Report

McAfee Threats Report: First Quarter 2011

By McAfee® Labs™

This edition of the McAfee Threats Report offers many of the elements of a good science fiction or cyberpunk novel: intriguing hacktivists and events, significant changes in the threats landscape, cybercrime arrests, clever new ways to compromise clever new devices, as well as the most active first quarter in malware history.

Some of the most significant changes this quarter revolve around botnets and threats to messaging and mobile devices. Globally we have seen a significant reduction in spam as well as a corresponding shift in botnets due to the Rustock botnet's being taken mostly offline. Although this is certainly good news, our research shows that many others are waiting in the wings to take its place.

Android has quickly become the third-most-targeted platform on the mobile front when viewed from a historical perspective. Malware threats to the mobile platform continue to evolve in sophistication and functionality at a pace that in many ways eclipses that of PC-based malware.

The fight against cybercrime continues to rage on, with several takedowns and arrests, while hacktivism appears to have entered a period of change. Recent activities in hacktivism continue to shape the technology and information security landscape.

Malware has just posted its busiest quarter in history. Fake anti-virus software seems to be on the rise again and password-stealing Trojans are demonstrating a consistent level of activity. At the same time, AutoRun malware and Koobface, though still prevalent globally, seem to be in a holding pattern. Our global Top 5 reflects this trend.

We noted consistent search-term abuse throughout the quarter, with 49 percent of the daily search terms in the top 100 results leading to a malicious website. Our quarterly word cloud reflects the trend of malware writers, scammers, and cybercriminals, who continue to use daily events, news, sports, and celebrities as bait for their schemes. The trend of client-side exploitation continues down a very Adobe-centric path and the top spot for SQL-injection attacks has once again flip-flopped. McAfee Labs also saw some interesting trends and activity in the growth of phishing websites and overall malicious websites.

Table of Contents

Malware Attracted to Android Phones 4

Botnet Takes a Fall 6

Malware Busier Than Ever 9

Password Stealers Take It to the Bank 11

PWS-Caberp 12

What’s in a Word? 13

Web Threats 14

Vulnerabilities and Network Attacks 17

SQL-Injection Attacks 18

Cybercrime 18

Hacktivism 21

Malware Attracted to Android Phones

The new frontier of malware and cybercrime may be mobile, but in many ways it looks very familiar.

During this quarter the Android was the second most popular environment for mobile malware, after Symbian OS. As the popularity of that platform continues to grow around the world, we expect to see more and more malware developed for it. Android malware remains third overall in our historical view, as shown in the pie chart on page 5.

McAfee Labs combats several developing families of malware that attack Android phones. One of the families, Android/DrdDream, comprises a variety of legitimate games and apps that have been injected with malicious code. These threats are unique and quite dangerous due to the use of two root exploits to gain greater control of those phones. The two exploits—Exploit/LVedu and Exploit/DiutesEx—were initially used by users trying to gain legitimate root access to their own devices, a process commonly referred to as rooting.[1] In the PC world, malware often uses exploits to enable drive-by downloads that infect machines visiting specially designed or compromised websites. For mobile devices, much of the malware has required user interaction, but in the near future mobile exploits will certainly allow automatic malware installation.

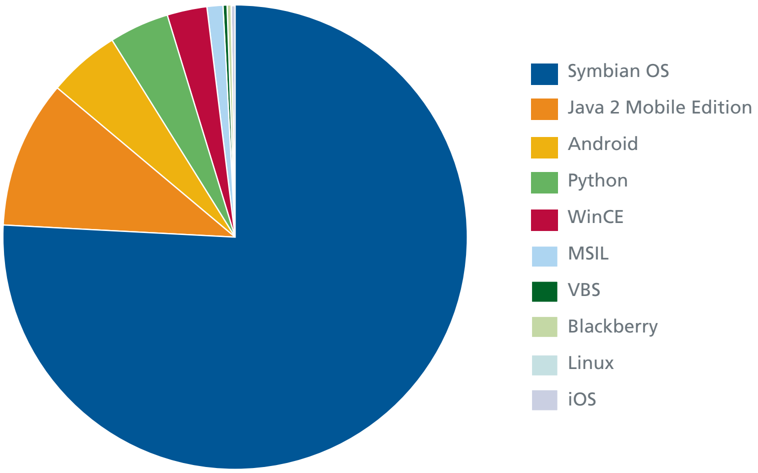
Like Android/DrdDream, the Android/Drad family is made up of maliciously modified applications. This family sends device information to an attacker-controlled site. Just like in the PC malware world, Android/Drad listens for commands from the attacker. The malware can also download additional software, though it stops short of being a full-fledged mobile botnet. It appears that the malware uses blackhat search-engine optimization techniques, a process of manipulating search engine results to place dangerous sites higher than they should appear in lists of hits.

The recently released Android/SteamyScr.A is a modified version of a novelty app that turns a phone's screen into a steamy window. This malware collects device information (International Mobile Equipment Identity and phone numbers) and sends it to the attacker. Android/SteamyScr.A also accepts a number of commands from botnet command servers. This malware is another example of attackers attempting to implement botnet functionality on Android devices.

Google created a security repair tool for Android/DrdDream infections that the creators of Android/Bgyoulu.A cleverly used for their own nefarious purposes. While pretending to be the official Android Market Security Tool, this malware actually monitors incoming SMS data and provides a backdoor for an attacker. Android/Bgyoulu.A appears to sign up a user to a premium-rate SMS service and then deletes the incoming confirmation message. With no indication that the user using a for-pay service, the malware manages to silently steal data and phone information.

[1] http://blogs.mcafee.com/enterprise/mobile/google-tool-cleans-up-mobile-malware-dream
Exploit/LVedu (exploid) http://vil.nai.com/vil/content/v_391661.htm
Exploit/DiutesEx (rageagainstthecage) http://vil.nai.com/vil/content/v_391671.htm

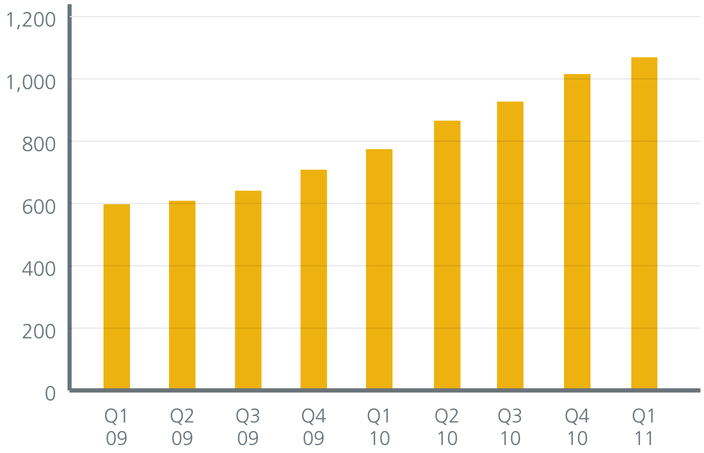
Mobile Malware, by Platform



The criminals who use the Zeus crimeware toolkit have created new versions of Zitmo for both Symbian and Windows Mobile systems. The bank account–stealing thieves who created SymbOS/Zitmo.A have expanded from Symbian to Windows Mobile.[2] MSIL/Zitmo.B is a .NET Compact Framework that is a functional clone of Zitmo.A. It looks like the crooks liked the previous malware's commercial spyware functions so much that they created a custom variant that uses the same command interface.

We expect to see much more development in this class of malware. As the world turns more to mobile devices, so too will cybercriminals and malware writers. Expect them to leverage, at Internet speed, everything they have learned from writing malware in the broader PC world.

