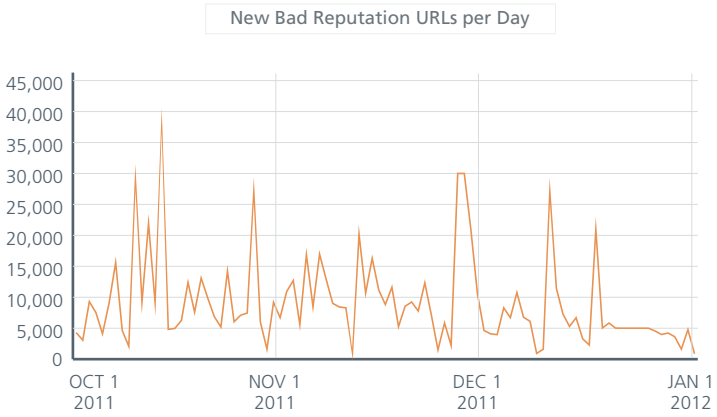


The leading network threat this quarter came via vulnerabilities in Microsoft Windows remote procedure calls. This was followed by a very close race between SQL-injection and cross-site scripting attacks. These two attacks are very much remote in nature, meaning they can be launched at selected targets around the globe. Browser attacks, on the other hand, are generally a client-side threat. Whether the high number of remote attacks leading to data breaches is reflective of increases in hacktivism and hacktivist-type activities is a question we will look at closely in the coming year.

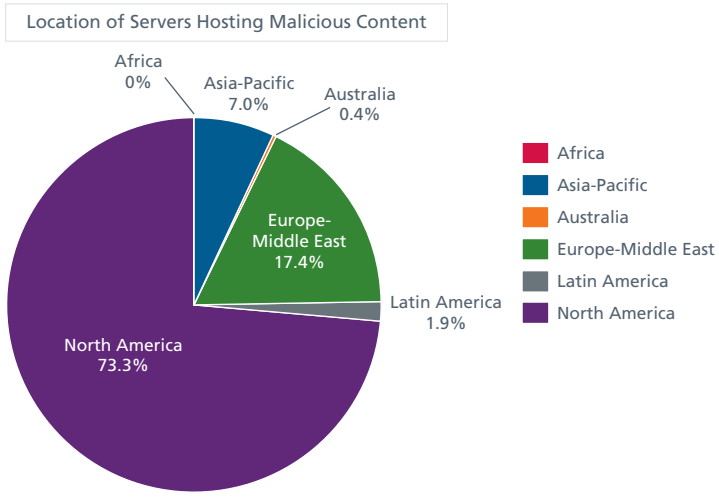
Web Threats

Websites can gain bad or malicious reputations for a variety of reasons. Reputations can be based on full domains and any number of subdomains, as well as on a single IP address or even a specific URL. Malicious reputations are influenced by the hosting of malware, potentially unwanted programs, or phishing sites. Often we observe combinations of questionable code and functionality. These are several of the factors that contribute to our rating of a site's reputation.

In the third quarter McAfee Labs recorded an average of 6,500 new bad sites per day; in this quarter that figure shot up to 9,300 hits. We also noticed that about one in every 400 URLs we attempted to load were malicious; some days that number was one in every 200 URLs! The holiday season was in full swing and cybercriminals like to abuse holidays, so these results came as no surprise.



The vast majority of new malicious sites are located in the United States. Next in line, we find the Netherlands, Canada, South Korea, Germany, the United Kingdom, Russia, and China. In the previous quarter, the top eight countries were the same though not in quite the same order. Our regional breakdown reveals where most malicious servers reside.

