Report

McAfee Threats Report: Second Quarter 2010

By McAfee® Labs™

Looking at changes over time in the computer threats landscape is always informative. This edition of the *McAfee Threats Report* examines the second quarter of 2010 and finds some very different results compared with previous quarters. Last quarter we saw a leveling off in some threat vectors while in others we saw some new developments. This quarter we find malware has resumed its usual rapid growth while the increase in spam has slowed. We see some very interesting geographical breakdowns for spam and botnets that we have not seen before. More threats have become specific and unique to those victims, both corporate and consumer, in different parts of the world.

This quarter we also see the global breakdown of malware to be quite different from that of previous quarters. From January to March we found the top malware to be the same around the world, a phenomenon we had not observed previously; but this quarter's breakdown shows specific threats tend to plague specific regions. We look very closely at growth trends for fake-alert software, password-stealing Trojans, social networking malware such as Koobface, as well as malware that abuses USB and other storage devices.

We examine event and keyword abuse through search engines as well as which vulnerabilities were most frequently exploited throughout the quarter. It should come as no surprise that events such as the FIFA World Cup in South Africa and incidents in the Middle East were highly abused by both cybercriminals and political hacktivists. Remember: the bad guys read the same news as we do. We report on web and network threats such as phishing and malicious website growth and see what parts of the world are engaging in the most SQL-injection attacks.

We finish with an overview of the quarter's most interesting incidents in both cybercrime and hactivism. We hope you find this edition of the *McAfee Threats Report* instructive.

Table of Contents

Same Old Spam

Daily spam volumes this quarter showed only a 2.5 percent increase when compared with the first quarter and a 7 percent increase when compared with the fourth quarter of 2009. Spam traffic in this period accounted for 88 percent of all email traffic on the Internet, down only slightly from the prior quarter. (See Figure 1.)

Overall, spam appears to again be on an upward trend, albeit a slow one, after its 20 percent drop between the third and fourth quarters of 2009. That third quarter was also the highest spam volume quarter on record—with almost 175 billion messages per day. Current volumes are similar to those we saw in mid-2008, right before major spam purveyor McColo was shut down in November of that year.

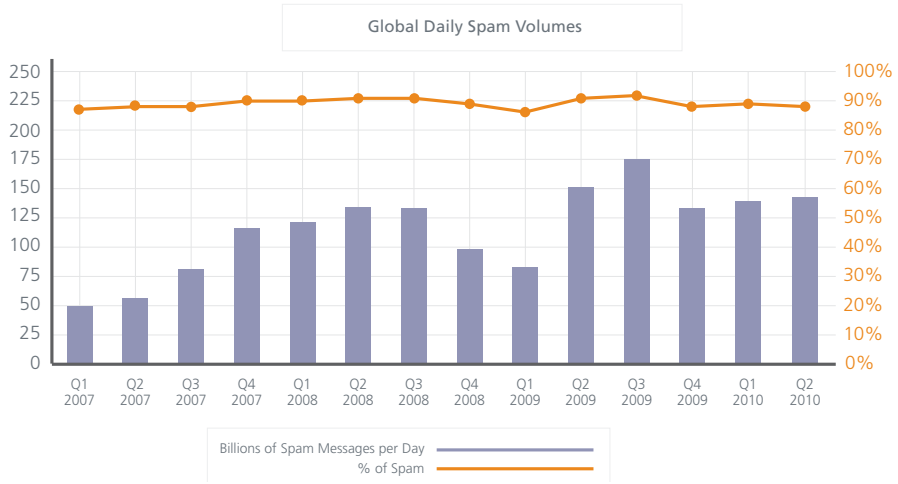


Figure 1: Global spam volumes (blue bars) and spam as a percentage of all mail (orange line). In this quarter McAfee Labs recorded a daily average of 142 billion spam messages.

Health and pill-related messages pointing to "Canadian pharmacy" sites continue to dominate the types of spam that are being sent from infected computers. During this quarter health-related email accounted for 63 percent of spam messages, leaps and bounds ahead of messages with generic offers, which accounted for a measly 10 percent of spam. Phishing emails, the third-most prevalent type of spam during this period, accounted for just 2 percent. As a percentage of overall spam volume, however, phishing is up 81 percent over the past year.

World Cup fever leads to infections

As the anticipation and tension built up among soccer fans for the FIFA World Cup in South Africa, cybercriminals anticipated their own celebration. Theirs, however, was of a different character. They were looking for ways to leverage the world's most popular sporting event to steal and inject malicious code onto PCs. Every major event—a tragedy, product release, sports, or other popular activity—always attracts a fair share of scams and search-engine "poisoning." Even so, the worldwide attention to this year's World Cup seemed to produce more than usual.

Brazilian soccer fans, which is to say all Brazilians, saw an attack that used the national soccer team's (now former) coach, Dunga, as bait. Users were advised to click a button to see photos of a fight between Dunga and two angry fans. The download was in fact malware, which we call PWS-Banker.dldr, a password-stealing Trojan that downloads additional malware.

One of the methods that criminals employed to trick victims out of personal information was a phishing scam that appeared to be affiliated with the World Cup organizers. The scam included an official-looking logo and several mentions of FIFA and the World Cup tournament throughout the message. This particular phish was different from most that we see because it did not immediately ask for credit card numbers, CVV codes, or PINs—a hallmark of many phishing scams. Instead, this phish asked for occupation, company name, email address, and mobile number. This may not seem like sensitive information at first glance, but once in the wrong hands it can be used to send spam, additional phish, or malware to mobile devices—as well as send targeted phishing or malicious emails to victims' inboxes.

We also saw criminals using the World Cup in a highly targeted attack that exploited a PDF zero-day vulnerability. (This one could easily recur, using the information provided by people victimized in the previous scam.) This attack dropped a malicious backdoor Trojan that turns computers into spam- or malware-sending zombies. Victims of this Trojan would not even know that their computers were compromised because the exploit occurred in the background while users viewed pictures of very enthusiastic fans.