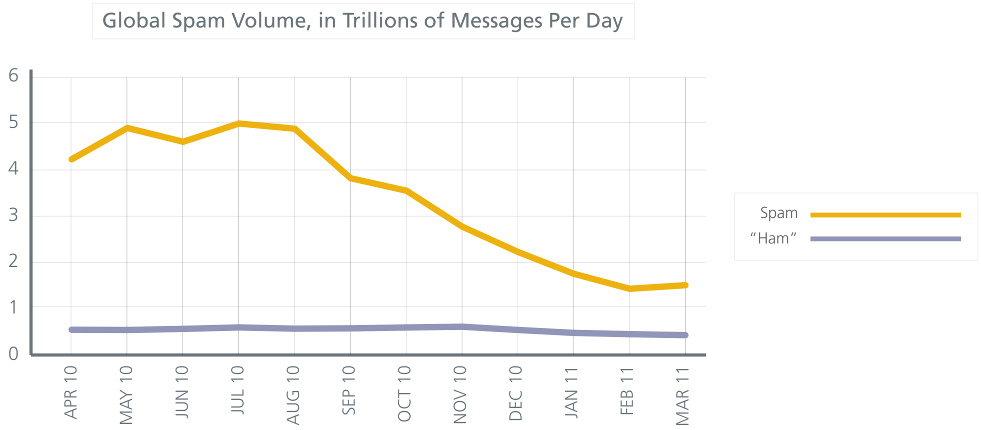
Total Mobile Malware Samples



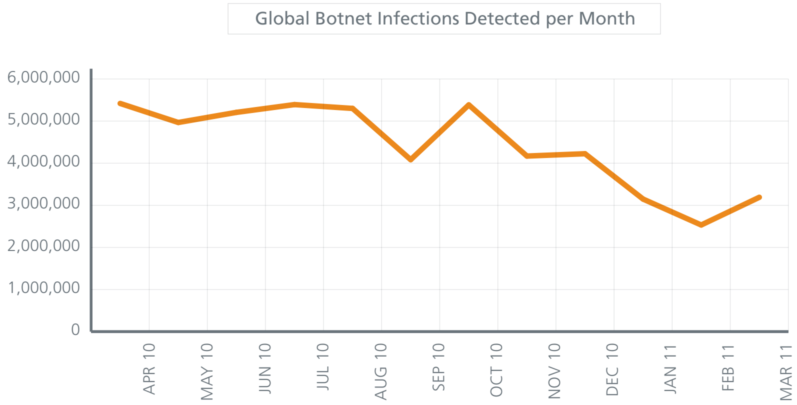
[2] http://blogs.mcafee.com/enterprise/mobile/write-once-mobile-malware-anywhere

Botnet Takes a Fall

One of the most important events of this quarter was the coordinated beheading of the Rustock botnet. This carefully scheduled effort among several security providers, law enforcement, and CERTs was able to shut off major amounts of the zombies and command structure of this very active botnet on a global level.[3] Spam, while already at its lowest point since 2007, dropped once again as a result of this action, outnumbering "ham" (legitimate traffic) by only a 3:1 ratio.



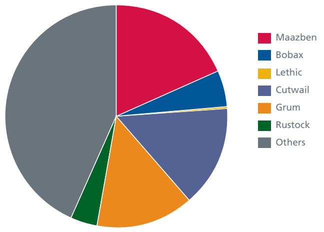
In spite of the success in crippling Rustock, McAfee Labs still sees a small amount of activity from the botnet. We expect Rustock will be reseeded by cybercriminals during the coming months. Although Rustock has suffered, there was a strong uptick in new botnet infections toward the end of this quarter. Whether this is due to reseeding efforts remains to be seen.



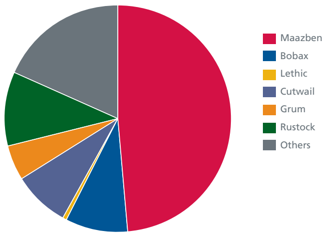
[3] http://blogs.technet.com/b/microsoft_on_the_issues/archive/2011/03/18/taking-down-botnets-microsoft-and-the-rustock-botnet.aspx

As we can see in the next graph, a global breakdown of botnet activity, many botnets are in position to fill the gap left by Rustock's decline. Aside from sending spam, botnets can control a variety of cybercrime—such as denial-of-service attacks, malware distribution and installation, and hosting phishing sites. Thus the information security community must remain vigilant.

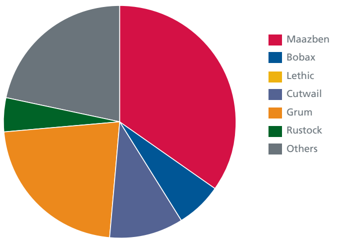
Argentina



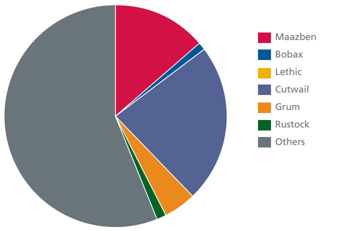
Australia



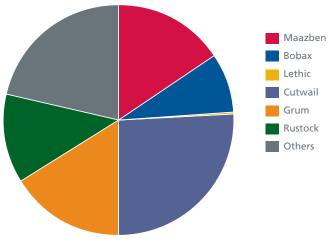
Brazil



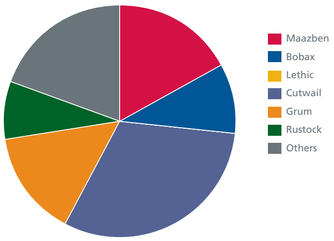
China



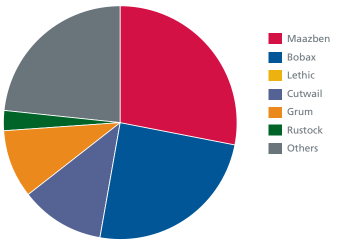
France



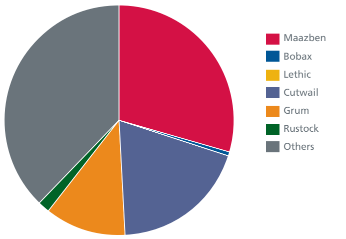
Germany



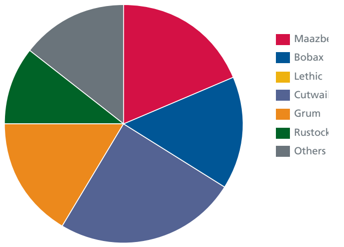
India



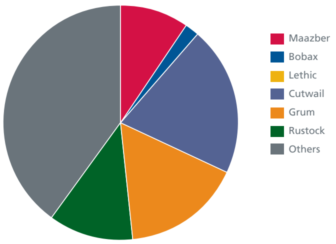
Indonesia



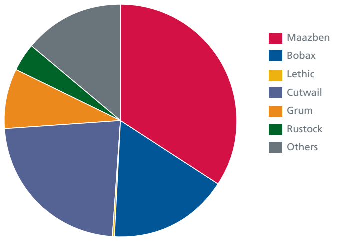
Italy



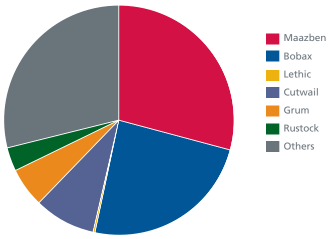
Japan



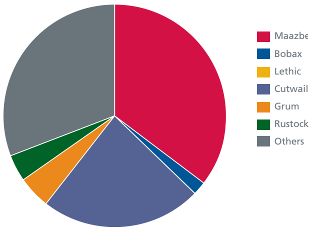
Philippines



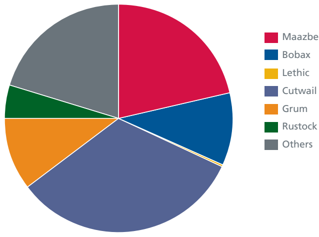
Russia



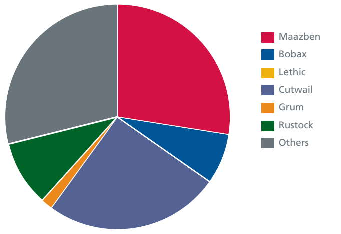
South Korea



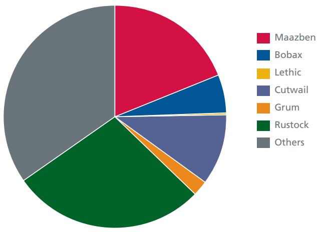
Spain



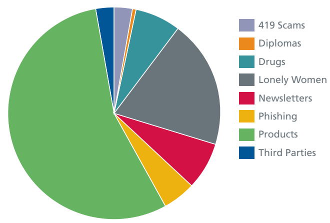
United Kingdom

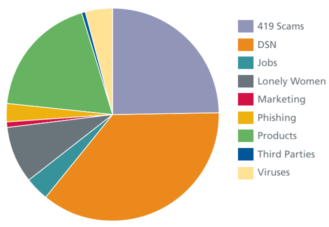


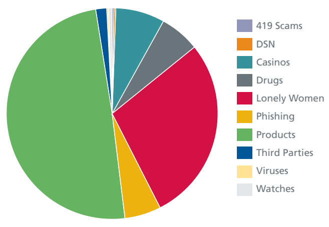
United States

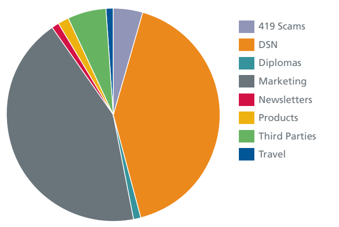


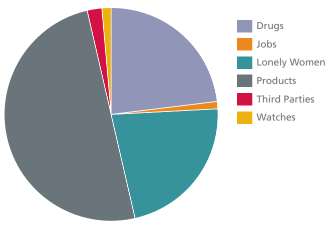
Spam lures and subjects showed their usual diversity this quarter. Product spam trended highly in many parts of the world, as did the topics of delivery status notification (DSN) and drugs. The trend of lure diversity based on location seems to show no signs of stopping, even though we saw several global similarities this quarter.

