Report

McAfee Threats Report: First Quarter 2010

By McAfee Labs™

Key Findings

The proliferation of remote devices makes it harder to defend corporate networks. But the gadgets are not going away. IT staffers need to expand security wherever their users go.

Recent tragedies continue to attract scammers. Earthquakes and other disasters are money-making opportunities for cybercriminals.

After a decline and spike in 2009, spam volume has returned to mid-2008 levels. Drawing data from our worldwide spam collectors, we illustrate which spam topics are most popular in 34 countries.

Malware growth seems to be leveling off or declining in some areas, but the cumulative numbers are still immense. We anticipate cataloging at least as much malware this year as in 2009.

Operation Aurora is one of the most important targeted attacks in Internet history. Aurora may have a significant impact for years to come on the perception of corporate-focused cybercrime.

Spring means tax time, and tax-services scams play along. Some look convincingly like legitimate banks and national tax agencies.

Manipulating search results can bring cybercriminals revenues from fake security software, as well as advertising income from click fraud.

The Zeus Trojan is just one of the key tools of cybercriminals, who often tie password stealers with other types of illegal online material such as pornography and fake security software. The prime target for these attacks? Facebook users.

Almost all URLs rated as malicious by McAfee's TrustedSource Technology are located in the United States. Malware distributors love to use Web 2.0 features, which abound in this country.

The most popular attacks on clients—including Operation Aurora—targeted Microsoft Internet Explorer and Adobe Reader and Acrobat.

The justice system caught up with several cybercriminals, in cases ranging from the theft of credit card numbers to the illegal purchase and sale of concert and sports tickets.

One of the most popular types of cybercrime is scareware, or fake security software. Installed invisibly, these scams convince users that their systems are infected and they must immediately purchase a tool to remove it. Scareware developers earn a phenomenal amount of money from their victims.

Political hactivism continues: Hackers interrupted service or defaced websites at a Russian magazine, the Latvian tax agency, and the Australian government.

Table of Contents

Do Technology Advances Threaten the Network?

Have you noticed how high-tech product announcements often create a lot of buzz? New gadgets that propose to make our work life more productive and our personal life more fun vie for our attention and money. Want to get more done in less time, in more places, and have more fun staying connected? Sign us up!

The edge of the enterprise network has expanded well beyond the office and data center and is now limited only by the geographical dispersion of the employees. In other words, your network is everywhere your people are. Advances in technology and connectivity allow this expansion to occur at a speed that often overwhelms IT departments, which exhaust themselves trying to keep up with changes while maintaining some control over what connects to the network. This rapid pace is made more difficult when executives purchase the coolest gadgets and blame the IT guys when their new toys don't talk to the network.

Every new device that employees bring into the organization opens new avenues for threats to enter the network from the inside. Prudent companies have made significant investments in stopping external threats. Many widely distributed attacks are easily identified and stopped before they become a danger to the network. These bulwarks have caused cybercriminals to look for ways to penetrate a network from the inside, where defenses are often less formidable. In many cases hackers attack the weakest link of the security chain, the user. Operation Aurora, which made headlines in January and continues to do so as more companies realize they may also have been compromised by Aurora-like attacks, is a prime example of user exploitation that can lead to the loss of valuable intellectual property.

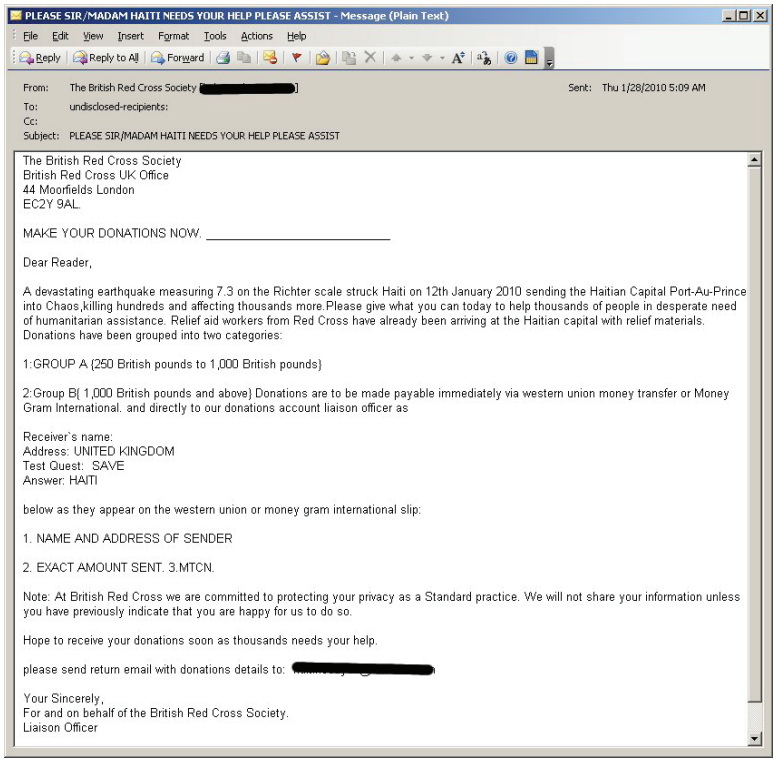
Computing devices of all shapes and sizes are frequently shared between a user's work and home networks; the latter typically have far less stringent security controls. This laxity at home allows home network infections to enter the office and threaten the safety of the corporate network and its data. Allowing technology to enable your employees can lead to increased productivity and better satisfaction in the workplace, but be sure to realize the potential risks to your organization if you do not control company data and how it moves in and out of the network.

Tragedy Can Bring Out the Worst in People

There is nothing like a catastrophe to bring people together for the common good. People from all around the world will band together in times of crisis to help strangers who have lost everything because of earthquakes, hurricanes, floods, or other events. It is a testament to the good nature of the human spirit to see such an outpouring of support.

Unfortunately, in spite of the good works that such events inspire, in the Internet security world we see some of the worst that comes out of these tragedies, especially cybercriminals who prey on that generous human spirit. They attempt to leverage the good nature of concerned people around the world to steal their money and identities using phishing scams. The scams claim to be legitimate relief efforts whose goal is to benefit those suffering.

The recent earthquakes in Haiti illustrate this criminal behavior. Shortly after the first terrible temblor struck the poor island nation, relief efforts started pouring in and the scams started pouring out. Emails sent to unsuspecting victims asked for donations to fraudulent causes.


PLEASE SIR/MADAM HAITI NEEDS YOUR HELP PLEASE ASSIST - Message (Plain Text)

File Edit View Insert Format Tools Actions Help

Reply Reply to All Forward

From: The British Red Cross Society [redacted] Sent: Thu 1/28/2010 5:09 AM

To: undisclosed-recipients:

Cc:

Subject: PLEASE SIR/MADAM HAITI NEEDS YOUR HELP PLEASE ASSIST

The British Red Cross Society
British Red Cross UK Office
44 Moorfields London
EC2Y 9AL

MAKE YOUR DONATIONS NOW. _____

Dear Reader,

A devastating earthquake measuring 7.3 on the Richter scale struck Haiti on 12th January 2010 sending the Haitian Capital Port-Au-Prince into Chaos,killing hundreds and affecting thousands more.Please give what you can today to help thousands of people in desperate need of humanitarian assistance. Relief aid workers from Red Cross have already been arriving at the Haitian capital with relief materials. Donations have been grouped into two categories:

1:GROUP A (250 British pounds to 1,000 British pounds)

2:Group B(1,000 British pounds and above) Donations are to be made payable immediately via western union money transfer or Money Gram International. and directly to our donations account liaison officer as

Receiver`s name:
Address: UNITED KINGDOM
Test Quest: SAVE
Answer: HAITI

below as they appear on the western union or money gram international slip:

1. NAME AND ADDRESS OF SENDER

2. EXACT AMOUNT SENT. 3.MTCN.

Note: At British Red Cross we are committed to protecting your privacy as a Standard practice. We will not share your information unless you have previously indicate that you are happy for us to do so.

Hope to receive your donations soon as thousands needs your help.

please send return email with donations details to: [redacted]

Your Sincerely,
For and on behalf of the British Red Cross Society.
Liaison Officer

Figure 1: This call for donations was typical of fraudulent emails sent in the aftermath of the Haitian earthquakes.