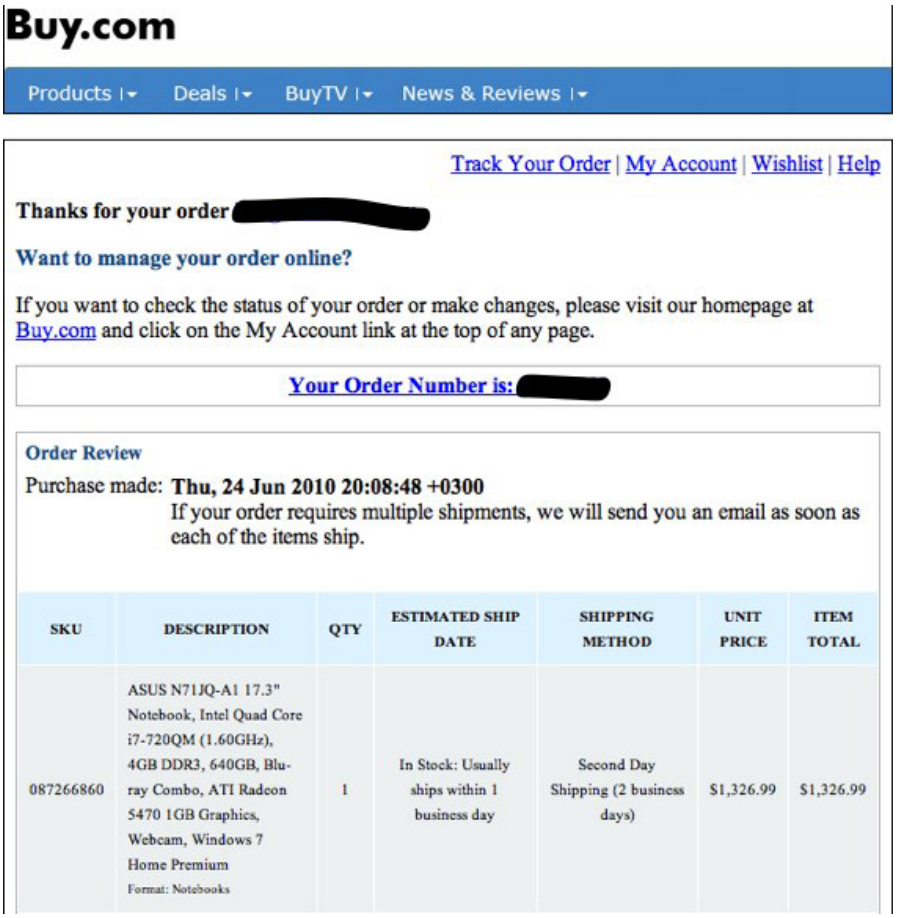
Attackers can "poison" search-engine results to present victims with bogus links to malicious sites. World Cup attacks included popular terms such as "Bafana Bafana" (the nickname of the South African team) and "best place to listen live World Cup." Every time users clicked those results, the victims ended up at a site with fake anti-virus software.

Many attacks are carried out in multiple stages. For example, an email with a link to a phishing site may first redirect victims through a URL that attempts to exploit an unpatched vulnerability on their computers. Thus a user's machine might become infected even before a scam asks for personal information.

Did you buy that laptop?

Another scam we saw this quarter may have duped more than a few IT and purchasing managers. Their email contained an apparent receipt for a purchase made on a major retail website such as Amazon, eBay, or Buy.com. We saw quite a few retailers being spoofed as part of this campaign.

This scam was pretty well crafted and could easily pass as legitimate to those who fail to look closely. The links in the messages connected either to compromised legitimate websites that were unknowingly hosting malicious executables or to malicious sites.



Buy.com

Products | Deals | BuyTV | News & Reviews

Track Your Order | My Account | Wishlist | Help

Thanks for your order [redacted]

Want to manage your order online?

If you want to check the status of your order or make changes, please visit our homepage at Buy.com and click on the My Account link at the top of any page.

Your Order Number is: [redacted]

Order Review

Purchase made: **Thu, 24 Jun 2010 20:08:48 +0300**
If your order requires multiple shipments, we will send you an email as soon as each of the items ship.

SKU	DESCRIPTION	QTY	ESTIMATED SHIP DATE	SHIPPING METHOD	UNIT PRICE	ITEM TOTAL
087266860	ASUS N71JQ-A1 17.3" Notebook, Intel Quad Core i7-720QM (1.60GHz), 4GB DDR3, 640GB, Blu-ray Combo, ATI Radeon 5470 1GB Graphics, Webcam, Windows 7 Home Premium Format: Notebooks	1	In Stock: Usually ships within 1 business day	Second Day Shipping (2 business days)	$1,326.99	$1,326.99

Figure 2: Realistic-looking receipts attempt to fool buyers into clicking malicious links.

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 is 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.

Adult Products: Spam mails that advertise pornography, usually DVD movies or download sites.

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.

Credit: These promise money, credit, or seek to leverage themselves based on the credit-worthiness of the recipient.

Diplomas: Offering fake diploma sites, where clients can request forged documents that "prove" they have graduated from a certain school.

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.

Drugs: This category includes the faux Canadian pharmaceutical spams that are generally hosted in China, açai-berry spam, dietary supplements, etc.

Horoscopes: Offer lists of your personal horoscopes.

Jobs: Many are a form of 419 scam or confidence scam.

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.

Malware: Anything that comes with a virus or Trojan attachment or that urges you to visit an infected website.

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.

News: Spam that uses real news from legitimate news sites.

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.

Phishing: Any email that begins a process of extracting personal information from a victim.

Products: Any unsolicited spam mail that tries to sell manufactured goods (usually replica purses or jewelry).

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

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.

Travel: Mail associated with legitimate travel-industry marketing.