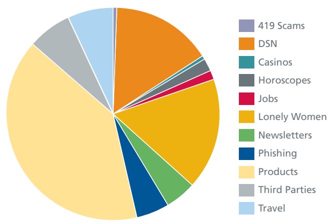

Argentina

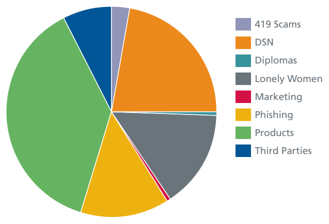

Australia

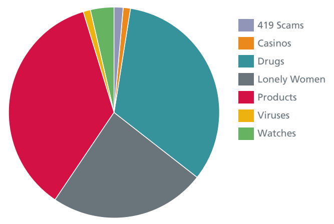

Brazil

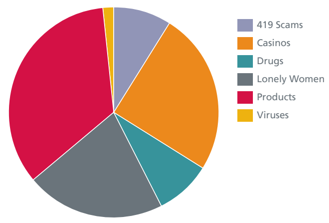

China

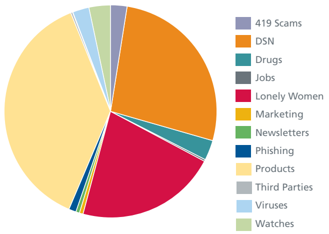

Columbia

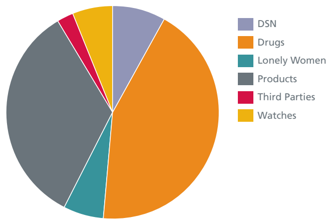

France

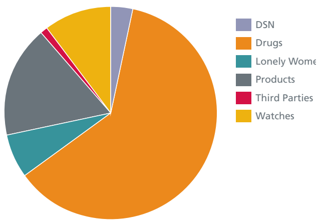

Germany

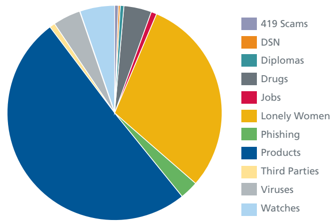

India

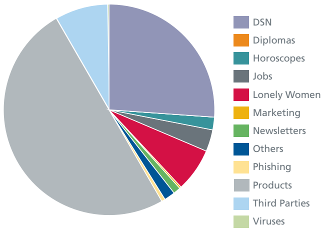

Indonesia

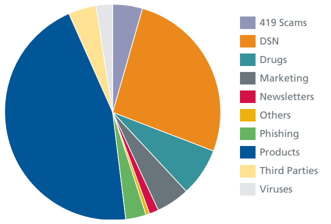

Italy

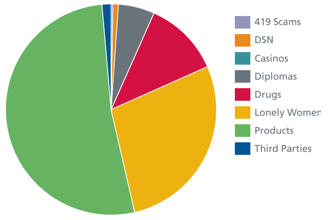

Russia


South Korea


Spain

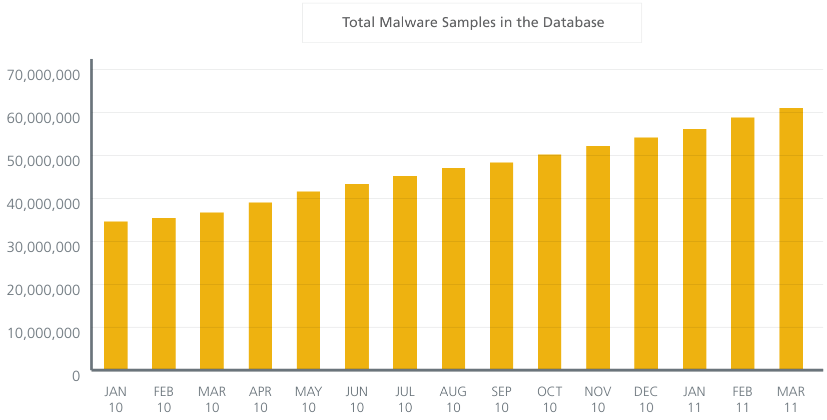

United Kingdom


United States

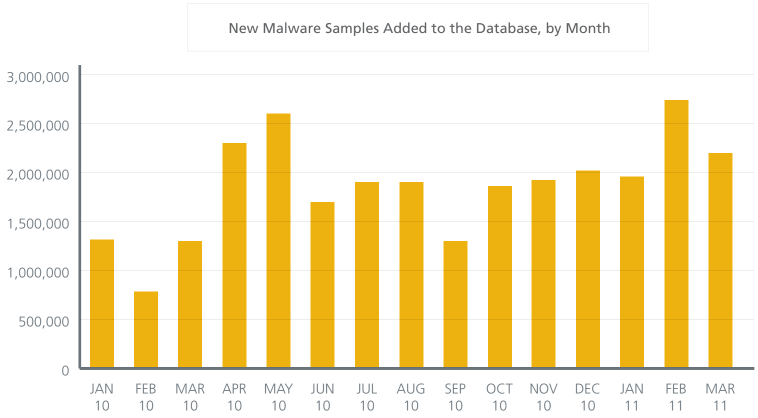

Vietnam

Malware Busier Than Ever

In case we were feeling blasé about the malware landscape, these three months turned out to be the busiest first quarter we have ever seen. McAfee Labs identified more than six million unique malware samples! This far exceeds any first quarter we have seen. Historically this period tends to be a slow quarter for malware, so it will be interesting to see how much malware we identify during the rest of the year. At the current rate of growth, McAfee Labs expects the cumulative "malware zoo" collection to reach 75 million samples by year's end.



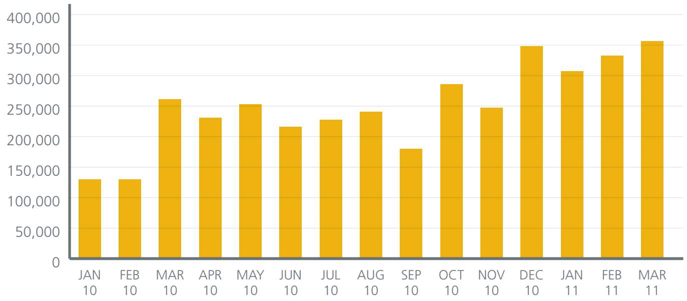
Just to reinforce how significant the growth has been during the last several years, let's take a look at the monthly incremental growth of unique malware binaries:



As the preceding graph makes plain, the last month to register fewer than one million samples was February 2010. Thus we predict more malware on a monthly and quarterly basis for a variety of reasons: more users online, more opportunities for scamming, as well as more efficient means of creating and distributing malware.

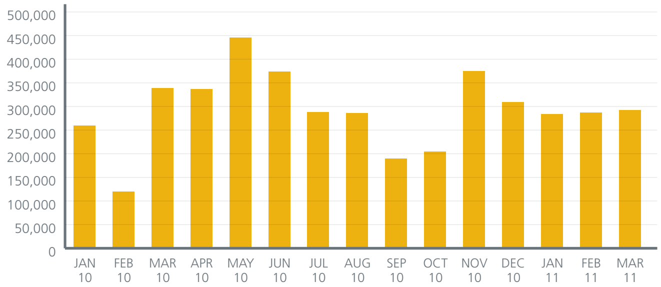
Fake anti-virus, also known as bogus or rogue security software, had a very strong quarter and its growth shows no real signs of slowing. This will remain an actively developed area of malware due to the amount of money cybercriminals can earn with these fake technologies.