At first glance these appeals may seem like noble causes that have the interests of the people of Haiti in mind, but the reality is that if you pledge a donation with these "services" your money will never arrive where you intended. In Figure 1 you'll notice that donations of more than UK£1,000 are highly encouraged and should be made directly via money wire services.

Of course not all relief services are fraudulent. There are many legitimate services that will make sure your donations are well spent and will go directly toward helping the victims. The key is to do your research and work only with those services that have a well-established reputation for appropriately handling relief funds. Be wary when responding to any request for money over email; you'll take some important steps to securing your identity online.

Spam Volumes Return to Mid-2008 Levels

Spam volumes remained relatively unchanged between the fourth quarter of 2009 and the current quarter, increasing only about 5 percent. Between January and March, spam traffic averaged approximately 139 billion messages per day, or 89 percent of all email traffic. In the prior quarter spam accounted for 133 billion email messages per day.

As we predicted in our *McAfee Threats Report, Fourth Quarter 2009*, the 24 percent decline in spam volumes that we saw at the end of last year was short lived.[1] After a record peak in mid-2009 in which spam traffic averaged 175 billion messages per day, volumes have returned to mid-2008 levels, as they were just prior to the shutdown of the McColo spam hosting provider in November of that year.

Pill and male-enhancement messages made up the majority of the spam this quarter, accounting for more than 71 percent of spam traffic. Emails containing generic offers came in a distant second, accounting for only 10 percent of spam traffic. Spam touting education or degrees, and personal ads represented less than 2 percent each.

1. The *McAfee Threats Report* is available in nine languages. http://www.mcafee.com/us/threat_center/white_paper.html

Global Spam Volumes

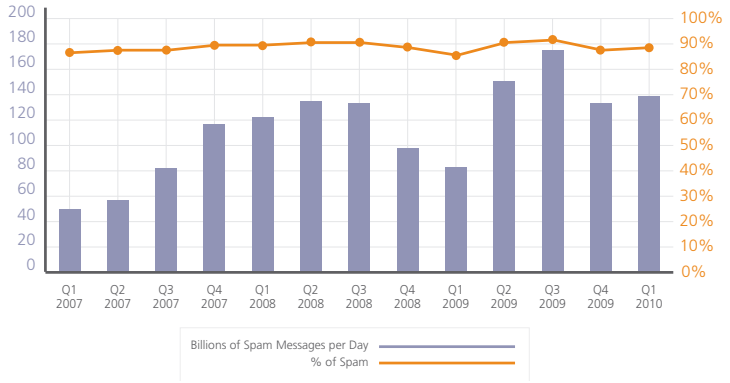


Figure 2: Global spam volumes and spam as a percentage of all mail.

Spam Trends Around the World

McAfee has a number of nodes throughout the globe collecting mail flow data that we use to observe spam trends. When we examine this data closely, we can determine the source country of certain types of spam. It's difficult to accurately compare this raw data from different geographies, but we can get a good view of the kinds of spam that most commonly come from various countries. The subject matter of the spam often touches on issues that concern people in those nations.

In this section we present a series of pie charts that show the most popular types of spam coming from 34 countries. We also categorize and explain the types of spam that appear in the charts. These collections do not represent all spam originating in a country, only the most popular types.

By volume these categorized messages account for between 40 percent and 70 percent of all data collected in the region. We eliminated personal messages, general communications, and low-volume spam campaigns from consideration. The results are meaningful as we present them here, but they do not represent a full overview of the types of mail originating from the individual countries.

We chose 20 common categories to classify these spam messages. Here they are with a brief description:

419 Scam: A confidence game in which someone will try to extort money from victims who willingly give it up because of a tragic story or the promise of a reward. Some formal-looking documentation usually completes the ruse. These types of messages often come from hosts that provide free email accounts, but we see an increasing trend of these messages coming from infected hosts as well.

Adult Products: Spam mails that advertise pornography, usually DVD movies or download sites. By volume, pornography is not as large a part of the spam world as most people think, but the effect of a single pornographic email on the recipient is exponentially greater than other types of spam, and the chance of its generating a complaint is greater still.

Casinos: These emails advertise for online casinos. They are often associated with botnet activity and require victims to download and install software to play the games.

Diplomas: Offering fake diploma sites, where clients can request forged documents that "prove" they have graduated from a certain school. These are not legitimate academic institutions and do not represent actual education. Often associated with botnet activity.

Delivery Status Notification (DSN): Also called NDRs (non-delivery receipts). These messages may be legitimate, but usually they are spam that bounces back to a forged From: address. Higher ratios of DSN messages could indicate larger volumes of individually maintained email servers.

Drugs: This category includes the faux Canadian pharmaceutical spams that are generally hosted in China, açai-berry spam, dietary supplements, etc. These messages are usually associated with botnet activity, but can also come from hosted web farms that send mail into some other country.

Jobs: Many are a form of 419 scam or confidence scam. They prey on the unemployed or underemployed and sap money from them through check fraud or entice them to launder money or perform activities of questionable legality.

Lists: Offering contact lists, such as a list of doctors or dentists in your area.

Lonely Women: Often a form of confidence scam. The criminals (probably males pretending to be females) try to get money from victims for plane tickets, customs, food, travel, or other expense to "meet" the sucker with the bank account. Russian bride spam is the most common form of this.

Lotteries: Your email address has been randomly selected from our database to get bags of cash; you just have to send us US$3,000 to handle the processing. This is another form of confidence scam.

Malware: Anything that comes with a virus or Trojan attachment or that urges you to visit an infected website. "UPS tracking number" and "Conficker.B Infection Alert" are common examples.

Marketing: Advertising or selling a product to a recipient who opted into receiving messages. An example of this is an airline or travel agency sending a list of deals to the recipient. These emails are first-party advertising, meaning that recipients should know why they are getting the email. These are different from third-party advertising, which we'll discuss later.

Newsletters: An informational email that recipients sign up for. A newsletter probably does not sell products directly, but often urges customers with fancy wording and flashing text. Examples are an alert from a news company or updates from discussion lists.

Phishing: Any email that begins a process of extracting personal information from a victim. Banking alerts that require your username and password are the leading example.

Products: Any unsolicited spam mail that tries to sell manufactured goods (usually replica purses or jewelry). These mails are not from a legitimate company and are often associated with botnet activity.

Social Networking Sites (SNS): Generated by social networking sites and sent to their subscribers. Such sites often send unsolicited emails to a user's entire address book, usually without alerting the subscriber. Although such spamlike behavior is undesirable, our data collections make no distinction between solicited or unsolicited social networking emails.

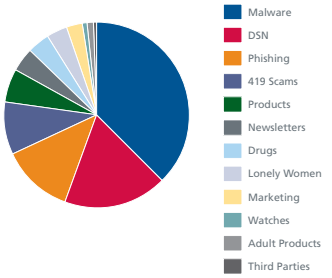
Software: Attempts to sell OEM licenses as individual licenses or tries to sell hacked or cracked copies of software at heavily discounted prices.

Stocks: Part of a "pump and dump" stock scheme. Someone buys penny stocks and then sends out a bunch of spam that creates a false demand, allowing the spammer to sell the stock for a profit.

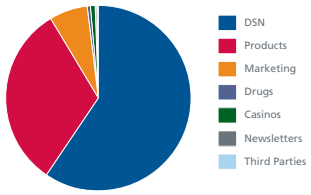
Third Parties: These lie between marketing and products spam. The company at one end of the spam mails is legitimate, and the recipients have probably inadvertently opted in to allowing partner advertisers to send them mail. Email lists can also be purchased from companies that are going out of business or in some cases the privacy statements allow companies to sell customer email addresses. Free t-shirts, insurance offers, and medical devices are all common examples. These spams are often sent from hosting facilities in foreign countries, which makes it more difficult for people to complain. Such spammers will subscribe to the letter of the CAN-SPAM Act while completely subverting its intentions by using anonymous domains, malformed and misspelled words, and embedded hidden text blocks.

Watches: This easily distinguishable message is the most common form of products spam.