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

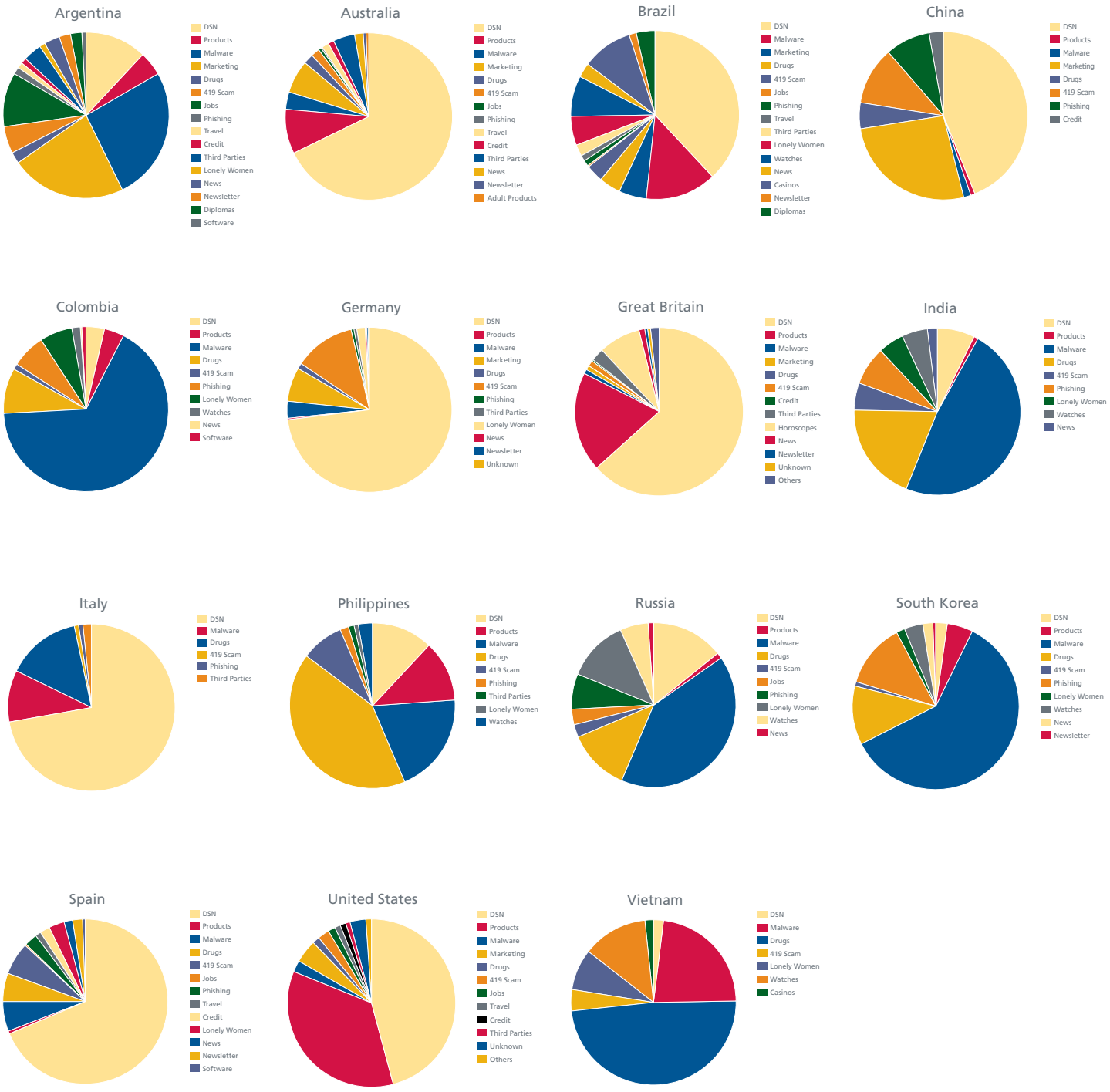


Figure 3: Spam subjects vary considerably among countries. These charts show the varying importance of the leading topics originating within each nation. These subjects do not represent all spam traffic, only the most popular.

No Surprises: Malware Shows Steady Growth

The malware landscape this quarter looks quite different than in previous quarters. Last time we saw a leveling off of overall malware and even some decline in the prevalence of certain malware types.

When we look at the broadest measure of malware numbers, we can clearly see that the slow growth in the first quarter has been replaced with more rapid growth in this quarter. (See Figure 4.) Malware developers are back in full swing. We have cataloged 10 million new pieces of malware in the first half of this year! During the same period last year we added 9 million, so the overall growth is still upward and significant. This makes the first six months of 2010 the most active half-year ever for total malware production.

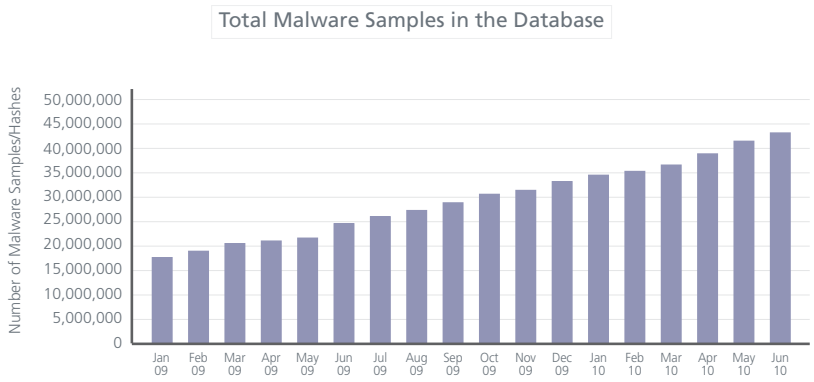


Figure 4: Total count of unique malware (including variants) in the McAfee Labs database.

Looking at some of the nastiest and most common types of malware for the quarter, we can see that AutoRun attacks (malware that uses USB or portable storage devices to spread) had a very busy April and May. (See Figure 5.) Meanwhile fake anti-virus software (malware that looks like legitimate security software but is a complete scam) has leveled off a bit. (See Figure 6.)