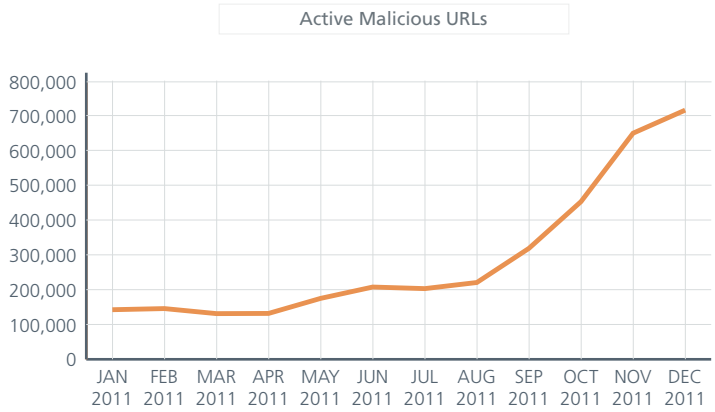


On the previous page, we can see that North America is still far in the lead and is at its highest percentage of the year. (The low point was 60 percent in the second quarter.) Europe and the Middle East remain in second place (ranging from 18 percent to 25 percent during the other three periods).

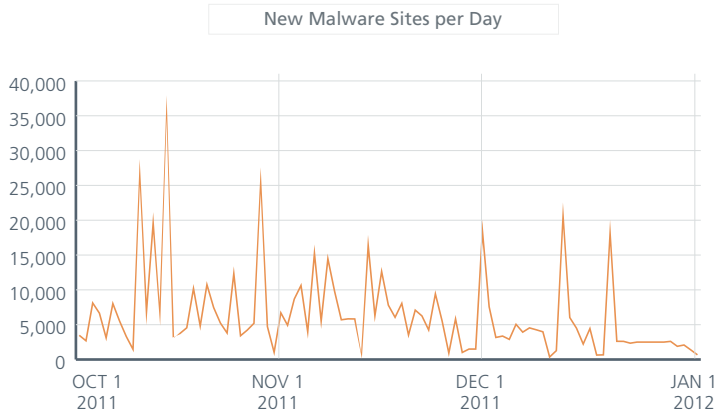
Looking closely at the classification by region, we can see that no area of the global Internet is without risk.

Location of Servers Hosting Malicious Content, by Country

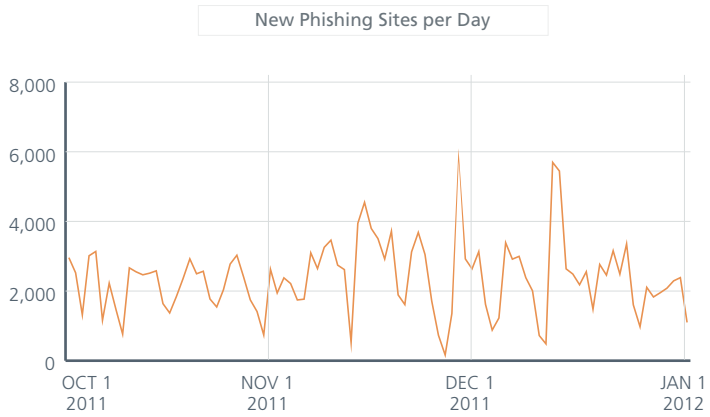
The number of websites hosting malicious URLs, a combination of bad downloads and browser exploits, continued their steady pace.



The number of websites delivering malware and potentially unwanted programs grew noticeably this quarter, with an average of around 6,500 new sites per day, compared with 3,500 per day during the third quarter.



Phishing sites showed a slight drop, as we identified approximately 2,200 new phishing URLs per day compared with 2,700 per day during the prior quarter.



Cybercrime

Crimeware tools

In October, a new Java vulnerability exploiting the Rhino Script engine was announced. This vulnerability allowed an unsigned Java applet to gain elevated privileges and to run arbitrary Java code outside of the "sandbox" environment. Not long after the discovery, an exploit module was published as a part of the Metasploit Project. It was also incorporated into various crimeware kits.