Unique Fake Alert Samples Discovered

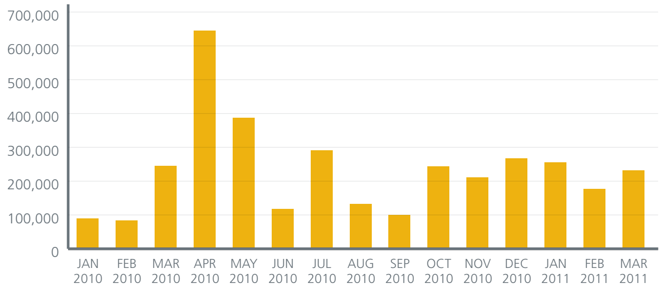


Generic password-stealing Trojans are showing a consistent, sustained level of usage, while AutoRun malware has leveled off a bit. During late 2010 Koobface rebounded to plague Facebook users but actually declined a bit this quarter. (Keep reading for more on password-stealing "banking" Trojans.)

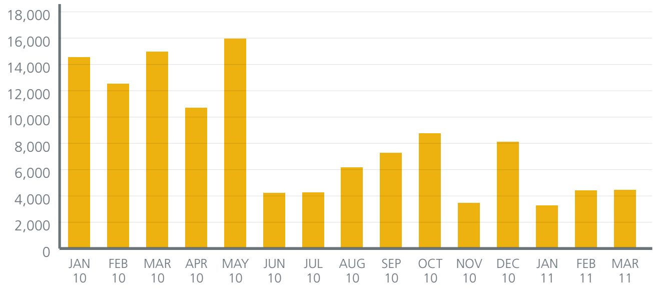
Unique Password Stealers Samples Discovered



Unique AutoRun Samples Discovered



Unique Koobface Samples Discovered



Globally and by geography much of the malware this quarter matched varieties we have already catalogued. We saw some differences among countries and regions but overall we found more similarities than differences.

Rank	Top 5 Global Malware
1	Generic!atr
2	Exploit-CVE2009-3867.b
3	Generic.dx
4	W32/Conficker.worm!inf
5	Exploit-CVE2010-0840

Rank	North America
1	Exploit-CVE2009-3867.b
2	Generic!atr
3	Exploit-CVE2010-0840
4	FakeAlert-WinWebSec!env.g
5	Adware-HotBar.d

Rank	Australia
1	Exploit-CVE2010-0840
2	Downloader-UA
3	FakeAlert-WinWebSec!env.g
4	Generic!atr
5	Exploit-CVE2009-3867.b

Rank	South America
1	Artemis!4D9014D7BB7D
2	Generic!atr
3	W32/Conficker.worm!inf
4	Generic.dx
5	Artemis!85F457A04C99

Rank	Africa
1	Generic!atr
2	Generic.dx
3	W32/Sality.gen
4	W32/YahLover.worm.gen
5	Downloader-CJX!lnk

Rank	Europe and Middle East
1	Generic!atr
2	Exploit-CVE2009-3867.b
3	W32/Conficker.worm!inf
4	Adware-OneStep.l
5	Generic.dx

Rank	Asia
1	Generic.dx
2	Generic!atr
3	W32/Conficker.worm!inf
4	Artemis!78A4F98A5D58
5	Adware-BDSearch

Password Stealers Take It to the Bank

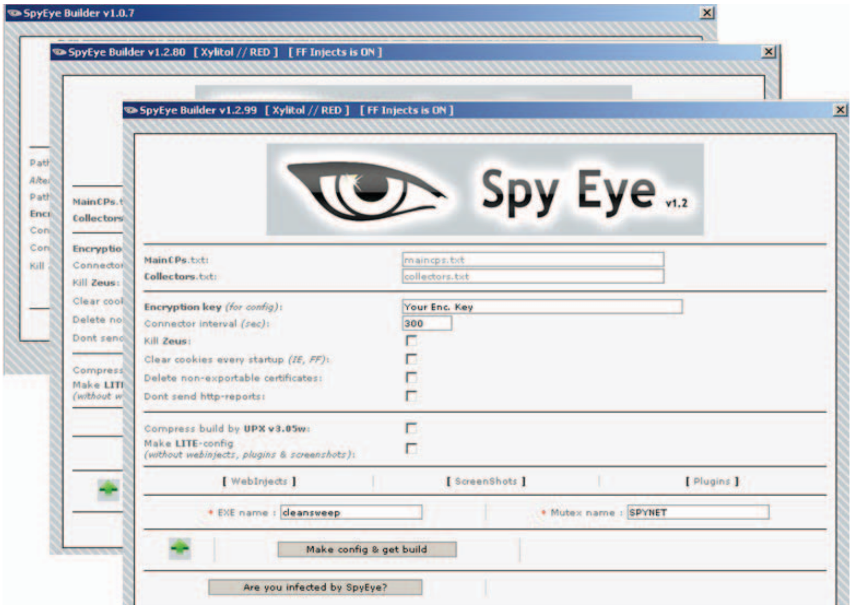
This quarter we noticed an interesting new trend among "banker" Trojans, malware that steals passwords and other data. Although Zeus (a.k.a. PWS-Zbot) continues to be prevalent, both the Zeus and (closely related) SpyEye Trojans are using almost the same phish-like email topics on their spam campaigns. Common lures used in such campaigns included:

- UPS
- FedEx
- NACHA
- USPS
- IRS

As we have discussed in previous Threats Reports, Zeus development appears to have ceased, with its author merging the source code with SpyEye. We haven't seen new developments on the Zeus front, but SpyEye is improving and becoming more potent.

A clear example of this is in SpyEye's architecture, which allows it to add functions via new modules. As of March, the most recent SpyEye (Version 1.3.05) can support more than 150 modules. Some of the most important ones are:

- *USBSpread:* For spreading via USB thumb drives
- *SpySpread:* For spreading via chat/instant messaging
- *CustomConnector:* For controlling communications infrastructure
- *CCGrabber:* For capturing credit card numbers during an online transaction
- *FFCertGraber:* For grabbing Firefox certificates
- *Webfakes:* For spoofing HTTP and HTTPS content. This is very useful for capturing and modifying online banking websites.
- *DDoS:* For launching DDoS attacks against a target using SYN or UDP floods
- *BugReport:* As the author has become more professional, the quality of SpyEye has increased and now includes this plug-in for acquiring and sending technical information


SpyEye Builder v1.0.7
SpyEye Builder v1.2.80 [Xylitol // RED] [FF Injects is ON]
SpyEye Builder v1.2.99 [Xylitol // RED] [FF Injects is ON]
Spy Eye v1.2
[WebInjects]
[ScreenShots]
[Plugins]
Make config & get build
Are you infected by SpyEye?

MainCPs.txt: maincps.txt
Collectors.txt: collectors.txt

Encryption key *(for config)*: Your Enc. Key
Connector interval *(sec)*: 300
Kill Zeus: □
Clear cookies every startup *(IE, FF)*: □
Delete non-exportable certificates: □
Dont send http-reports: □

Compress build by UPX v3.05w: □
Make LITE-config *(without webinjects, plugins & screenshots)*: □

* EXE name : cleansweep
* Mutex name : SPYNET

PWS-Caberp

At McAfee Labs we see a new password stealer variant every day, and they're not terribly hard to combat. However, a few of them continue to develop in a way that challenges security companies. One of these is PWS-Caberp.

PWS-Caberp (sometimes spelled "carberp") has been around since last quarter, but due to the improvements we've seen this quarter this banking Trojan deserves a special mention. This malware was named after some information found during the reverse engineering of the malware:

"G:\carberp\lastwork\carberp_loader\Release\carberp.pdb"

The line above shows a path on the malware author's system, which is probably where the source code resides. As with SpyEye, PWS-Caberp has a modular configuration that allows it to add new features and updates. As of this quarter, the latest version can handle the following plug-ins:

- *Passw.plug:* For the targets the malware will focus on to steal credentials. Currently it can steal credentials from banks in several countries, including the recent waves of attacks in the United States and the Netherlands. It can also steal the credentials of more than 50 applications, including (but not restricted to) operating systems (Windows), FTP clients (ClassicFTP, CoffeeCupFTP, CoreFTP, CuteFTP, FARManagerFTP, FFFTP, FileZilla), IM clients (Trillian, MSN Messenger, AIM, GoogleTalk, GAIM, Miranda), and many others.
- *Miniav.plug:* For removing competitors from the machine. As the name implies, Mini Anti-Virus will try to kill and remove other password-stealing Trojans such as Zeus. No need for competing credential theft!
- *Stopav.plug:* For stopping and neutralizing a variety of security software on the victim's machine

In the coming quarter, besides improvements to SpyEye and PWS-Caberp, we expect to see a revision of Zeus/PWS-Zbot. At the end of this quarter the Zeus source code was leaked on some underground forums, which will certainly result in new variants. What developments we'll find is uncertain, but new modules, or simply new packers and evasions to bypass antimalware detection, are not out of the question.