Given the huge user base of Facebook and its continued growth as the preeminent social networking site, it is no surprise that Koobface, Facebook-specific malware, continues to be one of the most prevalent threats we encounter. (See Figure 7.) Finally, the old standard and key money maker for cybercriminals globally—password-stealing Trojans—continues its unspectacular but steady rise in growth. (See Figure 8.)

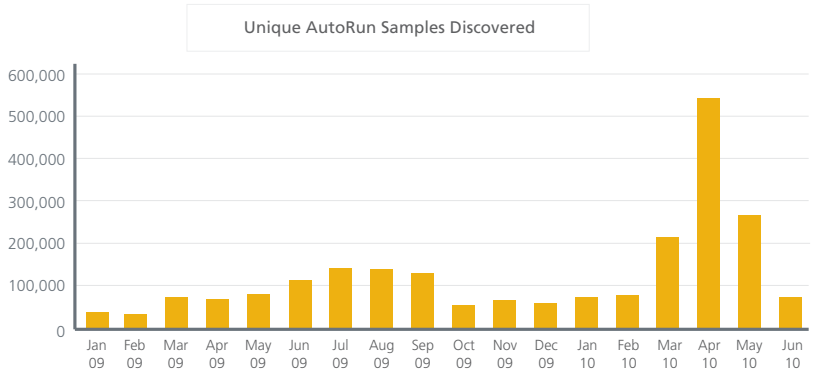


Figure 5: AutoRun worms were a very active category of malware during the quarter. They reached record numbers in April, and then fell rapidly to typical levels.

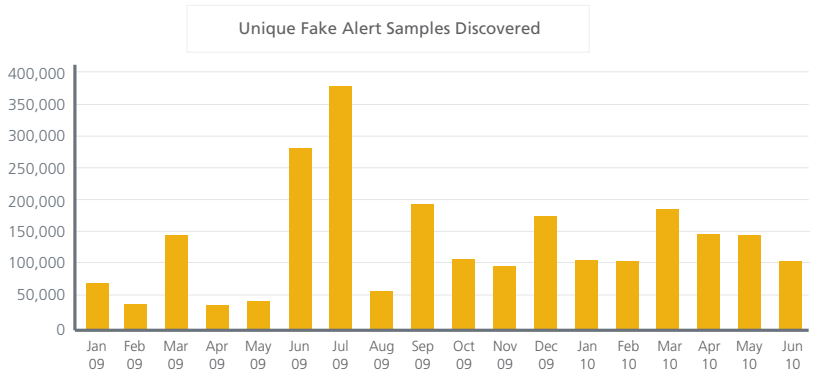


Figure 6: Fake security software samples peaked in the third quarter of 2009, but the overall numbers remain high for this lucrative form of cybercrime.

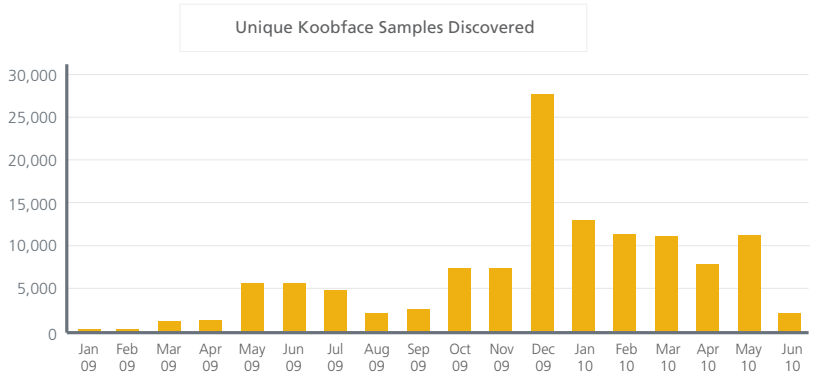


Figure 7: New Koobface variants dropped off sharply since peaking in December, but the malware continues to plague Facebook users.

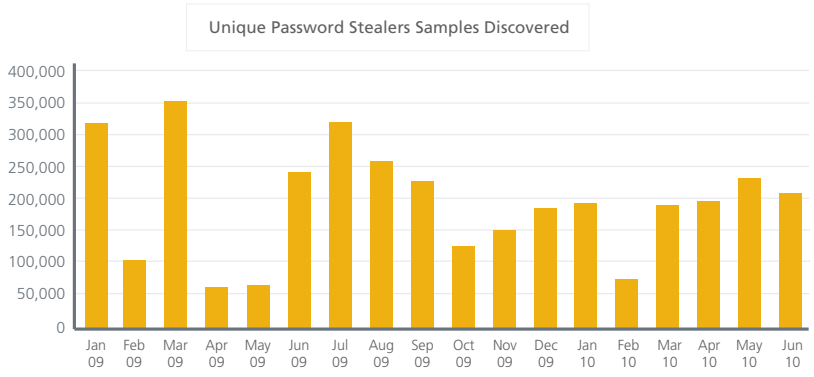


Figure 8: Password-stealing Trojans primarily target data in victims' bank accounts.

Changes in store for Mac users?

For a variety of reasons, malware has rarely been a problem for Mac users. But those days might end soon. In April, McAfee Labs detected the Mac-based Trojan OSX/HellRTS, which is remote-access malware with client, server, and server editor components. OSX/HellRTS has many of the same functions that a Windows Trojan has:

- Process Manager (list, kill running processes)
- File Manager (list, upload, download, delete files)
- Open a chat box and chat with the victim
- Play pranks on the victim (open and close CD drive, play videos/sounds)
- Read or modify contents of the clipboard
- Log off desktop, reboot, or shut down

We don't want to overstate this threat: We have not seen much activity with OSX/HellRTS and McAfee products detect and protect against it. But it serves as a reminder that in this age of cybercrime, data theft, and identity theft users of all operating systems and devices must take precautions.

