Report

McAfee®

McAfee Threats Report: Second Quarter 2009

By McAfee® Avert® Labs

Table of Contents

The McAfee Threats Report brings you the latest in statistics and analysis covering email- and web-based threats. This quarterly report has been created by the researchers at McAfee Avert Labs, whose worldwide staff provides a unique perspective of the threat landscape—ranging from consumers to enterprises, and from the United States to countries around the world. Join us now as we examine the leading security issues of the past three months. Once you've finished here, you can find more information at the McAfee Threat Center.[1] You'll also find our first-quarter Threats Report.[2]

In the second quarter of 2009, we saw spam production recover quickly from a recent setback and grow to record levels. Zombies, computers hijacked by spammers to send messages, also reached record numbers. We break down spam output by country and subject.

On the web, malware on both legitimate and malicious sites continues to exploit browsers. Robot networks "capture" and control machines to steal data and send spam. Twitter has become a popular target for attackers. It's the current darling among social networking tools, and malware authors are well aware of its potential to be abused. You know your new online lifestyle has made it big when it's scheduled for a Month of Twitter Bugs. Twitter has also played a "hacktivist" role in the Iranian election and its aftermath.

In the malware world, we've seen rapid growth among password-stealing Trojans, which primarily target your banking data. These programs are simple, stealthy, and now easier than ever to produce. Websites primarily hosted in Russia offer Trojan-creation tools that allow a neophyte attacker to purchase the means to steal your data. AutoRun malware is also easy to create, thanks to the ready availability of freeware compilers and packers.

Spam Bounces Back

If the economy could rebound as spam has done in second quarter, we would all be much happier with our retirement accounts. Spam has surged since the prior quarter, increasing nearly 80 percent. Last quarter's spam fell drastically from previous quarters in large part due to the shutdown of the McColo ISP. Nonetheless, this quarter's surge is significant and has approached record levels. The previous period we measured with a record increase was the second quarter of 2008, but the current quarter has beaten it by 10 percent. In our *July Spam Report* we reported that new zombies created in the first quarter would be a leading indicator of things to come; that prediction has proven true.[3]

Spam activity in June alone warrants specific mention. June produced the highest amount of spam we have ever seen, beating the previous high month, October 2008, by more than 20 percent.

Spam as a percent of total mail also set a record this quarter. We estimate its prevalence at 92 percent; this "outperforms" the 91 percent we recorded in the second and third quarters last year.

So maybe spam is the leading indicator for the economy and better times are just ahead. We can hope this is true, but the one thing we can predict is that spam is back and looks to be heading toward new heights.

[1] http://www.mcafee.com/us/threat_center/default.asp or www.trustedsource.org

[2] McAfee Avert Labs, *McAfee Threats Report: First Quarter 2009*. http://img.en25.com/Web/McAfee/5395rpt_avert_quarterly-threat_0409_v3.pdf

[3] http://www.mcafee.com/us/local_content/reports/mcafee_spam_report_july09.pdf

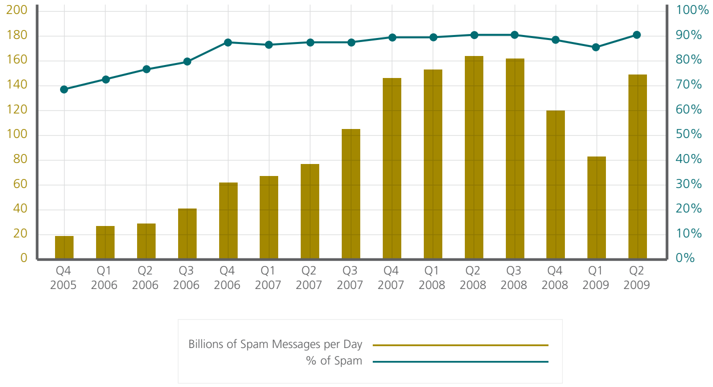


Figure 1: Global Spam Volumes and Spam as a Percentage of All Mail

New Zombies

We observed almost fourteen million new zombies this quarter. That's another record, and it broke the record set in the last quarter, in which we saw nearly twelve million new zombies come into service. That's an increase of more than 150,000 new zombies every day, systems that have the potential to send spam and other malicious items to your computer. With this type of zombie-creation trend in motion, we can easily predict that spam volumes will rise in the next quarter.