What's in a Word?

This quarter we noted much the same type of search abuse and term abuse that we have seen in past quarters. You will notice terms such as earthquake, Android, and app store were abused as well as sports terms like Chicago Bears, UFC fight card, bracket, and Daytona 500. All of these terms match popular or timely events. This is a trend we have come to expect; it will continue and eventually move on to new topics.

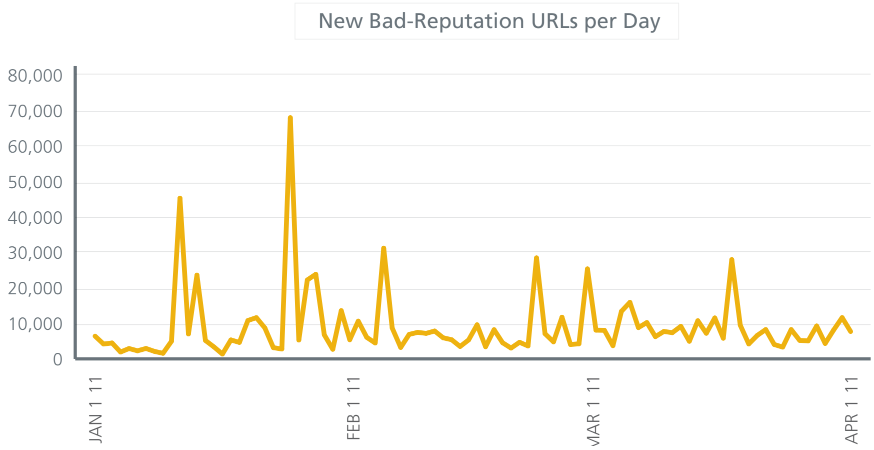
- 1.2 percent of search results this quarter led to a malicious site, down from 3.3 percent last quarter
- 49 percent of the daily top search terms led to malicious sites within the top 100 results (down from 51 percent). On average, each of these poisoned result pages contained more than two malicious links (down from five).

larry.wilcox
2011.nfl.draft.order
the.investment.answer
is.facebook.shutting.down
virginia.fox
dani.johnson
kristi.cornwell
esmeralda.spalding
chicago.airports
jets.vs.steelers.2011
wachovia.online
reality.steve
barney.s.version
bonnaroo.2011
ricky.hendrick
janet.templeton
verizon.news
furciferous
christa.mcauliffe.s.children
dennis.siver
lindbergh.baby
ncaa.basketball.scores
southwest.airlines.careers
channel.13.houston
bob.s.burgers
anthony.borgese
jared.kushner
texas.christian.university
ufc.126.fight.card
us.army.all.american.bowl.2011.roster
shari.s.berries
st.patrick.s.day.recipes
kelly.monaco.leaving.general.hospital
mumford.and.sons
jets.steelers.score
adam.housley
tory.burch
callie.s.biscuits
anderson.silva.vs.vitor.belfort.fight.video
vandenberg.launch
ufc.127.fight.card
megamillions.lottery.results
no.highway.in.the.sky
pat.barry
verizon.announcement
people.s.choice.awards.winners
vandenberg.launch.schedule
jim.tressel.leaving.ohio.state
megamillions.numbers
danny.mozes
earthquakes.today
india.vs.bangladesh.world.cup.2011.highlights
being.human.syfy
us.constitution.text
daytona.500.start.time
ion.tv
internet.explorer.has.stopped.working
jim.cornelison
the.cape.tv.show
roger.ebert.blog
who.does.brad.womack.pick
luigi.manocchio
hanie.chicago.bears
megan.mcallister
daniel.tosh.girlfriend
sandy.bentley
texas.lottery.mega.millions
ky.lottery
who.is.on.the.dime
amazon.app.store.for.android
simon.chipmunk
mike.kekich.and.fritz.peterson
backpage
you.are.resistance
tericka.dye
mps.disease
david.birney
chicago.election.results
superbowl.2011.time
nick.diaz
worldstarhiphop.shut.down
prison.cities
daylight.savings.time.2011
texas.chainsaw.massacre.true.story
romeo.and.juliet.script
tank.carder
highest.grossing.batman.movie
greg.kinnear.movies
one.flew.over.the.cuckoo.s.nest
theremin
a.bugs.life
katie.cassidy
carl.la.bove
faith.kroll
bill.erwin
ncaa.schedule
can.can.pearls
paul.mcdonald.american.idol
ancestry.com.search
dossier.for.m
sam.bradford.contract
bracket.predictions
my.best.friend.s.girl
national.margarita.day.2011
napa
who.did.brad.womack.choose
christine.paolilla
kyw.1060
which.chipmunk.wore.glasses
mega.millions.payout.chart
amanda.knox.update
adam.sandler.dead
ty.corbin
wsdot.cameras
thewless
how.i.met.your.mother.countdown
downton.abbey.season.2
earthquake.bay.area
black.men.earn.money
greely.expedition
big.east.tournament.bracket
ash.wednesday.fasting.rules
ufc.127.live.stream
antique.archaeology
bonnaroo.2011.lineup.rumors
tournament.of.roses.parade.2011
deepest.diving.sea.turtle
lizard.lick.towing
treasuryhunt.gov
syndal.gordon
selena.quintanilla
general.hospital.spoilers
spongebob.legends.of.bikini.bottom
aspen.rae
arepas.recipe
no.chaos.damn.it
omaha.news
w.magazine.kim.kardashian.pics
netflix.login
tracey.thurman
solid.gold.dancers
158.723
curve.treadmill
the.miz.twitter
oregon.basketball.court
stephanie.seymour.and.son
obama.gun.grabbing
les.miserables.25th.anniversary.concert
adam.young.owl.city
beale.street.music.festival.2011
maryland.staged.terror
ufc.126.results
sal.picinich
mark.kelly.astronaut
debbie.friedman.death
lindsay.lohan.white.dress
lea.t.model
what.happened.to.worldstarhiphop
mark.yagalla
megan.abrigo
ash.wednesday.fasting
art.schlichter
rivals.football.recruiting
miss.america.2011.contestants
tina.wallman
cheryl.tiegs.plastic.surgery
puxatony.phil
rose.mcgowan
china.new.boss
harry.s.law
mn.lottery
vinita.nair
wonderlic.sample.test
defriend.day
bank.of.america.website.down
ufc.fight.for.the.troops
sunny.wwe
mazda.recall.spiders
arianna.afsar
nfl.playoff.schedule
oprah.pregnant.at.14
ufc.126.live.stream
acc.tournament.2011
scelestious
tucson.newspaper
wral.school.closings
eddie.aikau.2011
elycia.turnbow
julissa.brisman
surcame
rikki.anderson
eddie.furlong

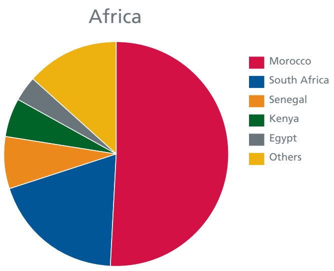
Web Threats

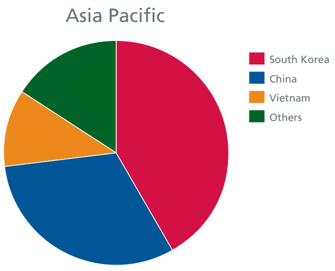
Last quarter McAfee Labs observed a significant increase in the number of domains, IP addresses, and URLs with malicious reputations. In addition to websites with bad reputations, we included in this category sites that host malware, potentially unwanted programs, and phishing sites. This quarter has dropped compared with the previous quarter but is higher than the same time last year.