Global and Regional Detections

The growth in the number of malware samples for which we add detection remains stable and at a fairly high level: Approximately 55,000 new pieces of malware appear every day. The fact that most of them are static and only slight variations of malware we've seen before—just obfuscated with different packers—helps us use generic detections to keep DAT (signature) sizes low. But it is still a lot of malware to handle.

Also most of these threats are in circulation for a very short time. The authors create them, do some quality assurance to make sure current anti-virus (AV) software doesn't detect them, and then distribute them via email, drive-by-downloads, or by tricking victims into downloading and executing them. The next day the authors go through these steps again, and the old malware never reappears. However, machines infected with them stay infected. To enjoy effective protection, consumers and businesses need near real-time detection—such as McAfee Artemis™ technology.

AutoRun still number one

The top detection continues to be the Generic!atr Trojan, which was reported on nearly 9 percent of machines scanned worldwide by McAfee. (We gather this data from users of our consumer products who choose to submit detection data to us. The information is available here: http://home.mcafee.com/VirusInfo/RegionalVirusInformation.aspx.) We strongly advise that you disable the AutoRun function unless you really need it.

Regional differences in malware

The most common detections are nearly the same for all regions of the world, but we do see some interesting differences in our Top 10s. (See Figure 9.) The worldwide Top 5, starting with Generic!atr, are AutoRun malware, a password-stealing Trojan, an AutoRun version of Conficker, potentially unwanted programs (PUPs), and a Java applet Trojan. In North America, FakeAlert, one of our detection names for fake anti-virus products and scareware, is much more prevalent than elsewhere. In Europe various generic detections for PUPs make it into the Top 10. Mostly they are fake AV products as well, but different from those in North America.

Worldwide Top 10 detections during June	% of scanned machines reporting
Generic!atr	8.9
Generic.dx	5.8
W32/Conficker.worm!inf	4.3
Generic PUP.x	3.2
Downloader-BCS	3.0
GameVance	2.8
FakeAlert-FakeSpy!env.a	2.1
Adware-BDSearch	1.9
Adware-WinAd	1.8
FakeAlert-FakeSpy.a	1.7

North America Top 10 detections during June	% of scanned machines reporting
Generic!atr	8.0
Generic.dx	4.1
GameVance	4.0
Downloader-BCS	3.6
W32/Conficker.worm!inf	3.2
Generic PUP.x	3.0
FakeAlert-FakeSpy!env.a	3.0
FakeAlert-FakeSpy.a	2.4
Adware-WinAd	2.3
Adware-HotBar.b	1.7

South America Top 10 detections during June	% of scanned machines reporting
Generic!atr	13.8
W32/Conficker.worm!inf	6.7
Generic.dx	5.8
W32/Autorun.worm.zf.gen	5.5
Downloader-BCS	5.4
Generic PWS.ak	3.0
W32/Conficker.worm.gen.a	2.6
Generic.dx!ssz	2.3
W32/Sality.gen	2.3
W32/Autorun.worm.ev	2.2

Europe Top 10 detections during June	% of scanned machines reporting
Generic!atr	9.7
Generic.dx	5.6
W32/Conficker.worm!inf	4.2
Generic PUP.x	3.7
Adware-Url.gen	2.9
Downloader-BCS	2.8
Generic PUP.x!dz	2.6
Generic PUP.x!dx	2.4
Adware-GameSpyArcade	2.3
Exploit-ByteVerify	2.1

Africa Top 10 detections during June	% of scanned machines reporting
Generic!atr	19.6
Generic.dx	11.9
W32/Sality.gen	7.4
PatchedSFC	5.1
W32/YahLover.worm.gen	5.1
Spyware-AdaEbook	4.9
Generic PUP.x	4.1
W32/Autorun.worm.ev	4.1
W32/Mabezat	3.8
W32/Fujacks.remnants	3.2

Asia Top 10 detections during June	% of scanned machines reporting
Generic.dx	12.7
Generic!atr	10.8
W32/Conficker.worm!inf	8.5
Adware-BDSearch	6.8
Generic Dropper!cqt	5.6
WebThunder	4.8
Generic PUP.x	3.8
Generic Downloader.ac	3.8
Spyware-AdaEbook	3.7
W32/Autorun.worm.bx	3.6

Australia Top 10 detections during June	% of scanned machines reporting
Generic!atr	10.5
Generic.dx	3.3
W32/GetCodec	3.2
W32/Conficker.worm!inf	2.9
Generic.dx!tal	2.9
Generic PUP.x	2.5
Adware-GameSpyArcade	2.1
CasOnline	2.1
FakeAlert-FakeSpy.a	1.9
Adware-Url.gen	1.8

Figure 9: Top 10 malware detections, globally and in regions of world.

Real viruses still exist and still cause problems. In South America and Africa, W32/Sality earns a place in the Top 10. On a global scale W32/Sality occupies the 19th spot, with 1.1 percent of machines reporting it. Sality is a family of polymorphic and very sophisticated viruses; an outbreak inside a network is bound to cause a lot of problems. With today's malware mostly Trojans, downloaders, and scareware, it is easy to forget that viruses are still dangerous.

Botnets make a comeback

This quarter we have also seen the comeback of two past threats: Storm Worm and Kraken. In April a new variant of Storm Worm botnet Trojans appeared. Although based on the original Trojan, this variant lacks some of the functionality—most notably peer-to-peer—that made Storm Worm so difficult to fight. After the initial noise, this Storm quickly dispersed. During the last days of June another botnet seemed to be resurrected from the dead. At its peak in 2008 Kraken was considered by some to be the biggest botnet on the planet; it certainly sent a lot of spam. The original was dismantled in 2009, but now a new botnet is on the rise. Whether this version will become as big a threat as the original remains to be seen. If it does, we'll certainly have more to say about it in the next *McAfee Threats Report*.