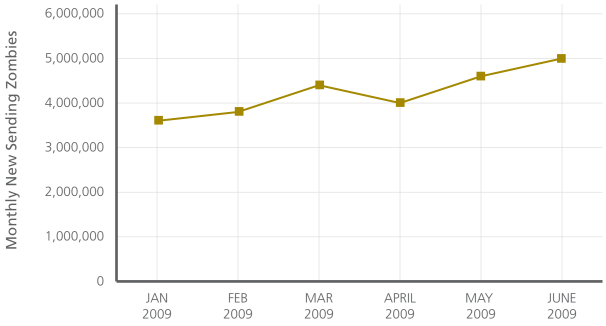


Figure 2: New Zombies Sending Spam, by Month.

New Zombies by Country

Looking at zombie production by country we see that the usual suspects make up our Top 10. The only country to break into the club this quarter is Italy; however, this is not the first Top 10 appearance for the Italians.

The United States alone produced an estimated 2.1 million new zombies this quarter, up 33 percent from the last period. South Korea experienced the largest jump (by 45 percent) in zombies created quarter over quarter, and contributed more than a half-million new zombies to the party this quarter. Italy also nearly doubled its zombie output in the quarter. Even with the global increase, two countries that contribute heavily to zombie creation, China and Russia, both had a reduction in the number of new zombies created.

Q2 2009

Country	%
United States	15.7
China	9.3
Brazil	8.2
Russia	5.6
Germany	5.3
Italy	4.0
Rep. of Korea	3.8
India	3.2
United Kingdom	3.0
Spain	2.6
Total	60.7

Figure 3: Top 10 Countries of Newly Created Zombie Computers, by Quarter. These Systems Are Hijacked to Send Spam to Millions of Email Addresses.

Spam by Country

The total percentage of spam produced in our Top 10 countries dropped by 5 percent from last quarter, indicating that more countries are taking part in spam production. Nonetheless, 65 percent of spam production still comes from these ten nations, which continue to dominate the business.

Spammers in the United States may be feeling the economic crisis. The amount of spam producing there dropped to 25 percent from 35 percent last quarter. However, spam volumes increased by nearly 80 percent over last quarter, so the estimated volume of spam coming from the States was up almost 25 percent.

Brazil, Turkey, and Poland saw significant increases as well as sizable increases in total output.

Spain returns to the Top 10 after a one-quarter absence, and we "welcome" the Czech Republic to our infamous collection.

Q2 2009		Q1 2009		Q4 2008	
Country	Percent of Total	Country	Percent of Total	Country	Percent of Total
United States	25.5	United States	35.0	United States	34.3
Brazil	9.8	Brazil	7.3	Brazil	6.5
Turkey	5.8	India	6.9	China	4.8
India	5.6	Rep. of Korea	4.7	India	4.2
Poland	4.9	China	3.6	Russia	4.2
Rep. of Korea	4.6	Russia	3.4	Turkey	3.8
Russia	2.4	Turkey	3.2	Rep. of Korea	3.7
Romania	2.3	Thailand	2.1	Spain	2.4
Spain	2.1	Romania	2.0	United Kingdom	2.3
Czech Rep.	1.9	Poland	1.8	Colombia	2.0
Percent of Total World Spam	64.9		70.0		68.3

Figure 4: About 65 Percent of Global Spam Originated in Just Ten Countries.

Spam by Subject

Your local pharmacist must be working overtime, as the amount of prescription drug spam has skyrocketed this quarter, accounting for 60 percent of the total spam that our sensors gathered.