Name	Prices (all in US$)	
Phoenix Exploit Kit 3.0 (December)	$2,200 (single domain) $2,700 (multithreaded domain)	In our second-quarter report, we noted Version 2.7. This quarter we saw three updates. Version 3.0 includes the Java Rhino exploit (CVE-2011-3544).
BlackHole Exploit Kit 1.2.1 (November)	Annual license:$1,500 Half-year license:$1,000 3-month license:$700	This update also includes Java Rhino.

Key events

This quarter a variety of attacks targeted industrial systems and national infrastructure. Two of the attacks were in the southern United States.

- At the beginning of November, malware in New Zealand disabled the automated response system of St. John ambulances communication centers, which receive more than one million calls a year. The incident forced staff to temporarily abort the automated facilities and allocate ambulances manually.[3]
- On November 18, an attacker known as Pr0f released screenshots showing a user interface used to monitor and control equipment at the Water and Sewer Department for the city of South Houston, Texas.[4]
- From December 7 to December 10, malware detected on the networks of Lawrenceville and Duluth, Georgia, forced an area hospital system to declare "total diversion" status and shut its doors.[5]

On November 10, an Intelligence Note from the Illinois Statewide Terrorism & Intelligence Center announced a SCADA[6] water utility was hacked in a cyberattack traced to Russia.[7] Six days later, the Industrial Control Systems CERT reported that the incident was *not* hacking related.[8] We find it interesting that it took several days to determine this was not a cyberattack.

Actions against cybercriminals

November was a good month for taking down cybercriminals.

- On November 9, the FBI announced six Estonian cybercriminals who stole US$14 million after hacking into at least four million computers in an online advertising scam had been arrested in their country after a two-year investigation dubbed Operation Ghost Click.[9] Suspects are pending extradition to the United States. They are alleged to have used malware from the DNSChanger family to redirect unsuspecting users to rogue servers they controlled instead of to the official merchandising websites the victims wanted to reach. This takedown is potentially one of the most important in recent years.
- On November 15, the 26-year-old Romanian known online as Iceman was apprehended by Romania's organized crime and antiterrorism division after being suspected of illegally accessing NASA servers in December 2010.[10]
- On November 23, Philippine police and the FBI arrested four people suspected of diverting funds from bank accounts through hacking into the PBX phone lines of several telecommunications companies, including AT&T. Investigators explained that the attackers were possibly related to the terror group responsible for financing the deadly 2008 terrorist attack in Mumbai, India.[11]
- On December 5, a group of Thai and Nigerian individuals and corporations were sentenced to pay US$610 million in a default judgment. They are accused of spamming, between 2006 and 2009, Yahoo customers about a fake lottery.[12]

- On December 9, United Kingdom Police Central e-Crime Unit investigators arrested six people in connection with a sophisticated phishing scam that targeted hundreds of UK students in August 2011. The attackers compromised data to steal more than UK£1 million.[13]
- A decorated Ukrainian general was arrested on December 9 in Romania along with two other men suspected of being part of an organized cybercrime gang that laundered at least US$1.4 million stolen from US and Italian firms.[14] The three are accused of stealing login data for Internet banking accounts of their victims, and then transferring money from the victims' accounts to their firms.
- On December 9, the US Federal Trade Commission announced it had reached a settlement with the Ukrainian-founded company Innovative Marketing, which will provide refunds to 320,000 consumers tricked into paying for the company's scareware programs.[15] The average payout will be around US$20. Between 2003 and 2008, Innovative Marketing was a leader in the scareware market. McAfee relates the IMU saga in the report "Running Scared: Fake Security Software Rakes in Money Around the World," written by McAfee Labs senior researcher François Paget.[16]

Hacktivism

Dissension in the ranks of hacktivist group Anonymous was one of the key events this quarter.