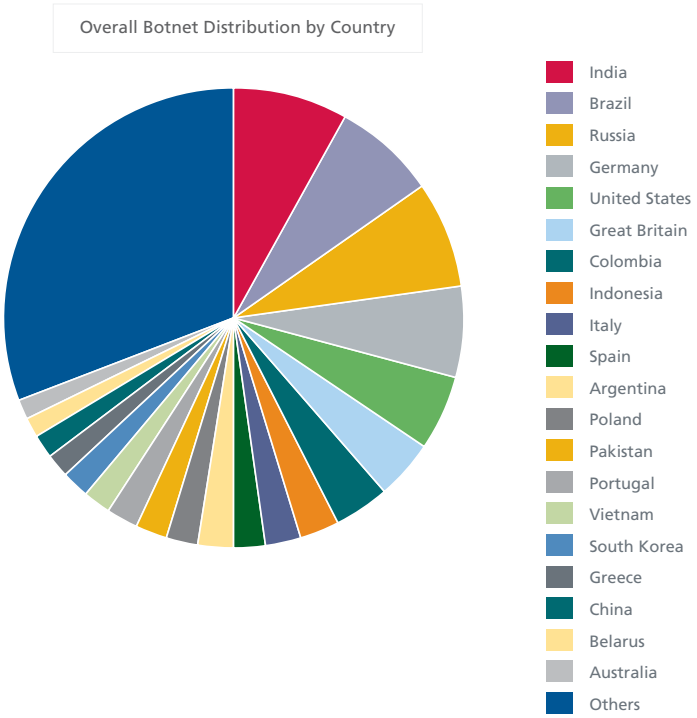


Figure 10: McAfee Labs has detected more botnet infections—almost 1.5 million—in India than in any other country. Brazil, Russia, and Germany also exceed one million infections.

Search Engine Patrol

Attackers continue to target the masses by keeping up with the hottest search terms. They regularly monitor Google Trends data to identify targets, weaving a web of cross-linked fabricated sites, and hacking vulnerable sites from which to launch their malicious payloads.

Figure 11: Top 50 poisoned search terms during the quarter

During this quarter, celebrity names often topped the charts as the most "poisoned" search terms. (See Figure 11.) Searching for the answer to "How old is Prince?" had the greatest likelihood of presenting malicious results. Following such a link might land you on a fake YouTube page, enticing users to download a file with a name such as download.exe or install.#####.exe—both examples of a downloader Trojan that attempts to install fake-alert software.

Searching for "ynn news rochester," "valmeticulous," "val meticulous," "justine musk," or 52 other top terms could bring you to the same fake site as well.

There's something odd about the terms *valmeticulous* and *val.meticulous*; they seem to be made up. We've already seen this phenomenon, in which very unusual words or phrases appear on the top terms list. In this case, followers of Google Trends noted the anomaly. At least one person went so far as to dream up a profile for a fictitious gal named Val. It's unclear how or why such terms appear on the list. Perhaps this is a sort of Google tracer, injected into the search-o-sphere as a means of flushing out those seeking to manipulate search results.

We were surprised to find the BP oil spill in the Gulf of Mexico was not present in the daily Top 20 search terms during this quarter.

Malware Sites Increase Dramatically

Last quarter we wrote about the high percentage of malicious URLs hosted within the United States. This discussion may have caused some confusion because we and others often report web risks at the domain level, yet concentrating on domains is no longer sufficient to understand these threats. Although there are definitely malicious servers and domains, we discover more and more path-level malicious URLs that are present within legitimate domains. Some of the instances include malware embedded in Wikipedia JPGs or Facebook profile pictures, malicious downloads posted on media-sharing sites or personal network storage sites, and malicious content stored within a forum or discussion board. The list goes on and on. In 2009, 6 percent of the malicious URLs that McAfee identified and protected our users from were at the path level. Already in 2010, that has increased to 16 percent. As registrars continue to work to keep their domains safe, we expect this trend to continue.

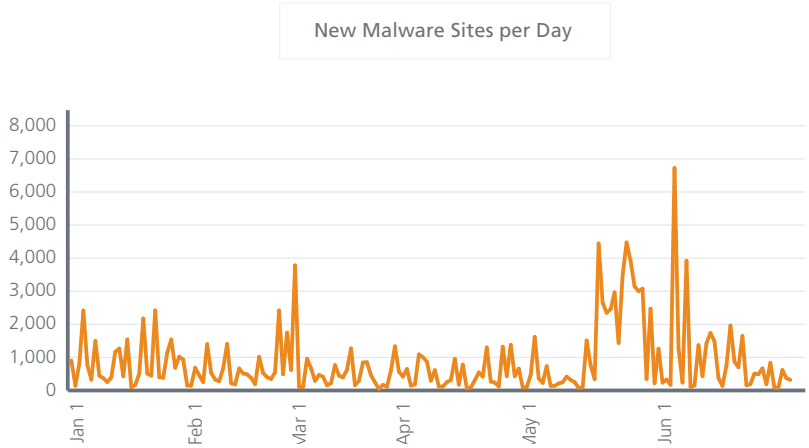


Figure 12: McAfee Labs sensors discover daily hundreds to thousands of new sites that host malware. Zeus and other botnet activity fueled the spike in late May and early June.

Figure 12 shows the trend in new malicious websites during the first half of the year. These sites distribute malware, serve exploits, update and coordinate botnets, proxy malicious traffic, or serve other malicious purposes. We saw a significant increase in the graph from May 13 to June 4. Our investigation found the extra numbers were due primarily to various ongoing targeted attacks and increased Zeus and other botnet activity. When we look at our chart of new phishing sites we notice a very similar pattern—but without the downturn. (See Figure 13.)