	Q2 2009		Q1 2009		Q4 2008		Q3 2008
Pitch	Percent of Total	Pitch	Percent of Total	Pitch	Percent of Total	Pitch	Percent of Total
Prescription drug	60.0	Prescription drug	25.0	Prescription drug	37.0	Male enhancement	31.2
Advertising	16.0	Advertising	21.9	Advertising	19.3	Advertising	19.3
Male enhancement	7.3	Product replica	18.8	Male enhancement	16.8	Prescription drug	10.7
DSN	6.6	Male enhancement	17.5	DSN	9.5	Storm	8.0
Product replica	2.0	DSN	7.1	Dating	3.9	DSN	7.7
Dating	1.2	Storm	1.6	Product replica	2.6	Breaking news	6.7
Storm	1.1	Diploma	1.1	Employment	1.7	Product replica	6.0
Job	1.0	Software	1.1	Software	1.5	Debt loan	1.6
Debt loan	1.0	Debt loan	1.0	Debt loan	1.2	Banking	1.1
Other	3.8	Other	4.9	Other	6.5	Other	7.7
	100.0		100.0		100.0		100.0

Figure 5: Spam by Type. Prescription Drug Spam, Always Popular, More Than Doubled this Quarter, Leaping Up to 60 Percent of all Spam We Measured.

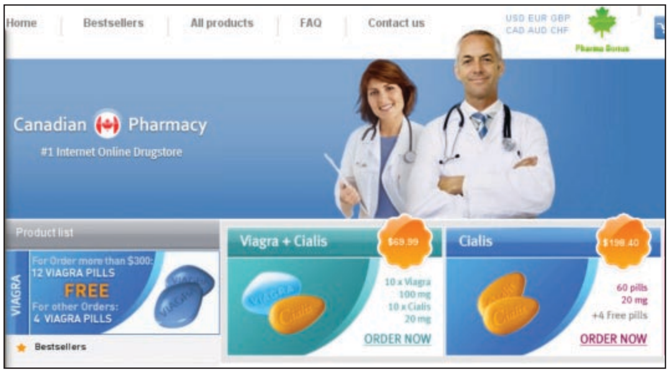


Figure 6: This "Pharmacy" Sends Most of Today's Spam.

Most of the spam we see today claims to come from one Canadian pharmacy. This website is generally linked to a Chinese or Russian URL that was registered with a Chinese registrar. A distinguishing feature of this spam is that it claims it was sent because the recipient requested it or a friend sent it, usually from a newsletter or mailing list. This species of spam with all its offshoots currently accounts for 60 percent of common spam we see. Although many other spam campaigns exist, prescription drugs are the ones that cause the biggest headache if you do not have proper spam filters in place.

Web Attacks Change Target

Last quarter we saw plenty of headlines regarding browser exploits, mainly thanks to the Conficker worm. The attention this quarter, however, appears to have returned to website attacks. This transition can be seen in Figure 7, below, which illustrates the number of new web pages exploiting browsers that are discovered each day. There were a number of attacks that plagued legitimate websites during the quarter, many of them gaining access using standard SQL injection and password theft. Typically attackers inserted obfuscated scripts that redirected users to a malicious domain or set of malicious domains, which would then attempt either to trick the user into installing the payload or to find an unpatched vulnerability in the user's web browsing tool set.

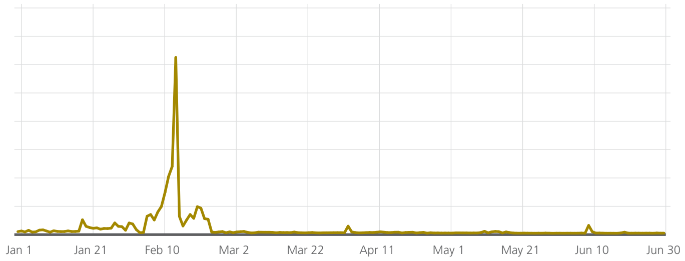


Figure 7: Web Pages Discovered Daily That Exploit Browsers.