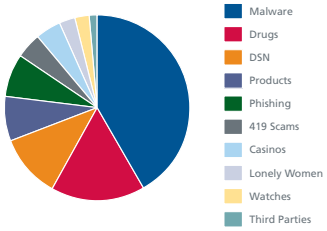
Argentina



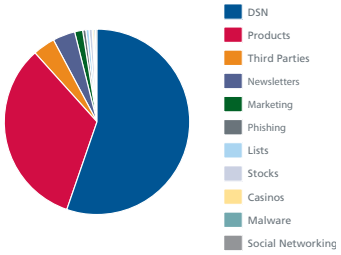
Australia



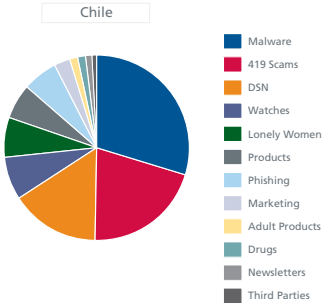
Brazil



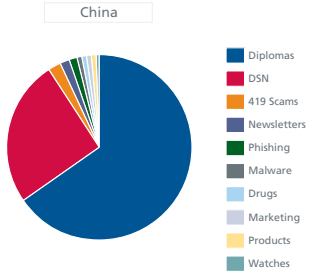
Canada



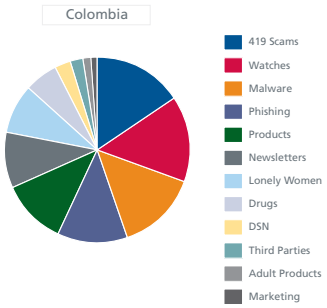
Chile



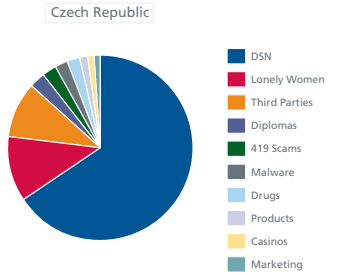
China



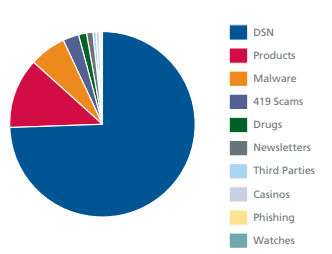
Colombia



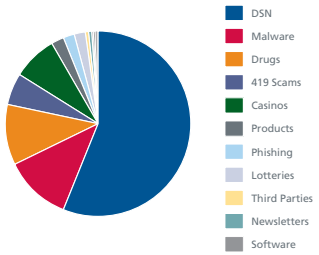
Czech Republic



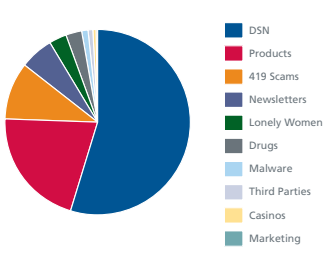
Germany



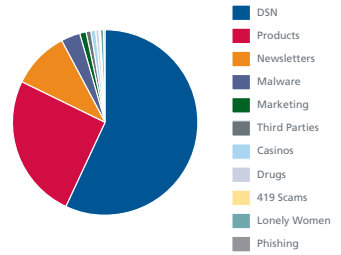
Spain



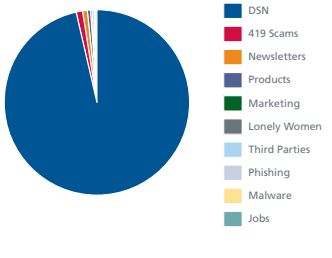
France



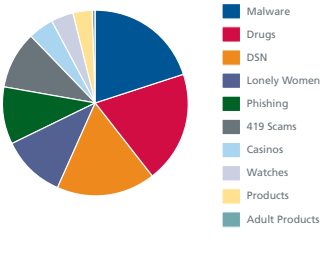
United Kingdom



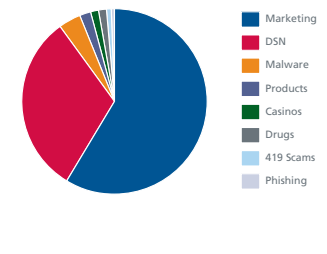
Hong Kong



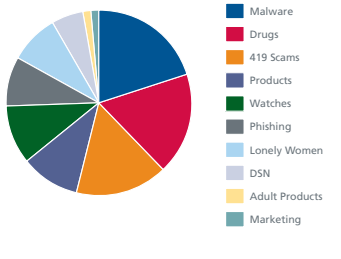
Indonesia



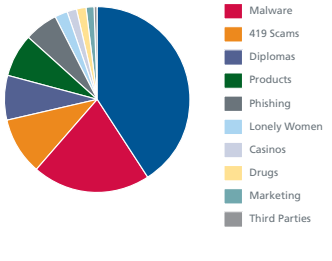
Ireland



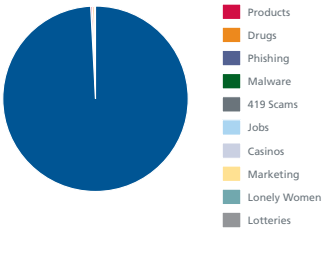
India



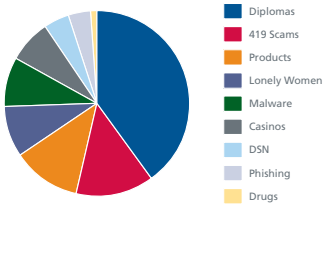
Italy



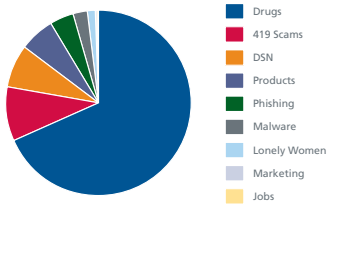
Japan



South Korea



Kazakhstan



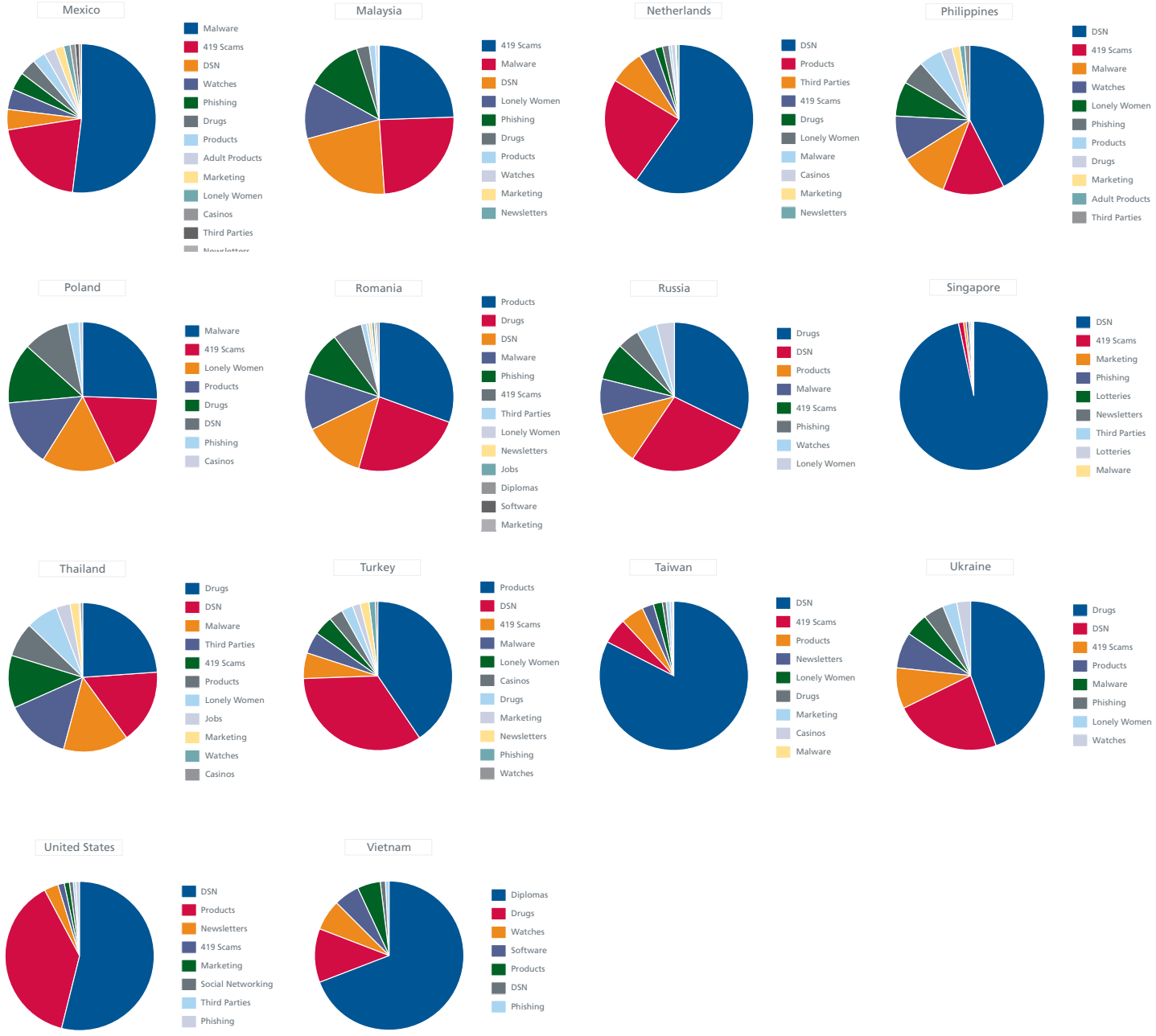


Figure 3: Spam subjects vary considerably among countries. These charts show the varying importance of the leading topics originating within each nation. These subjects do not represent all spam traffic, only the most popular.

A few surprises

The most unexpected result of this analysis is the significant amount of diploma spam coming from China, South Korea, and Vietnam. Diploma spam advertises forged documents to establish qualifications for jobs and other activities.

Singapore, Hong Kong, and Japan all had exceptional DSN message rates. These numbers could indicate mail-filtering problems that prevent spam from being caught and stopped early enough to prevent the generation of the notices to the forged From: address.

Thailand, Romania, the Philippines, India, Indonesia, Colombia, Chile, and Brazil have all made huge strides in Internet development during the last five years. This fast growth and focus on access instead of security may have resulted in a higher portion of malware infections and spam.

Malware Growth Remains 'Healthy'

In 2009, McAfee Labs catalogued and protected against more than 16 million pieces of malware. This figure rose from a little over 10 million malware in 2008. By the end of March 2010 we have already seen and protected against more than three million pieces of malware. The first-quarter results suggest that overall growth has leveled off; however, we anticipate that we're on track to catalog *at least* as much malware in 2010 as in the prior year.

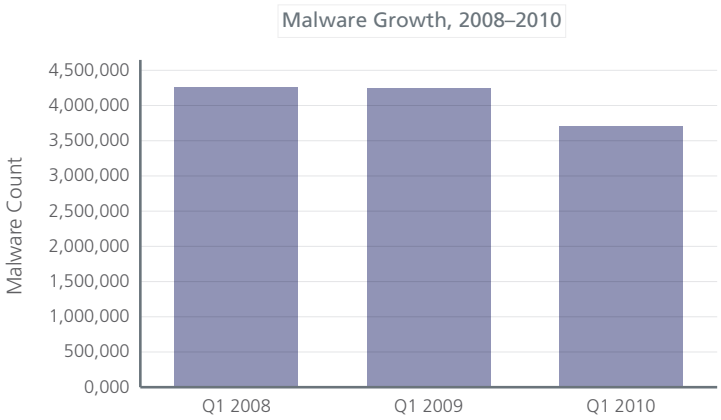