- As part of their on-going support and sponsorship of Occupy Wall Street, Anonymous announced Operation Invade Wall Street. It promised that "on October 10th, NYSE shall be erased from the Internet" through a distributed denial of service (DDoS) attack on the New York Stock Exchange. Denials from other Anonymous factions may have disrupted the attack, which had a very small impact.
- A similar attack targeting the Toronto Stock Exchange was announced for November 7.[17] However, the story again apparently ended in an internal Anonymous disagreement, with no trading or other business disruptions seen.
- Facebook was still alive despite a controversial and disputed attack scheduled on November 5.
- On December 24, people claiming to be part of Anonymous announced it penetrated the network of US security consultant Stratfor. After stealing confidential client lists and mining more than 4,000 credit card numbers, passwords, and home addresses, the attackers used credit card information to make contributions to charitable organizations such as the American Red Cross and CARE. The main Anonymous group quickly claimed that it played no part in the breach and blamed Sabu and LulzSec members.[18]
- The year ended with the operation #lulzxmas, described by Anonymous as a weeklong hacking campaign against sites related to global finance, militaries, and governments. Its goals and targets remain to be seen.

This quarter "doxing" the police (releasing photos of police and publishing their personal and family details on the Internet) was another frequent hacktivist activity.

- On October 26, information about Oakland, California, police officers was released online in response to the police's use of force during a demonstration protesting the clearing of the Occupy Oakland encampment.[19]
- On November 18, the California Department of Justice announced that an attacker gained access to the Gmail/Google account of a special agent supervisor in charge of computer crime investigations.[20] That day, 38,000 emails from two accounts and various personal materials were published on a hidden site on the Tor network and released on file-sharing sites.
- After photos surfaced of a policeman pepper-spraying Occupy protestors on the University of California, Davis campus on November 18, his personal contact information was spread online.[21]
- At the end of November, LulzSec Portugal launched DDoS attacks against state services, political parties, and national police websites to denounce austerity measures, social inequalities, and alleged episodes of police brutality against demonstrators on November 24. The group also released the name, rank, identification number, contact information, and employment history of more 107 Lisbon police officers.[22]

- For several months in France, the Copwatch site published personal data on police members accused of brutality or linked to far-right ideals. A High Court injunction requested that the main French ISP block the site.[23]

Doxing as a technique not only targets the police, but also public figures such as politicians as soon as they are perceived to take unfavorable stances or actions against certain hacktivist ideals. On December 15, Anonymous released various dumps of information on American senators who passed the National Defense Authorization Act (NDAA). In France, we saw right-wing and far-right-wing politicians have their personal information spread online after they made some controversial opinions, statements, and policies.

Cyberskirmishes

The topic of hacktivism became popular only in 2010. At that time we included the cyberactions in Estonia (2007) and Georgia (2008) as examples. Again this quarter, several events appear to move beyond hacktivism to possible government or political sponsorship.

- On November 1, the Palestinian communications Minister Mashur Abu Daqqa blamed hackers from around the world for attacking Palestinian servers, and for cutting phone and Internet services across the West Bank and Gaza as well as those of the Palestinian communications minister. The incident came a day after the Palestinians won full membership in UNESCO, over objections from the United States and Israel, and the minister suggested that Israel could be behind the attack.
- In South Korea on December 3, the National Police Agency's Cyber Terror Response Center announced that it had apprehended and requested detention warrants for four individuals on charges of ordering the denial of service attack on the National Election Commission website on the morning of October 26, election day. This cyberattack made information on voting locations inaccessible. One suspect is a former aide of the ruling Grand National Party lawmaker. It is rumored a sum of 10 million won (US$8,619) was transferred six days before the Seoul mayoral by-election from the bank account of a secretary of the former National Assembly Speaker into that of the suspect. Five days later, various money transfers were also detected to another individual who allegedly carried out the attack.[25]
- As Russia was about to hold elections at the beginning of December, popular liberal Russian media outlets and an election watchdog were brought down by coordinated denial of service attacks. Several other independent media sites that had covered voting violations were also affected by cyberattacks.[26]
- Attackers calling themselves Moroccan Deterrence Forces carried out what they called Moroccan Vengeance by attacking several Qatari official websites after the League and Cup channel presented pictures of the Moroccan delegation at the Pan Arab Games (December 9–December 23) with a Moroccan map that excluded the Moroccan Sahara.[27]

Cyberevents sponsored by governments are difficult to pin down. The coming year is certain to provide more examples of attacks of and defenses against cybercrime, hacktivism, and possible cyberwarfare.