Some of the attacks that gained media attention included Gumblar, which first appeared at the end of April and peaked around the end of May. It was followed by the Martuz and the Beladen attacks. We read headlines trumpeting the infections of thousands of legitimate websites. Regardless of the actual number, these attacks merely redirect users to the key malware-serving sites that we have already seen. It's interesting that long after these malicious domains were shut down they continued to top Google's hit results with respect to malicious domains.[4] This longevity illustrates how much time it takes many legitimate web servers to notice that they have been attacked and to clean up the damage.

Gumblar also illustrates how often these malicious websites, servers, and URLs are reused for various activities. While monitoring and tracking Gumblar, we identified several domains that operated in conjunction with this exploit. Seventy-one percent of the domains that we identified in this attack were already noted and in use with other attacks. An additional 13 percent of the domains already had "earned" our TrustedSource Malicious Web Reputation designation prior to joining in the current attack. (The TrustedSource Malicious Web Reputation label is based upon advanced behavioral analysis that identifies a site as potentially harmful.)

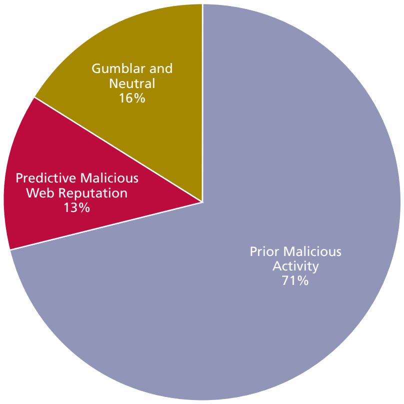


Figure 8: Gumblar Sites, by Type.

[4] Google Online Security Blog, "Top 10 Malware Sites." http://googleonlinesecurity.blogspot.com/2009/06/top-10-malware-sites.html

How did the overall web threat picture look this quarter? Ignoring April's Conficker effect, which attracted considerable media attention, we saw a slight decrease in the rate of growth of URLs with a malicious web reputation compared to last quarter. One of the reasons for this decrease has to do with the evolution of malicious domains. Historically, we identify and protect against many of these domains as soon as they register. That remains true more often than not, although we now see new trends in the methods that malicious domains use to register and the sites that these domains associate themselves with. As cybercriminals appear to adjust to the security techniques of tracking and measuring hosting services and the types of activities they support, attackers are adapting to new ways to hide themselves. This has caused a decrease in the number of domains that we can identify upon registration as malicious. However, the spikes noted during this quarter correlate to noticeable malicious domains using domain-registration practices and other predictive indicators; so our traditional methods of association are still quite effective.

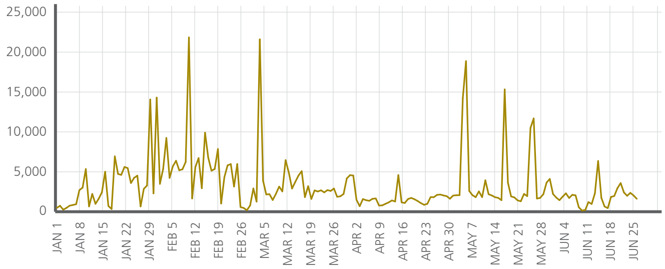


Figure 9: New Websites with Malicious Reputations, Reported Daily

We saw no significant changes regarding where malicious web servers are located. (See Figure 10, below.) However, when we step back from looking at the individual servers and focus on the domains and URLs that are hosted on those servers, the geographical perspective changes. (See Figure 11, below.) This brings to light some new countries that make the list—including Australia and the Bahamas. The latter yields an average of 1,482 malicious URLs per malicious web server. In this quarter, our investigations of malicious servers in Central America and the Caribbean have increased.