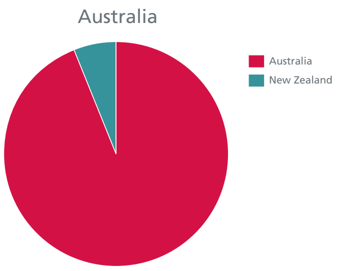
For the quarter McAfee Labs recorded an average of 8,600 new bad sites per day:

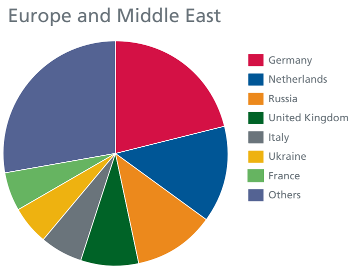

New Bad-Reputation URLs per Day

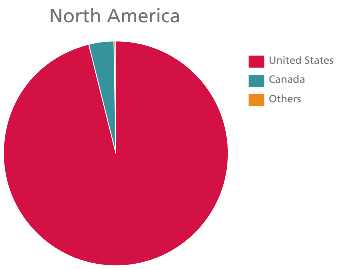
We saw some significant spikes in malicious web content this quarter. Many of these sites correspond to high-impact news events such as the assassination attempt on U.S. Representative Gabrielle Giffords, the Japanese earthquake and tsunami, and major sporting dates. These events are continually exploited by cybercriminals as lures for scams and attacks. The vast majority of these new malicious sites are located in the United States. Next in line, we find South Korea, Germany, and China. Our regional breakdown reveals the most common hosts:

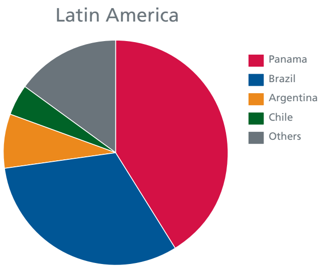

Africa


Asia Pacific

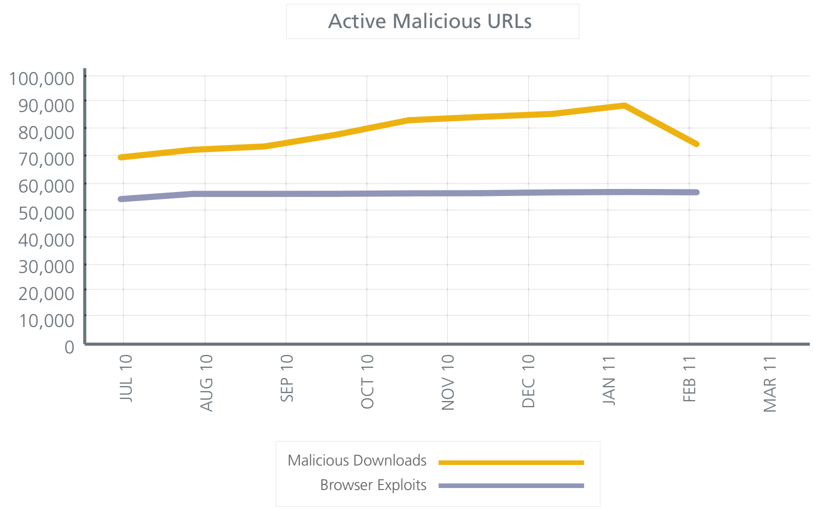

Australia


Europe and Middle East


North America


Latin America

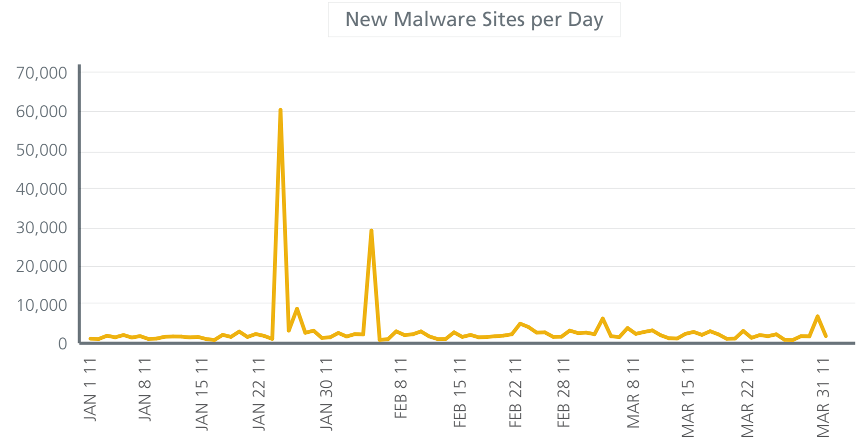
Websites hosting malicious downloads dropped notably this quarter while sites that host browser exploits remained unchanged:



This quarter we also observed a continued increase in blogs and wikis with malicious reputations.

Websites Delivering Malware and PUPs

The next chart provides a picture of the number of websites delivering malware and potentially unwanted programs (PUPs) that McAfee Labs detected this quarter.

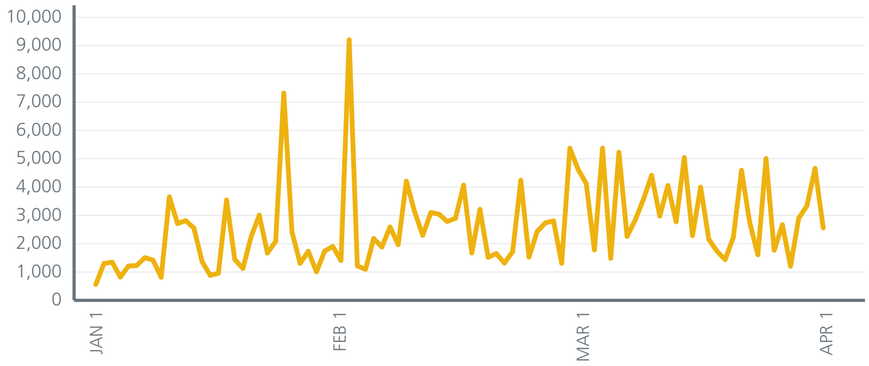


With two notable exceptions, new malware sites were relatively flat this quarter compared with last quarter, increasing slightly on average. But the two exceptions were outstanding. The spike on January 24 was due to W32/Conficker.worm. That day, we found a tremendous amount of Conficker .info and .org domains. The second pronounced spike, in the first days of March, is not linked to any particular attack.

Phishing Sites

After a rapid increase during the first part of 2010, the number of phishing sites discovered each day has been fairly stable since the second half of that year. This quarter we identified approximately 2,500 sites per day, with two large leaps at the end of January. The main lures used that month were Wells Fargo, Paypal, and the French banking group Caisse d'Epargne.

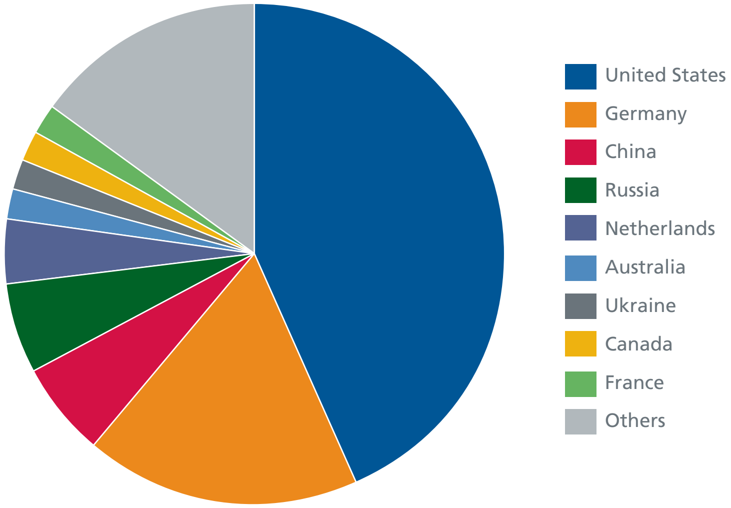
New Phishing Sites per Day



Illegal File Sharing

This quarter we identified around 14 new sites per day used for the illegal exchange of copyrighted files. These sites illegally distribute software or electronic media such as copyrighted music or film, illegal license key generators, software cracks, and serial numbers. We include in this category sites that allow users to search for and exchange files from peer-to-peer networks. The United States is the clear leader in this area, with Germany a strong second ahead of China, Russia, and the Netherlands.