Figure 4: A comparison of malware growth in the first quarter of the last three years shows a slight decline in the first three months of 2010.

In other major areas of malware we also see this leveling-off trend. Bear in mind these numbers are incremental, meaning they represent new malware that we record each quarter. The need to stay protected and vigilant remains unchanged. Any way you look at it, three million pieces, just shy of 40,000 pieces daily, is still a lot of malware.

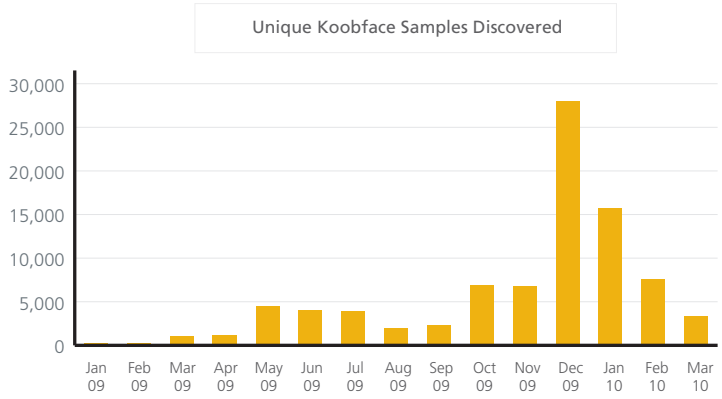


Figure 5: New Koobface variants have declined rapidly since peaking in December, but the malware continues to plague Facebook users.

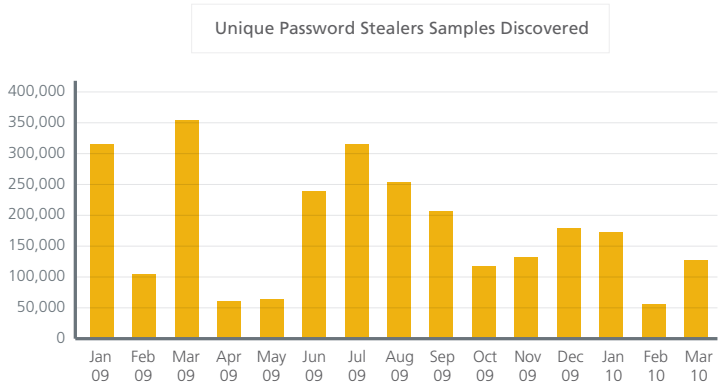


Figure 6: Password-stealing Trojans primarily target victims' bank accounts information.

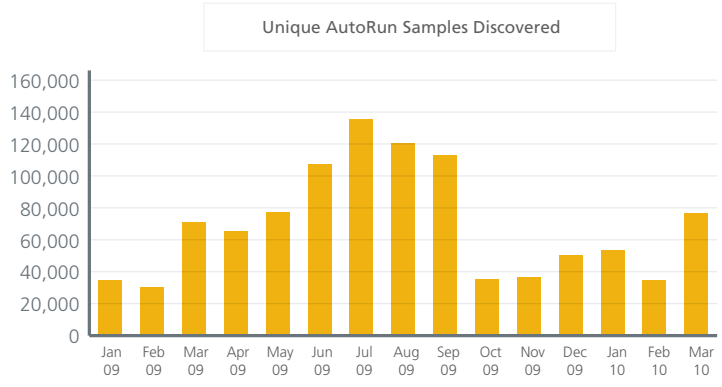


Figure 7: One of the most active categories of malware this quarter was AutoRun worms (malware found on removable storage, mainly USB drives). Due to the widespread adoption of USB drives by both consumer and enterprise users around the world, this infection vector continues to be a leading source of pain.

Let's take a moment to look at the most "popular" malware. The following list shows the leading reported consumer detections of malware worldwide. (Often this list varies in different parts of the world, but this quarter all the geographies we track reported the same top threats.)

Worldwide Top 5 Malware

1. Generic! Atr: Generic removable-device malware
2. Generic.dx: Generic downloaders and Trojans
3. W32/Conficker.worm!inf: Removable-device Conficker worm detection
4. Generic PUP: General-purpose potentially unwanted programs
5. GameVance: Online gaming software that collects stats anonymously

This Top 5 is very much in line with results from previous quarters. Two of the Top 5 are AutoRun malware (even one with Conficker), while others are for a variety of password-stealing Trojans. Often we detect fake security products generically as PUPs, and Internet Explorer is always a favorite target of cybercriminals, which leads us to Operation Aurora.

Operation Aurora

One of the most talked about attacks this quarter was Operation Aurora. Though it actually took place in late 2009, we now consider Operation Aurora one of the most important targeted attacks in Internet history. Leveraging a zero-day vulnerability and exploit in Internet Explorer with highly customized malware and many layers of obfuscation, this attack precisely targeted more than 30 companies and their data. Aurora may have a significant impact for years to come on the perception of corporate-focused cybercrime.