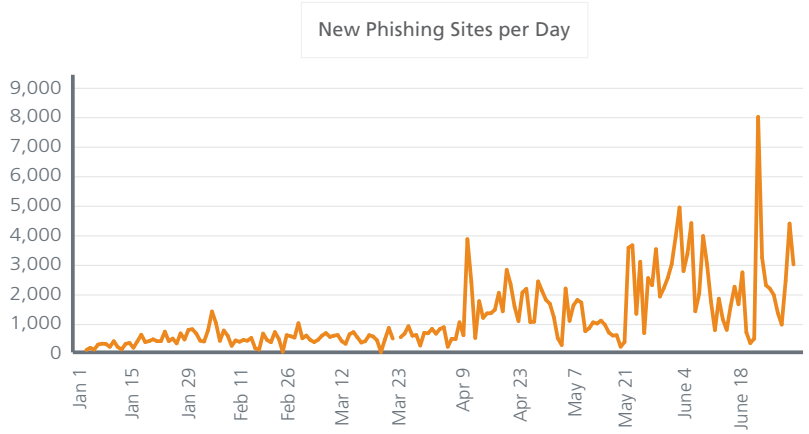


Figure 13: McAfee Labs count of new phishing sites closely followed that of new malware sites.

Our examination of new phishing sites turned up a similar spike to the one we saw among new malware sites. However, the phishing sites lagged a bit behind the latter. Many of these phishing sites appear to be generated with a very similar toolkit as malware sites use and to follow standard patterns. Attackers targeted a wide variety of brands and accounts during the most recent spike: The leading targets were PayPal, Bank of America, and Halifax Bank of the United Kingdom. But banks were not the only victims. Others included messenger and mail accounts, gaming accounts, pornography subscription accounts, gas cards, air and other travel planning services, online shopping accounts, and social networking and online interactive accounts.

One of the biggest news items from early June was a massive SQL-injection attack. A "spatter" attack

across tens of thousands of websites inserted an iframe that redirected users to a malicious page, which then downloaded and executed a file. These attacks happen periodically—at least once a quarter. Once the malicious domain is taken down, the news and concern over that particular attack fades into the background. But what we don't hear about are the number of sites that fail to clean up after such an attack. One month after the June attack, known as ww.robint.us, we counted 51,900 sites that were still infected with this SQL injection. This lack of house cleaning is not unique. The attack 2677.in still redirects users on 26,800 web pages, yahoosite.ru still impacts 1,380 sites, the killpp.cn exploit from 2008 is still present on 680 pages, and k.18xn.com plagues another 538 sites. These problems will likely become much worse as the dynamic and fluid nature of the web makes it easy to inject and hide attacks.

Another trend that was reported in the media this quarter was an increased number of malicious web attacks and threats that occurred on Fridays through Sundays. However, at McAfee Labs we have not seen this trend. We do find Friday is the busiest day for new threats to appear, but that trend is by no means new. What we have seen is a significant increase this quarter in the number of malicious websites regardless of the day they appear.

Busy Patches

The past three months constituted one of the largest "patch quarters" we've seen. Microsoft and Adobe, two of the largest software vendors, sent out huge updates. Adobe repaired 87 flaws listed in the Common Vulnerabilities and Exposures database, and Microsoft patched another 61 CVEs. Microsoft also released seven security advisories, six of which were issued in response to the public disclosure of problems in Windows and other applications.

Let's recap some of the most notable vulnerabilities analyzed by McAfee Labs this quarter:

- *Windows Help and Support Center—CVE-2010-1885:* This vulnerability affects Windows XP and Windows 2003. User interaction is required to successfully exploit this vulnerability on unpatched systems. The author published proof-of-concept code, which elevates the risk of this issue. This vulnerability was unpatched as we wrote this report. McAfee Labs urges readers to update their security software relating to this issue and implement stringent controls within their networks to disallow malicious usage of the HCP handler until the vendor issues a patch.
- *Adobe Flash Memory Corruption Vulnerability—CVE-2010-1297:* On June 4 Adobe acknowledged the exploitation of a critical vulnerability in Adobe Flash that could lead to remote code execution. Adobe released a patch on June 10 to solve this issue.[1] McAfee Labs is aware of malware that is actively exploiting this flaw.
- *PDF /Launch Attack—CVE-2010-1240:* On March 29 a security researcher demonstrated a way to run code by embedding an executable within a PDF and triggering the process via social engineering. This attack—which affects some versions of the PDF viewers Adobe Acrobat, Adobe Reader, and Foxit—was widely discussed. McAfee Labs is aware of in-the-wild exploitation. The attack on Foxit was slightly more severe, as no warning dialog appeared to give users a hint of suspicious activity. Both Adobe[2] and Foxit[3] have released patches.
- *Oracle Java Toolkit Insufficient Validation of Parameters—CVE-2010-0887:* In April a security researcher publicly disclosed details with proof-of-concept code that exploits a vulnerability in the Java virtual machine plug-in released in Java 6 Update 10. This flaw can be used to pass arbitrary parameters that can lead to code execution. Oracle released a security alert for this issue.

1. Adobe Systems. http://www.adobe.com/support/security/bulletins/apsb10-14.html
2. Adobe Systems. http://www.adobe.com/support/security/bulletins/apsb10-15.html
3. Foxit. http://www.foxitsoftware.com/pdf/reader/security_bulletins.php

SQL-injection attacks

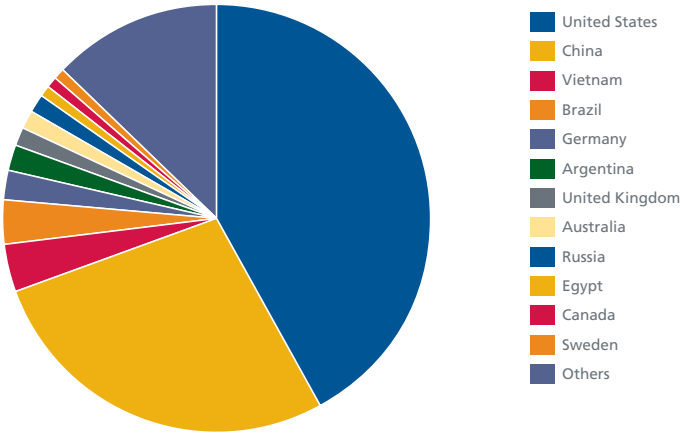


Figure 14: McAfee Labs sensors caught numerous attempts of clients attacking servers via SQL injection. The United States and China are the prime sources of these attacks.