Locations of New Sites for Illegal Exchange of Copyrighted Files



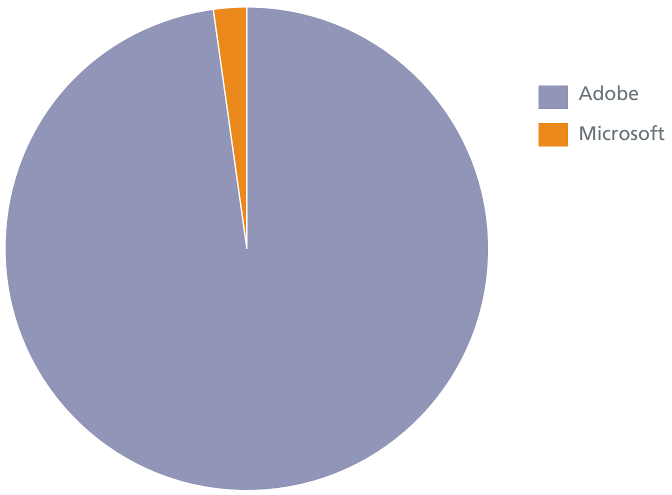
Earthquake and Tsunami in Japan

Only two hours after the Japanese earthquake and tsunami struck we spotted the first potential scam donation site. During the few next hours we collected more than 500 malicious domains or URLs with the terms *Japan*, *tsunami*, or *earthquake* in their titles. Most were created in association with spam campaigns, false news sites to distribute malware, and especially fake charity actions. This behavior will never go away.

Vulnerabilities and Network Attacks

This quarter continued the trend of malware authors heavily exploiting weaknesses in both Adobe Flash and PDF technologies. Our malware database reveals that malicious exploits of Adobe products (more than 36,000 this quarter) topped the number of malicious exploits of Microsoft Office products by a wide margin, again making the former applications the favorite targets of client-side exploitation. McAfee Labs predicted in 2009 that vulnerabilities in Adobe products would become the clear choice of malware authors and cybercriminals for distributing malware and compromising systems and networks. Why? Because of Adobe's huge success and wide deployment footprint. Malware and exploit writers go where the bulk of users go, and those users heavily favor Adobe technologies.

Vulnerabilities in Adobe and Microsoft Applications, by Quarter

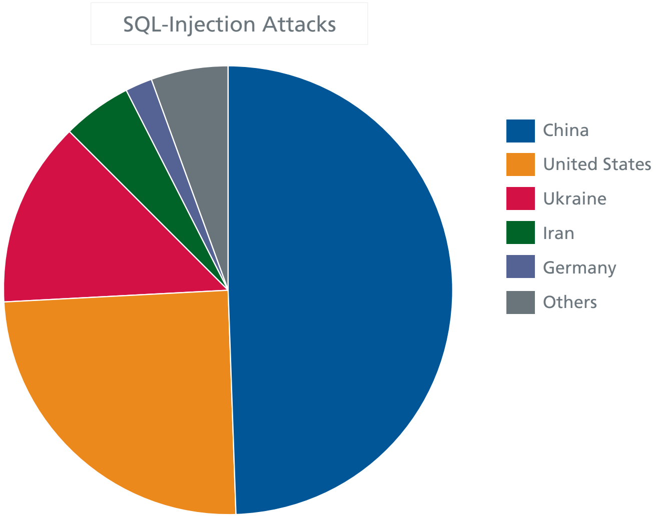


Here's a short list of notable vulnerabilities that appeared this quarter:

- CVE-2010-3971. *CSS Memory Corruption Vulnerability:* Caused by improper memory handling while parsing cross-site scripting that refers to itself recursively. This issue was exploited by zero-day attacks in the wild. Patched by Microsoft on February 8.
- CVE-2010-3970. *Microsoft Windows Shell Thumbnail View Stack Buffer Overflow Vulnerability:* High-risk vulnerability in the Microsoft Graphics Rendering Engine resulted in a stack overflow. An attacker can exploit this issue by enticing the victim to open a malicious .MIC or Office file. Exploits found in publicly available exploit frameworks like metasploit, which can lead to wider exploitation. Patched by Microsoft in MS11-006.
- CVE-2011-0609. *Adobe Reader and Acrobat Authplay.Dll Remote Code Execution Vulnerability:* Exploited by targeted malware in the wild. Reports of a vulnerable Flash file embedded within an Excel sheet being used to exploit via email attachments. Patched by Adobe out of band.

SQL-Injection Attacks

China and the United States continue to be the primary sources for SQL-injection attacks. Generally used to access databases of various types, SQL-injection attacks usually represent a sophisticated class of attacks with a determined aggressor. This quarter again sees China as number one (hosting 50 percent of attacks), with the United States second (25 percent). The Ukraine moved into third position (13 percent), pushing Iran down to fourth (5 percent). Other host countries support no more than 2 percent of attacks.



Cybercrime

This quarter saw some interesting price fluctuations in the services and tools that the cybercrime underground provides. This could be because the tools and services are becoming more widely available, thus driving down the price, or because cybercriminals are using their own tools instead of the services of others.

Botnets as a Service

Botnets can be used for a variety of purposes: denial of services attacks, mail relays for spam, click fraud, and malware implementation. It is also possible for cybercriminals to subcontract these services. Let's look at some current prices we encountered on a variety of forums and cybercriminal websites this quarter:

Name	Prices (all in US$)	Comments
DDoS service	10 minutes: $1 1 hour: $10 2 hours: $15 5 hours: $25 1 day: $50	Prices are falling steadily. Just one year ago prices were generally $20 for one hour and between $100 and $200 for 24 hours.
Install software	Asia: $8 Europe: $50 Canada : $100 Australia : $140 USA: $160	Price is for 1,000 installs of one malware application
Spam service (in millions of emails)	1: $100 3: $200 5: $300 8: $500 16: $900 32: $1,500	Prices for these services are increasing. In 2007, the same business offered 32 million emails for $1,000.
Socks/Proxy service	1 day: $120 1 week: $500 2 weeks: $950 1 month: $1,500	

Crimeware tools

Some of the various exploit tools we track were also updated this quarter:

Name	Prices (all in US$)	Comments
Phoenix V2.5 (January)	V2.5 mini: $150 V2.5 full: $650	Three new exploits: • JAVA RMI (CVE-2010-0094) • JAVA MIDI (CVE-2010-0842) • JAVA SKYLINE (unknown CVE related to Java OBE)
Bleeding Life V2 reloaded (March)	New buyers: $400 V1 buyers: $250	Includes exploits from 2010: • PDF LIBTIFF: CVE-2010-0188 • JAVA MIDI: CVE-2010-0842 • PDF SWF1: CVE-2010-1297 • PDF SWF2: CVE-2010-2884 • Java JRE/JDK: CVE-2010-3552 • JavaSignedApplet (unknown CVE, requires user interaction)
Eleonore V1.6.3.a (February)	$2,000	We noted V1.6.2 last quarter. This version adds a new exploit: • IE CSS PARSER: CVE-2010-3971

Other notable cybercrime events:

Region or Country	Date	Description
Europe	January	The European Commission, the Brussels-based regulator, suspended operations at 30 of the region's greenhouse-gas emissions registries after a Czech firm reported about €6.8 million of carbon allowances were stolen in a hacking attack.[4]
South Africa	January	*The Mail & Guardian Online*, one of South Africa's oldest and most respected sources of news and opinion, was taken offline after an attack by Russian cybercriminals who wanted to use the newspaper's servers as a base for scam operations and other malicious activities.[5]

[4] http://www.businessweek.com/news/2011-01-20/hacking-attack-prompts-doubts-about-security-of-eu-carbon-market.html

[5] http://memeburn.com/2011/01/russian-hackers-target-mail-guardian-online-site-taken-down/

Actions against Cybercriminals

A wide array of global enforcement agencies have enjoyed successes this quarter:

Country	Date	Description
United States	January	In New Jersey, two men were charged with allegedly hacking AT&T's servers. They stole email addresses and other personal information belonging to approximately 120,000 Apple iPad users who accessed the Internet via AT&T's 3G network. The attack occurred in June 2010.[6]
United States	January	Federal Trade Commission officials claimed they have shut down an Internet scam known as "I Works," which duped hundreds of thousands of people into providing their credit and debit card information and forcing payment for items they did not purchase.[7]
Holland	January	Around 60 people were arrested by police in Amsterdam in connection with a money mule operation that stole money from online bank accounts. The arrested group has been questioned about phishing attacks, bank fraud, and money laundering.[8]
United States	January	Facebook announced that a federal court has awarded PP Web Services $360,500,000 in statutory damages and issued a permanent injunction against spammer Philip Porembski, who was said to have obtained the login details of at least 116,000 Facebook users and sent more than 7.2 million spam messages to victims' online friends.[9]
Russia	February	A Russian court passed down a five-year suspended sentence for Yevgeny Anikin, 27, one of the cybercriminals involved in the 2009 RBS WorldPay systems heist.[10] The light sentence was reportedly due to assistance Anikin offered authorities with the investigation. He is the second person involved in the breach to get off without prison time. In September, Viktor Pleshchuk, 29, who also was tried in Russia, got a six-year suspended sentence and four years of probation.
Romania	February	Romanian law enforcement authorities, in close cooperation with Europol, have successfully disrupted an international organized crime group responsible for payment card fraud. The criminal group was active in many E.U. countries, including Poland, Romania, Sweden and the United Kingdom. The main focus of their criminal activities was the skimming and counterfeiting of payment cards and illegal cash withdrawals all over the European Union.[11]
Great Britain	March	The Metropolitan Police of London arrested three men and a woman who ran the GhostMarket forum. They were sentenced to a combined total of more than 15 years.[12] This English-language criminal forum was one of the largest for selling stolen credit card numbers and the tools to steal data. It had more than 8,000 members.