About the Authors

This report was prepared and written by Zheng Bu, Toralv Dirro, Paula Greve, David Marcus, François Paget, Ryan Permeh, Vadim Pogulievsky, Craig Schmugar, Jimmy Shah, 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 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, 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 finding new ways to keep our customers safe. www.mcafee.com

[1] https://blogs.mcafee.com/mcafee-labs/the-day-of-the-golden-jackal-%E2%80%93-further-tales-of-the-stuxnet-files
https://blogs.mcafee.com/mcafee-labs/of-kernel-vulnerabilities-and-zero-dayz-a-duqu-update
[2] "Databases are more at risk than ever: Oracle 2011 IOUG Data Security Survey."
[3] http://www.stuff.co.nz/waikato-times/news/5953497/Computer-virus-hits-ambulances
[4] http://news.cnet.com/8301-27080_3-57327968-245/hacker-says-he-broke-into-texas-water-plant-others/
[5] http://www.securitynewsdaily.com/computer-worm-shuts-down-atlanta-hospitals-1416/
[6] Supervisory Control and Data Acquisition
[7] http://community.controlglobal.com/content/water-system-hack-system-broken
[8] http://us-cert.gov/control_systems/pdf/ICSB-11-327-01.pdf
[9] http://www.fbi.gov/news/stories/2011/november/malware_110911/malware_110911
[10] http://news.softpedia.com/news/Romanian-NASA-Hacker-Graduates-From-University-of-Weed-235069.shtml
[11] http://www.reuters.com/article/2011/11/26/us-philippines-usa-idUSTRE7AP06320111126
[12] http://news.cnet.com/8301-27080_3-57338828-245/yahoo-awarded-$610-million-from-lottery-spammers/
[13] http://content.met.police.uk/News/Six-arrested-arrested-in-million-pound-phishing-scam/1400005228273/1257246745756
[14] http://krebsonsecurity.com/2011/12/ukrainian-general-arrested-in-cyber-heists/
[15] http://www.ftc.gov/opa/2011/12/rebates.shtm
[16] http://www.mcafee.com/us/resources/white-papers/wp-running-scared-fake-security-software.pdf
[17] http://www.nowtoronto.com/news/webjam.cfm?content=183319
[18] http://www.talkleft.com/story/2011/12/25/124727/35
[19] http://www.scmagazineus.com/anonymous-downs-oakland-police-site-after-violence/article/215433/
[20] http://arstechnica.com/tech-policy/news/2011/11/anonymous-exposes-cybercrime-investigators-gmail-voicemail.ars
[21] http://www.washingtonpost.com/blogs/blogpost/post/anonymous-targets-pepper-spraying-uc-davis-cop/2011/11/22/gIQA0Pr8lN_blog.html
[22] http://tek.sapo.pt/noticias/internet/lulzsec_ataca_mai_e_divulga_dados_pessoais_de_1204169.html
[23] http://blog.indexoncensorship.org/2011/10/17/france-copwatch-site-blocked/
[24] http://www.google.com/hostednews/afp/article/ALeqM5hsZ6qUDvnFIrgo9CyZ9u_NhGu-Og
[25] http://english.hani.co.kr/arti/english_edition/e_editorial/510303.html
[26] http://www.euronews.net/2011/12/04/russian-election-hackers-attack-opposition-sites/
[27] http://moroccoworldnews.com/2011/12/moroccan-hackers-attack-media-websites-in-qatar/18702

41604rpt_quarterly-threat-q4_0112_fnl_ETMG

McAfee
An Intel Company

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