Cybercrime

In April, the Romanian police announced the arrest of 70 members of three separate organized cybercrime groups. Since 2006 these groups have allegedly stolen funds from citizens of Spain, Italy, France, New Zealand, Denmark, Sweden, Germany, Austria, the United States, Canada, and Switzerland—primarily through online auction fraud. International authorities have identified more than 800 victims with more than €800,000 worth of losses.[4]

The criminals are said to have sold fictional electronic, luxury cars, yachts, villas, and even airplanes. Recent sales included a BMW X5, Lexus and Infiniti vehicles, and even a recreational aircraft that sold for €67,000 to a rich American.[5]

CallService closed

Later in April, the FBI announced the unsealing of an indictment against Dmitry M. Naskovets, the Belarusian creator and operator of CallService.biz.[6] This website allegedly assists identity thieves in exploiting stolen financial information, such as credit card and debit card numbers.

To help their Russian-speaking customers, Naskovets and his accomplices offered English and German speakers to conduct fraudulent transactions on their behalf.

CallService.biz managers posted advertisements for their services on other websites used by identity thieves, including CardingWorld.cc, which was operated by Sergey Semashko, a co-conspirator named in the indictment. The advertisements boasted that they had "over 2,090 people working with" it and had "done over 5,400 confirmation calls" to banks.

Naskovets was provisionally arrested by Czech law enforcement authorities on April 15, at the request of the United States and pursuant to bilateral treaties between the countries. Also that day, in a joint operation, Belarusian law enforcement authorities arrested Semashko in Belarus and Lithuanian authorities seized the computers on which the CallService and the CardingWorld.cc websites were hosted.

4. DIICOT. http://www.diicot.ro/index.php?option=com_content&view=article&id=298
5. Gandul. http://www.gandul.info/news/ce-vand-infractorii-romani-pe-internet-avioane-de-agrement-si-masini-de-lux-5825091
6. Federal Bureau of Investigation, New York. http://newyork.fbi.gov/dojpressrel/pressrel10/nyfo041910b.htm

Gang warfare

Carder.cc is a German online forum that helps criminals in trading stolen credit card and login details obtained via their carding or phishing activities. These forums are a major source of income for their administrators (who are involved in this black market), so the best-known platforms are forever engaged in underground infighting to stay above the rest. If a competitor can demonstrate another forum is insecure, the former will win market share.

Thus some individuals hacked the carder.cc forum and publicly posted the results of their hack—including information about thousands of forum members with, in many cases, their passwords. One interesting file is a RAR archive containing a dump of the forum and a tool allowing anyone to reconstitute it. This file contains data about the four administrators, their emails, and when they joined the group. The file includes the (real or anonymous) IP address used to reach the forum and function titles.

Besides the administrators, the file contains:

- 4,121 simple members
- Five global moderators
- 258 second-level members
- Seven third-level members
- Four moderators
- 17 verified vendors
- 497 banned members

The file includes age, nationality, and other personal data, though we can't be certain it is accurate. Websites, ICQ, AOL Messenger, Yahoo Messenger, and MSN contacts are also noted.

Figure 15: Exposed data for some carder.cc forum members.

Visiting carder.cc demonstrates that the identity theft market is thriving. The proof lies in the number of free payment accounts—used to attract customers—that contain the full identity of the victims.

Hacktivism

The recent Israeli attack against the Gaza Flotilla stirred various political hacktivist groups into action. Some hackers claiming to be Turks defaced Israeli domain sites such the Tel Aviv Municipality's. We frequently encountered a virtual protest message with a video shot by the news service Al Jazeera while on board the flotilla.

Turkish hackers also defaced several Facebook accounts owned by Israelis.[7] They sometimes replaced the original profile with the same message before posting their protest to a group. (See Figure 16.)

Figure 16: Turkish hacktivists defaced websites and Facebook accounts to protest Israel's action against the Gaza Flotilla.

Israeli hackers fired back. One infiltrated the site of Turkish charity and Mavi Marmara sponsor IHH.[8] The hacker replaced a large photo of the Marmara vessel with an image of an Israeli fighter jet and the caption: "Yes, we can."

The situation of Gilad Shalit, an Israeli soldier captured in June 2006 and still held by Hamas-led Gaza militants, has created side effects on the web. In April, Hamas released an animated cartoon portraying Noam Shalit, the solder's father.[9] In response to this broadcast, Israeli hackers defaced the Arabic, English, and French sites of the Lebanon National News Agency (NNA).[10]

Figure 17: The Gaza conflict has inspired political cartoons and defaced websites.

7. "Turkish Hackers Defacing Israeli Facebook Accounts," Dark Reading. http://www.darkreading.com/blog/archives/2010/06/facebook_accoun.html
8. "Israeli hacker hits IHH terrorist website: 'The real war today is online,' " JIDF. http://www.thejidf.org/2010/06/israeli-hacker-hits-ihh-terrorist.html
9. "Hamas Release Animated Gilad Shalit Cartoon," Sabbah Report. http://sabbah.biz/mt/archives/2010/04/26/hamas-release-animated-gilad-schalit-cartoon-video/
10. Lebanon news agency: Website hacked by Israel to post Ron Arad message: http://www.haaretz.com/news/diplomacy-defense/lebanon-news-agency-website-hacked-by-israel-to-post-ron-arad-message-1.285018

About the Authors

This report was written by Pedro Bueno, Toralv Dirro, 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 McAfee Artemis™ and McAfee TrustedSource™. The McAfee Labs team of 350 multidisciplinary researchers in 30 countries follows the complete range of threats in real time, identifying application vulnerabilities, analyzing and correlating risks, and enabling instant remediation to protect enterprises and the public.

About McAfee, Inc.

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

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

10104rpt_quarterly-threat-q2_0710_fnl_ETMG