For a detailed analysis of the attack, refer to the following McAfee blogs:

http://siblog.mcafee.com/cto/source-code-repositories-targeted-in-operation-aurora/

http://siblog.mcafee.com/cto/operation-%E2%80%9Caurora%E2%80%9D-hit-google-others/

http://www.avertlabs.com/research/blog/index.php/2010/01/14/more-details-on-operation-aurora/

http://www.avertlabs.com/research/blog/index.php/2010/01/15/operation-aurora-leading-to-other-threats/

http://www.avertlabs.com/research/blog/index.php/2010/01/18/an-insight-into-the-aurora-communication-protocol/

An excellent whitepaper offers insight on what we learned about Aurora and how we can prevent similar attacks from succeeding:

http://resources.mcafee.com/forms/Aurora_VDTRG_WP

Tax Scams, Phishes, and Websites

Tax-related messaging is always a popular lure for cybercriminals, growing in volume as tax season approaches. This year the IRS fun appeared to start early: We began to find and track tax-related scams, phish, and fake websites as early as late January. This year also has an international feel, as many of the scams and phish we see are faking overseas financial institutions.

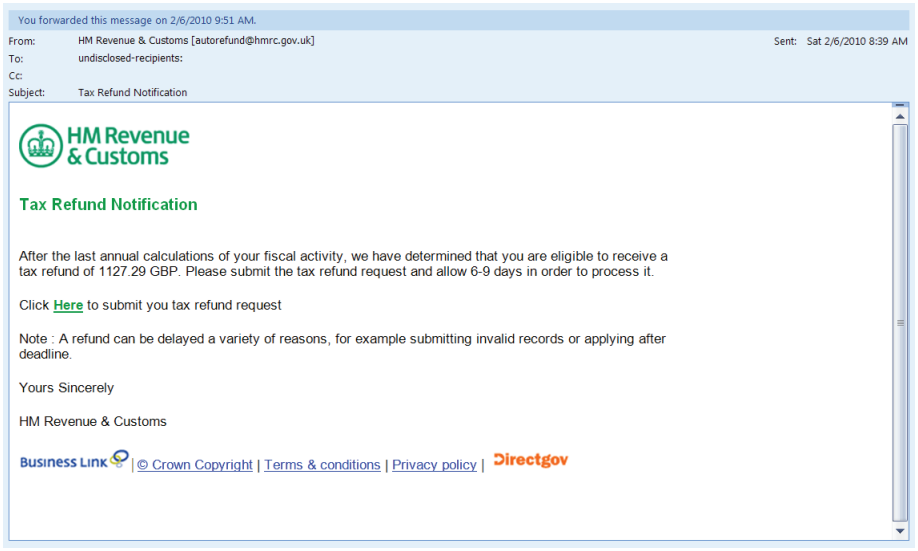


Figure 8: This HM Revenue & Customs fake has been very popular lately.

Unsuspecting users view the usual types of lures, although the come-ons are specific to the time of year: They are eligible for tax refunds if they would kindly submit the appropriate online paperwork. Of course, there is no real refund, just an opportunity for identity theft and financial losses.

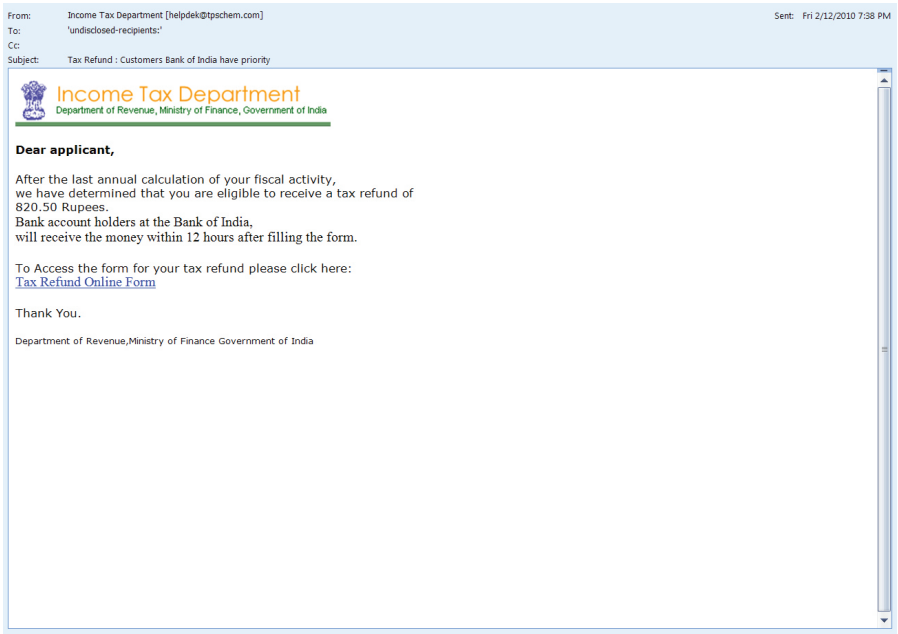


Figure 9: We have seen quite a few scams and spams pretending to be from The Bank of India.

As well as fake Internal Revenue Service websites:

Figure 10: This site was hosted on a Brazilian server, but we find these worldwide.

As of mid-February we had started to see a spike in these types of websites. Such sites claim to distribute tax forms and applications that assist with tax submissions. All are fakes and malicious.

Search Engine Manipulation Grows More Complex

McAfee Labs observed a noticeable uptick in the volume of search engine manipulation in 2009. Attackers took advantage of the page-ranking logic used by search providers to raise the positioning of links leading to malicious websites. As usual, cybercriminals went after the hottest terms and topics of the day, maximizing their potential to snare victims. During the first quarter of 2010 we saw the following most poisoned search topics:

- Haiti earthquake
- Chile earthquake/Hawaii tsunami warning
- Toyota recall
- Apple iPad
- 2010 NCAA bracket/March Madness
- Tiger Woods apology
- Shamu attack/Florida shark attack

- Luge tragedy
- Groundhog Day
- U.S. Health Care Reform Bill

Attackers commonly cross-link web pages with popular search terms extracted from RSS feeds such as Google Trends. We can often spot the manipulation when following a malicious link: Instead of seeing the content we would expect, we find a page containing nothing but a snippet of text and a bunch of links. Recently attackers have put their content in PDF documents to help fool victims.

Google will often crawl, index, and convert poisoned PDF documents to QuickView, opening the door to unwitting victims. The goal of such attacks is often to redirect users to a fake anti-virus software website, enticing users to purchase a bogus security product.

Figure 11: Once the "scan" is completed, the bogus product reports that it has found malware and gives victims the opportunity to purchase useless security software to remove the "infections."

Recently McAfee Labs has seen search engine manipulation leading to various forms of click fraud, and to network abuse. One example this quarter was a scam that leveraged the reputation of Digg to pull off the attack. When unsuspecting users followed the hyperlink on Digg, they saw the video in Figure 12.

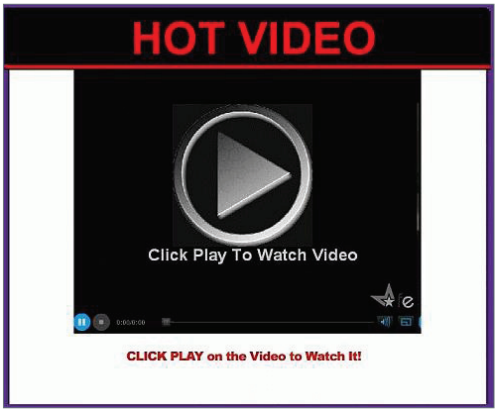


Figure 12: This example of Google click fraud took advantage of Digg to trap victims.

Behind the scenes of this "Hot Video" were some JavaScript and Google ads that could have paid ad revenue to the scam's creator if the victims were to click anywhere on the page. Other examples are more obvious: Browsers are redirected to another page of search results that, though similar to the originals, may yield the attacker some ad revenues.

Poisoned search spam has a long way to go before it will rival the amount of email spam, which accounts for approximately 90 percent of all email traffic, but the rise in search manipulation is worrisome.

Password Stealers and Fake Security Software Penetrate Social Networks

In our *2010 Threat Predictions*, published in December 2009, we anticipated that attacks on social networks by password-stealing Trojans and other malware would increase in 2010.[2] During the current quarter we have seen several examples of that prediction in action.