[6] http://newark.fbi.gov/dojpressrel/pressrel11/nk011811.htm
[7] http://www.ftc.gov/opa/2011/01/iworks.shtm
[8] http://news.hostexploit.com/cybercrime-news/4760-dutch-police-stop-phishing-and-money-mule-gang.html
[9] http://www.facebook.com/security#!/note.php?note_id=442722120765&id=31987371885
[10] http://english.ruvr.ru/2011/02/08/43313934.html
[11] http://www.europol.europa.eu/index.asp?page=news&news=pr110216.htm
[12] http://content.met.police.uk/News/Internet-fraudsters-jailed-for-online-criminal-forum/1260268602623/1257246741786

Hacktivism

This quarter, the Anonymous group continued its campaigns against countries and ideologies that do not agree with them, but the group seems to be in a period of transition. Whether the various arrests, warrants, or mere public disclosures gave them pause is uncertain. During the recent revolts in Arabic-speaking countries in North Africa and the Middle East, IRC channels were not as full of discourse as they have been in the past. Hacktivists, and even more numerous non-hacktivists from these countries and around the world, used Twitter, YouTube, and Facebook to promote their messages and circumvent government-controlled media outlets.

- The “We are all Khaled Saeed” Facebook page, created in January by Wael Ghonim, was seen as a catalyst for the Egyptian revolution
- During the last two weeks of January, Sysomos Company studied the posts of 14,642 Twitter users from the Middle East (88 percent were from Egypt). They posted 122,319 tweets from January 16 to 23 and 1,317,233 from January 24 to 30.[13] Tweets increased by a factor of ten during the week following January 25, the “Day of Wrath,” when thousands of Egyptians were in the streets rallying.
- In Morocco the Facebook group “February 20th movement, people want change…” rallied more than 19,000 sympathizers
- “The Syrian Revolution 2011” page accumulated 96,000 “likes” and raised awareness of Syrian freedom and rights issues

Country/Target	Date	Description
Turkey	February	Turkish hacktivists launched a massive campaign against the Armenian genocide international recognition process, breaking 6,173 Armenian websites worldwide.
Korea	March	About 40 sites—including the Presidential, National Intelligence Service, Foreign Ministry, Defense Ministry, and the National Assembly—were targeted with denial-of-service attacks, beginning March 4
Thailand	March	A Thailand-based news website critical of Myanmar's military government says it was hacked by unknown attackers who posted fake articles intended to create confusion and misunderstanding, and to discredit the news agency [15]
United States	March	The web collective Anonymous took aim at Bank of America, releasing emails leaked from a former employee that purported to show widespread "corruption and fraud" at the banking giant and its subsidiary, Balboa Insurance [16]
France	March	The French Finance Ministry had its computers infiltrated by attackers searching for confidential governmental information. According to the current Minister of Budget, the attackers were interested in information about the G-20.[17]
Belgium (European Commission)	March	As a sensitive summit of E.U. leaders drew near, a “serious attack” occurred against the European Commission websites for diplomatic relations. Sites for 27 E.U. states were also shut down.[18]
United States (Comodo Group Inc.)	March	On March 26, an independent Iranian attacker took credit for the Comodo affiliate Registration Authority compromise. In his manifesto, he claimed no association with the Iranian Cyber Army and insisted he was simply a hacker “with a 1000 times the knowledge and experience as everyone else.”[19] Nonetheless, he clearly supports the Iranian president.

[13] http://www.vincentabry.com/crise-egypte-twitter-infographie-10756/

[14] http://www.armeniadiaspora.com/component/content/article/84-news/2096-turks-break-over-6000-armenian-websites-to-counter-genocide-recognition-process.html

[15] http://www.cbsnews.com/stories/2011/03/13/ap/asia/main20042597.shtml

[16] http://theweek.com/article/index/213212/anonymous-bank-of-america-takedown-why-did-it-flop

[17] http://blogs.mcafee.com/mcafee-labs/cyberattack-targets-france%e2%80%99s-g20-plans

[18] http://www.google.com/hostednews/afp/article/ALeqM5iqMq8cBf3olYzAhkajYGscTTKB7A?docId=CNG.552ff9f9a78416c1f5ab7234144d85ce.a91

[19] http://arstechnica.com/security/news/2011/03/independent-iranian-hacker-claims-responsibility-for-comodo-hack.ars

As we can see, hacktivism is not limited to actions in favor of oppressed peoples or individual freedom. This quarter democratic countries and minorities were also the victims of individuals or groups with extremist tendencies supporting authoritarian regimes.

Cyberwarfare?

The border between pure hacktivism and online attacks that appear to be driven by governments is a thin line. The French and European Union attacks listed in the previous tables are examples. In addition to these attacks, several others this quarter were notable:

Country/Target	Date	Description
Tunisia	January	Based on reports of users in the country, Tunisian authorities appeared to launch man-in-the-middle attacks to steal usernames and passwords from sites such as Facebook. One Facebook response was to route all Tunisian requests to an https server.[20]
Canada	February	The Treasury Board of Canada announced that the department had suffered "an unauthorized attempt to access its networks," after a CBC report said a cyberattack originating in China had compromised the emails of top-ranking government officials.[21]
Global oil, energy and petrochemical companies	January	Named "Night Dragon" by McAfee, this long-term targeted attack was launched against five confirmed companies. Gigabytes of documents related to oil-/gas-field bidding projects, oil discoveries, and industrial control (SCADA) data were compromised. Control servers and source attack traffic came from IP addresses in China, Ireland, and the Netherlands.
Iran	March	Brig. Gen. Ali Fazli, deputy commander of Iran's Basij Forces, said in an interview that Basij hackers were behind cyberattacks against "enemies of the Islamic Revolution."[22]
Australia	March	Cyberattackers reportedly compromised computers in the offices of Australian Prime Minister Julia Gillard and senior ministers. Press investigators say that four separate government sources confirmed that Chinese intelligence agencies were among a list of foreign hackers under suspicion.[23]

Cybercrime and hacktivism are clearly here to stay. We'll have to wait to see whether cyberwarfare develops into another form of worldwide violence; it certainly has the potential to do so. Our world is now so technology-based that these threat vectors will certainly become more pervasive.

[20] http://www.theatlantic.com/technology/archive/2011/01/the-inside-story-of-how-facebook-responded-to-tunisian-hacks/70044/

[21] http://www.montrealgazette.com/news/Chinese+cyber+attack+targets+Canadian+government+departments/4298184/story.html

[22] http://www.insideiran.org/media-analysis/commander-admits-basij-hackers-conducted-cyber-attacks/

[23] http://www.nzherald.co.nz/australia/news/article.cfm?l_id=15&objectid=10715773

About the Authors

This report was prepared and written by Pedro Bueno, Toralv Dirro, Paula Greve, Rahul Kashyap, David Marcus, François Paget, Craig Schmugar, Jimmy Shah, and Adam Wosotowsky of McAfee Labs.

About McAfee Labs

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

About McAfee

McAfee, a wholly owned subsidiary of Intel Corporation (NASDAQ:INTC), is the world's largest dedicated security technology company. McAfee delivers proactive and proven solutions and services that help secure systems, networks, and mobile devices around the world, allowing users to safely connect to the Internet, browse, and shop the web more securely. Backed by its unrivaled Global Threat Intelligence, McAfee creates innovative products that empower home users, businesses, the public sector, and service providers by enabling them to prove compliance with regulations, protect data, prevent disruptions, identify vulnerabilities, and continuously monitor and improve their security. McAfee is relentlessly focused on finding new ways to keep our customers safe. www.mcafee.com

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

The information in this document is provided only for educational purposes and for the convenience of McAfee customers. The information contained herein is subject to change without notice, and is provided "as is," without guarantee or warranty as to the accuracy or applicability of the information to any specific situation or circumstance.