The Zeus family, which we usually observe as PWS-Zbot and Spy-Agent.bw, is the preeminent password-stealing Trojan malware. It specializes in capturing bank credentials. Zeus is just one of the key tools of cybercriminals, who often tie password stealers with other types of illegal online material. We see, for example, Zeus hosted on the same machines as child pornography, or being installed along with other families of Trojans, such as fake security software (also called fake-alert or fake-AV software).

In this quarter we saw all kind of goodies being installed with Zeus. And whom do you imagine was the prime target for these attacks? Facebook users.

Most assaults follow this pattern:

- The attackers launch a large scam campaign. In most of the cases we observed, they used a fake password-reset message to get their victims' attention, such as the following:
  - » "Because of the measures taken to provide safety to our clients, your password has been changed. You can find your new password in attached document."
- The attached document will usually contain a variant of the Bredolab or Pushdo Trojan.
- The Bredolab/Pushdo network works as an installer for the Zeus family and requires no user interaction. But that's not all. Because Bredolab/Pushdo is installed when the user opens the attachment, it can install and maintain Zeus as well as install any other Trojan that its controllers think will benefit them.
- The most common cases we observed this quarter were installations of fake security Trojans.

Why fake AV? It makes money for both the malware developers and their distributors. Most fake-alert Trojans operate by an affiliate program, with an intermediary making a small cut for each new installation of their software.

Facebook users suffered not only from Zeus and fake security attacks but also from new variants of the W32/Koobface worm. In March, more than 150 websites were discovered hosting malicious files in the folder .sys, which is hidden on Unix systems.

Some example of those websites:

brand[removed]b.dk/.sys/?getexe=p.exe

brand[removed]b.dk/.sys/?getexe=v2captcha21.exe

brand[removed]b.dk/.sys/?getexe=go.exe

alv[removed]n.dk/.sys/?getexe=pp.14.exe

alv[removed]n.dk/.sys/?getexe=v2prx.exe

car[removed]ort.com.au/.sys/?getexe=pp.14.exe

car[removed]ort.com.au/.sys/?getexe=fb.101.exe

2. The report is available in nine languages. http://www.mcafee.com/us/threat_center/white_paper.html

The files served by those compromised hosts were essentially Koobface malwares, but also included generic downloaders, host-file modifiers, password stealers, and others.

Malicious Domains Increase

Web threats were very active this quarter. McAfee Labs identified several trends: from servers supporting highly targeted attacks to the usual Koobface, Zeus, and phishing attempts employing cash cards, romantic schemes, IRS forms, and generic account information. We also noticed a significant increase in the number of companies labeled as spyware or adware firms that challenged these claims.

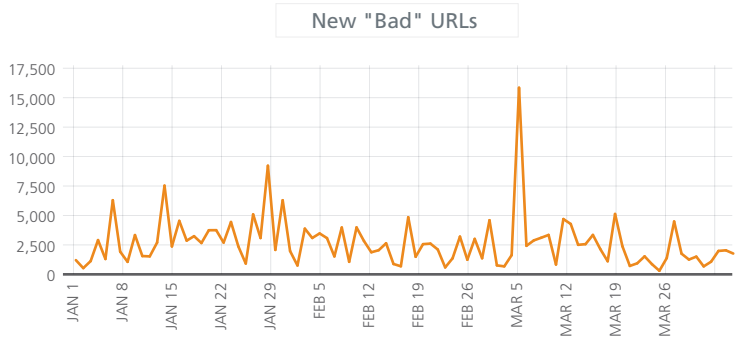


Figure 13: New websites with malicious reputations, reported daily by McAfee's TrustedSource Technology. This quarter we saw a return to more malicious-domain registrations, including a spike of more than 15,000 new bad sites in a single day.

Figure 13 illustrates the patterns of malicious activity that we identified. As a new exploit struck, or a new botnet was released, we saw a clear spike in the numbers of websites with malicious reputations. Within a day or two, however, the number of new bad sites would drop to customary levels. McAfee Labs has also seen a distinct increase in communications to and from malicious servers that control botnets. The vast majority of these servers show certain traits that our unique threat-vector cross-correlation can identify. The leap in bad URLs on March 2, for example, was preceded by a distinctive spike in email threats on February 14.

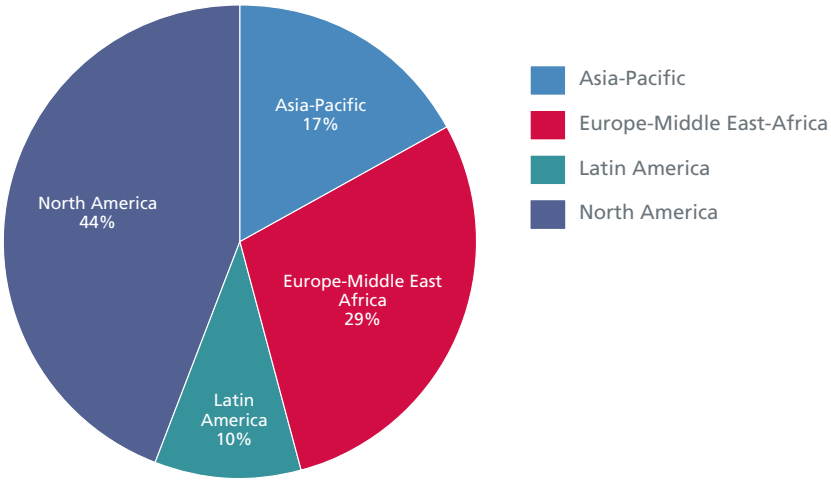


Figure 14: As usual, the majority of the servers hosting malicious web content are located in the United States.

This U.S. centricity becomes even more significant when we look past servers to the location of malicious

URLs. Due in large part to the general Internet services that are essential to Web 2.0 and are abused en masse by malware distributers, 98 percent of the malicious URLs are hosted on a server within the United States. Within the remaining 2 percent, China hosted 61 percent and Canada hosted 34 percent.

One of the biggest increases we have seen in malicious URLs and websites is the rapidly growing Zeus family. Given Zeus' ease of use for and prevalence among cybercriminals, we have seen distinct shifts during the quarter to truly malicious servers using automated domain registration practices and fast-flux IPs. Once we find one Zeus machine it is easy to find dozens more. One Zeus command server we identified yielded another 160 malicious domains carrying on everything from social networking and media sharing infections to IRS and other credential phishing.

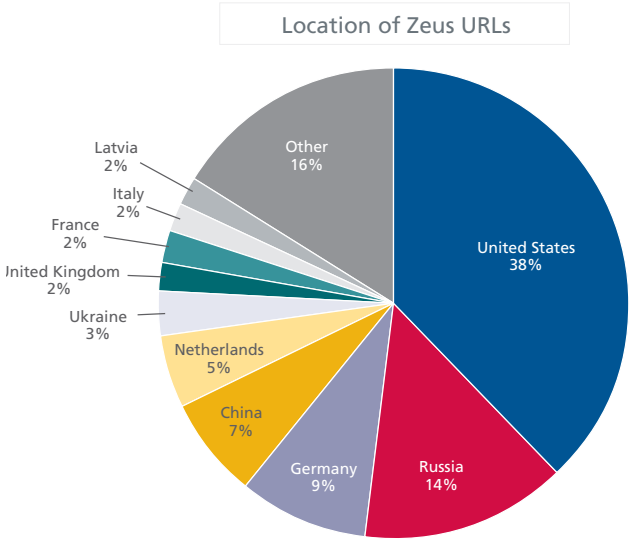


Figure 15: The Zeus URLs are found primarily in the United States, with around 40 percent in all of Europe.

Clients Under Attack

Client security issues continue to dominate the list of high-profile vulnerabilities this quarter. Our sensors recorded multiple attacks via the Secure Sockets Layer (SSL) communications protocol that emerged from the Pushdo botnet. We saw attempts to launch targeted denial-of-service assaults using SSL requests.

McAfee Labs witnessed multiple zero-day attacks during this quarter. Some of the most notable affected Microsoft Internet Explorer and Adobe Acrobat and Reader.

- *"Operation Aurora" MS10-002 HTML Object Memory Corruption Vulnerability*—CVE-2010-0249: On January 13, McAfee Labs confirmed a targeted zero-day exploitation of a previously unknown vulnerability in Internet Explorer and notified Microsoft, which confirmed the issue and released an advisory the next day.[3] Metasploit released a working exploit one day later. Due to the ensuing widespread exploitation of this vulnerability, Microsoft released an out-of-band patch on January 21. Our live sensors still see multiple attempts to exploit this issue.
- *Internet Explorer Dynamic OBJECT tag and URLMON sniffing vulnerabilities*—CVE-2010-0255: On February 3, a group of researchers presented two vulnerabilities in Internet Explorer at the Black Hat DC 2010 conference. The issues received further discussion on the Core Security website. The vulnerabilities lead to cross-domain information disclosure, which can allow an attacker to access sensitive files that can later be used to launch targeted attacks. These issues remain unpatched at the time of writing this report.

3. http://www.microsoft.com/technet/security/advisory/979352.mspx

- *Adobe Acrobat and Reader Remote Code Execution Vulnerability*—CVE-2010-0188: On February 16, Adobe patched a critical vulnerability in Reader that could lead to remote code execution. McAfee Labs has come across malware samples that are actively exploiting this issue in the wild. Acrobat and Reader users should update with these patches.[4]
- *Uninitialized Memory Corruption Vulnerability*—CVE-2010-0806: On March 9, Microsoft reported the exploitation of a previously unknown vulnerability affecting Internet Explorer Versions 5, 6, and 7. (Internet Explorer 8 is not affected.) Internet Explorer users are advised to update with the out-of-band patch released on March 30.[5]

Cross-Site Scripting Opens the Door

Our live sensors caught multiple attempts of script-injection attempts this quarter. We have divided this data into some broad categories for the attacks that we witnessed over HTTP.

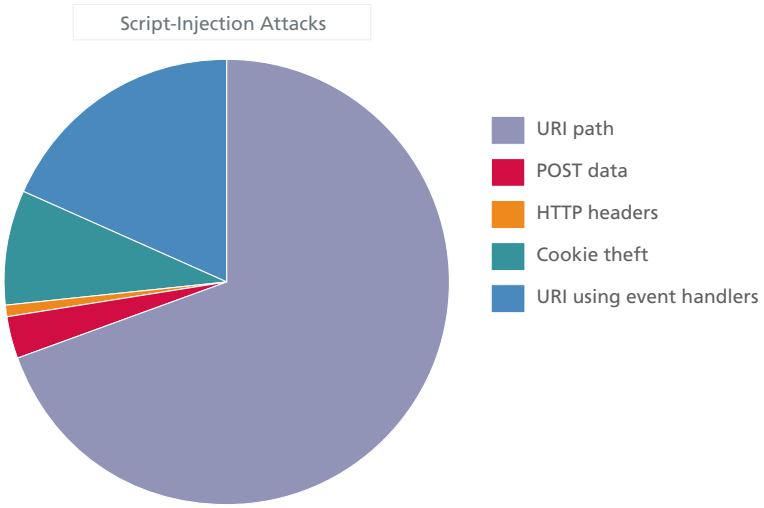


Figure 16: Cross-site scripting attacks using HTTP, by category.

Cybercrime Justice

DarkMarket: Devilman and JiLsi plead guilty

Between 2006 and 2008, DarkMarket was one of the busiest underground forums in the carding field, which steals credit and debit card numbers and sells them for profit. Although entry into DarkMarket was only by invitation, it boasted more than 2,000 registered users.

The forum was infiltrated by the FBI and closed down in October 2008. With help from other police organizations, the FBI made more than 50 arrests in the United States, United Kingdom, Turkey, and Germany. Among those arrested were Cagatay Evyapan (a.k.a. Chao, in Turkey), Mert Ortac (Kier, Turkey), and Markus Kellerer (Matrix001, Germany).

This quarter, two eminent DarkMarket members pleaded guilty at the Blackfriars Crown Court in London for their activities. They face a maximum sentence of 10 years.

The first was Renukanth Subramaniam, known as "JiLsi." This 33-year-old Sri Lankan was a website administrator and one of the earliest forum members.[6] The second was John McHugh. Aged 69, "Devilman" was a reviewer. One of his jobs was to verify the compromised credit cards that new subscribers supplied to the board to be accepted as members. [7]

4. http://www.adobe.com/support/security/bulletins/apsb10-07.html
5. http://www.microsoft.com/technet/security/Bulletin/MS10-018.mspx
6. "Pizza delivery man cops to life in DarkMarket," The Register. http://www.theregister.co.uk/2010/01/14/darkmarket_fraudster_guilty_plea/
7. "OAP internet fraud expert," The Star. http://www.thestar.co.uk/doncaster/OAP-internet-fraud-expert.5985536.jp

Wiseguys Botnet

We frequently read that spammers circumvent CAPTCHA (Completely Automated Public Turing test to tell Computers and Humans Apart) authentication. Using bot-infected machines, they can create a vast number of random email accounts for spamming.

In February, a U.S. federal judge in Newark, New Jersey, revealed the latest use of a botnet-supported CAPTCHA breaker. In this case, the computers operated by the defendants were used for buying seats to high-profile concerts and sports events from legitimate ticket sellers' websites. The botnet operators later resold the tickets online at inflated prices.

According to the indictment, the distributed software was developed by programmers in Bulgaria. The application defeated security measures designed to limit individual ticket purchases and snatched up the best seats. Unlike botnets we frequently encounter, this one was set up on dedicated computers designed for that purpose. This network purchased more than 1.5 million premium tickets to events from late 2002 to about January 2009, making a profit estimated at $28.9 million.

The employees, contractors, and defendants behind this rip-off are known as the Wiseguys, based on the name of the Nevada corporation they created (Wiseguy Tickets, Inc.). The Wiseguys botnet was a nationwide network of computers that purchased thousands of tickets per minute. The network had an impressive feature list:

- Monitored the online ticket vendors' websites for the exact moment that tickets to popular events went on sale
- Opened thousands of connections at the instant that tickets went on sale
- Defeated the CAPTCHA challenge in a fraction of a second (a human needs five to 10 seconds), thus racing past legitimate buyers
- Supervised by the Wiseguys' employees, it prepared lists of hundreds of the best tickets almost instantly
- Filled in all the fields necessary to complete the purchases, including customer credit card information and false email addresses

Figure 17: A fraudulent online offer made by Wiseguy Tickets. (Source: McAfee)

The indictment explains how the Wiseguys took advantage of many popular events, including the BCS Football Championship Game, a Barbara Streisand concert in Chicago, Hannah Montana concerts in New Jersey, and the 2008 Bruce Springsteen Tour.[8] For this last event, the botnet was purchased approximately 11,800 tickets.

8. "United States of America v. Kenneth Lowson et al.," US District Court, District of New Jersey. http://media.nj.com/ledgerupdates_impact/other/Wiseguys%20Indictment%20-%20Filed.pdf

One of their last crimes occurred in January 2009, when the botnet impersonated 1,000 individual ticket buyers for the New York Giants vs. Philadelphia Eagles NFL playoff game at Giants Stadium in East Rutherford, New Jersey.

Operation Bottom Dollar

This quarter, the U.S. Federal Trade Commission filed seven cases against work-at-home and job-placement scammers.[9] In the legal actions announced in February, the FTC charged seven institutions. This brings to 11 the number of cases the agency has brought in the last 12 months.

One of the accused, Real Wealth Inc., victimized more than 100,000 people by selling them booklets that supposedly explained how they could earn money by applying for government grants and working from home mailing postcards and envelopes, according to the FTC complaint. Using direct mail campaigns that sometimes targeted the elderly and disabled, Real Wealth lured consumers with deceptive solicitations such as "Collect up to $9,250 with my simple 3 minute form" or "All I do is mail 30 postcards everyday and I make an extra $350 a week!" Real Wealth also claimed that consumers could "rake in up to $1,500+ per week or more in solid cash" by learning "secrets" about the "$700 billion banking industry bailout."

In another complaint, Darling Angel Pin Creations claimed in Internet advertisements that by purchasing a starter kit, consumers could earn up to $500 per week assembling angel pins.

Mariposa Botnet

In February the Spanish Civil Guard arrested several people from a criminal gang operating the Mariposa botnet. First appearing in May 2009, the various malware behind this botnet had hijacked more than 13 million PCs in 190 countries.[10] Shut down in December 2009, it was designed to steal credit card data, online banking passwords, account information for social networking sites, and other sensitive data. It spread via peer-to-peer networks, infected USB drives, and MSN links that directed surfers to infected websites. Once it found a victim, the Mariposa bot client would install various strains of malware (advanced keyloggers, banking Trojans including Zeus, remote access Trojans, and others) to obtain greater control of the compromised systems.

The criminal gang called themselves the DDP Team (for *días de pesadilla*, or nightmare days). We found this reference in some WHOIS queries linked to websites these criminals created to spread their malware.

Cybercrime Attacks

In March, McAfee warned consumers that "scareware"—fake security or fake anti-virus software—may be the most costly online scam in 2010, causing significant monetary losses and damage to users' computers.[11] In this section we'll give you some details and background about the figures we introduced in this announcement.

At McAfee, we use the label Fake Alert to cover this Trojan family, which includes scareware, rogue anti-virus programs, and other examples. As we can see in Figure 18, this category of malware exploded in 2009. During the current quarter, from March 1 to March 10 alone, 45,000 new samples entered our malware collection. (Samples comprise all types of malware related to scareware: downloaders, droppers, scripts, installers, and the many files that make up each product.)

9. "FTC Cracks Down on Con Artists Who Target Jobless Americans," Federal Trade Commission. http://www.ftc.gov/opa/2010/02/bottomdollar.shtm
10. "How FBI, Police Busted Massive Botnet," Hacking Expose. http://hackingexpose.blogspot.com/2010/03/how-fbi-police-busted-massive-botnet.html
11. "McAfee, Inc. Unveils New Consumer Threat Alert Program: A Warning for Consumers about the Most Dangerous Online Threats," McAfee. http://newsroom.mcafee.com/article_display.cfm?article_id=3631

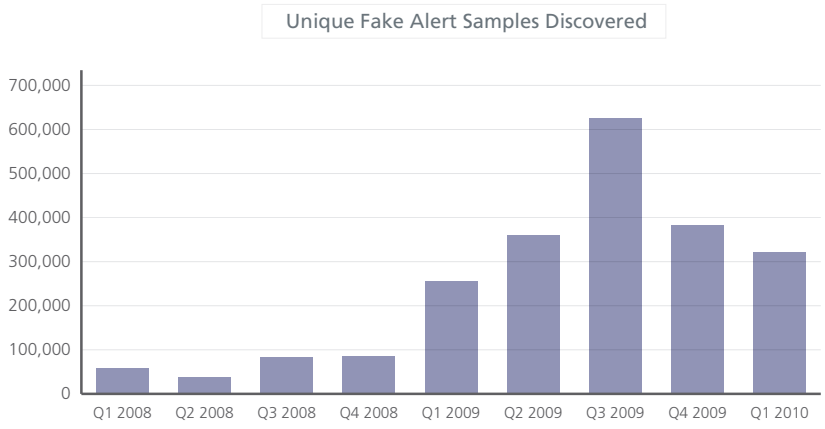


Figure 18: Fake security software samples peaked in the third quarter of 2009, but the overall numbers remain high for this lucrative form of cybercrime.

Between January 2004 and December 2009, McAfee Labs detected more than 3,000 scareware products. Many of these have a short lifecycle (perhaps weeks or months), but others, created as far back as 2004, are still available on the web. For half of them, we know the year they appeared. More than 170 have appeared this quarter.

For many products, only the name changes. This trick maximizes the chances of catching victims and reduces the amount of work for the developers. The scareware companies create numerous websites with a single fake offer repeated under various names.

Figure 19: Fake-alert software often have a consistent look yet change the product names to fool victims.

We see thousands of fake-alert products, yet we have found only a small number of scareware companies, perhaps 30 to 50. The developers create many subsidiaries and work with affiliates to help cover their tracks and increase sales. During our analysis of 2,000 products, we were able to name the company in each case.

Often scareware companies work openly; some are not afraid to create LinkedIn profiles, for example. When the pressure gets too great, they can simply start a "new" business. To multiply sales, scareware companies hire affiliates and promise them high commissions, up to 75 percent of the sales price.

A security colleague watched—for six months—the production servers of one of the main scareware companies. In just 10 days, he counted 4 million downloads (that is, 4 million scareware infections). This was only one company, and some victims made more than one download in a day. Extrapolating this figure, we can estimate that perhaps one million people worldwide fell victim to scareware scams each day.[12]

Not all downloads are intentional. Yet in 11 months, this scareware company received more than 4.5 million orders—actual user requests. Using this figure, we can assume this firm had annual revenues greater than US$180 million.

But that's not all: These companies sell more than scareware. They offer many other fake products (multimedia software, fitness software, family software, etc.). And above all, they peddle pornography. Consequently, their revenues are greater still.

Hacktivism

In addition to cybercrime, we see attacks motivated by politics. In January, the Belarusian human rights association Charter97 was once again under assault. Distributed denial-of-service campaigns have often struck this news and opposition website in recent months.[13] In January, Russia's *Novaya Gezeta* website was paralyzed for a week by a sustained attack from hackers.[14] "It was not amateurs, not hooligans [who] did this," said *Novaya Gazeta*'s Andrei Lipsky. "It is a deliberate act. We can only guess who stands behind this."

In February, a hacker cracked the Electronic Declaration System database of the Latvian revenue service.[15] A group calling themselves the Fourth Awakening People's Army (4ATA) had accessed more than seven million documents from the tax authority. "The purpose of the group is to unmask those who gutted the country," an alleged hacker using the alias Neo told producers of the Latvian current affairs talk show Kas Notiek Latvija in an interview on the show's website. A worldwide group of hackers adopted the unoriginal moniker Anonymous and notably promulgated Project Chanology, an ongoing 2008 campaign of disruption against the Church of Scientology.[16] In February this year, the group launched denial-of-service attacks against Australian government websites. Calling their protest Operation Titstorm, they opposed a government proposal to filter internet content and to block access to sites featuring extreme sexual content. Their targets included the Australian Communications Department, which is piloting the controversial plans, and Prime Minister Kevin Rudd's home page (defaced with pornography).[17] Hackers also attacked a website belonging to the Australian Communications and Media Authority.

12. Panorama de la Cybercriminalité–Année 2009, Club de la Sécurité de l'Information Français. http://www.clusif.asso.fr/fr/infos/event/#conf100113
13. "DDoS attack on charter97.org," Charter97. http://ww.charter97.org/en/news/2010/1/29/25857/?1
14. "Russia's Novaya Gazeta Web Site Hacked, Paralyzed," NBC4i. http://www2.nbc4i.com/cmh/news/local/article/russias_novaya_gazeta_web_site_hacked_paralyzed/31084/
15. "Massive security breach suspected at Latvian tax office," Monsters and Critics News. http://www.monstersandcritics.com/news/europe/news/article_1533738.php/Massive-security-breach-suspected-at-Latvian-tax-office
16. "The Assclown Offensive: How to Enrage the Church of Scientology," Wired. http://www.wired.com/culture/culturereviews/magazine/17-10/mf_chanology
17. Kathy Marks, "Operation Titstorm—Hackers Declare War on Aussie," The New Zealand Herald. http://www.nzherald.co.nz/compute/news/article.cfm?c_id=1501832&objectid=10625493

Figure 20: Hackers distributed this flyer to recruit participants for an operation opposing Internet censorship of sexual sites.

About the Authors

This report was written by Pedro Bueno, Paula Greve, Rahul Kashyap, David Marcus, Sam Masiello, François Paget, Craig Schmugar, and Adam Wosotowsky of McAfee Labs.

About McAfee Labs™

McAfee Labs is the global research team of McAfee, Inc. With the only research organization devoted to all threat vectors—malware, web, email, network, and vulnerabilities—McAfee Labs gathers intelligence from its millions of sensors and its cloud-based reputation technologies such as Artemis and TrustedSource. McAfee Labs team of 350 multidisciplinary researchers in 30 countries follows the complete range of threats in real time, identifying application vulnerabilities, analyzing and correlating risks, and enabling instant remediation to protect enterprises and the public.

About McAfee, Inc.

McAfee, Inc., headquartered in Santa Clara, California, is the world's largest dedicated security technology company. McAfee is relentlessly committed to tackling the world's toughest security challenges. The company delivers proactive and proven solutions and services that help secure systems and networks around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by an award-winning research team, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. www.mcafee.com.

McAfee, Inc.
3965 Freedom Circle
Santa Clara, CA 95054
888 847 8766
www.mcafee.com