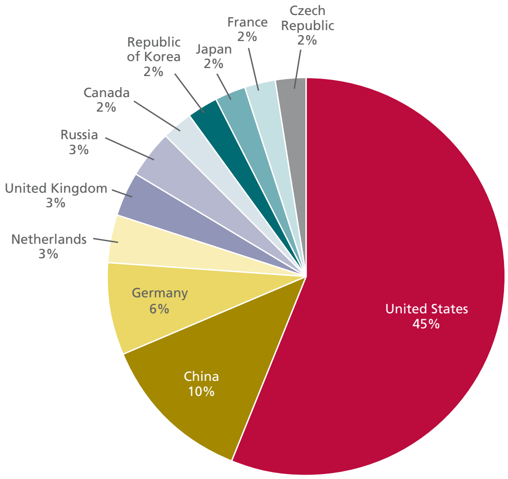


Figure 10: Distribution of Web Servers with Malicious Reputations.

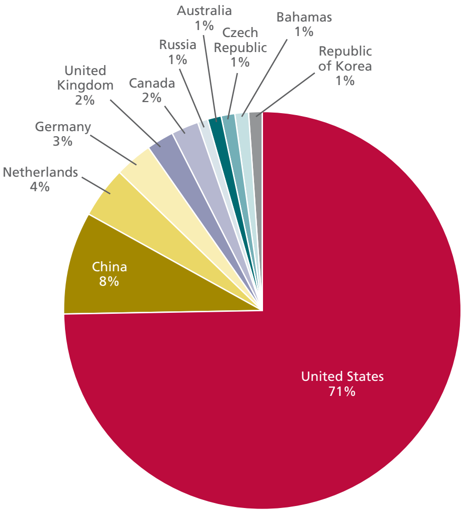


Figure 11: Distribution of Total URLs with Malicious Reputations

Coming From a Home Near You

Another web threat comes from underprotected home machines. These systems may be infected and controlled by outsiders as part of their "botnets for hire" and are used to send spam, steal home users' information, and much more. We also see home users setting up various remote access services, anonymizers, and similar services to allow them access to their home computers from anywhere—including the corporate network. This quarter we took a look at what websites reside on these systems. We excluded all home PCs that are *not* hosting active, advertised websites. Of those that are hosting active sites, we were not surprised to find that most of these are serving spam URLs.

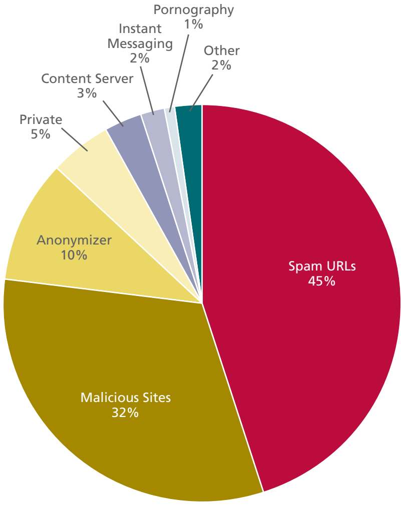


Figure 12: Home-Based Websites, by Usage

Malware and PUPs

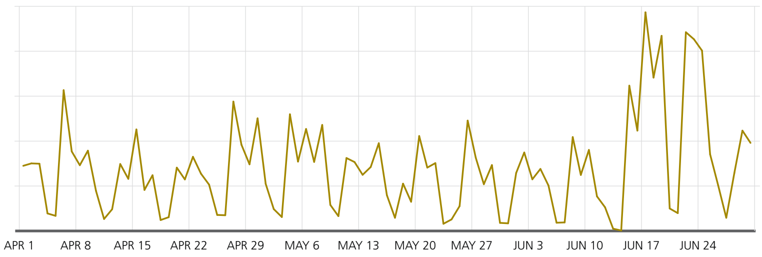


Figure 13: New Websites Delivering Malware and Potentially Unwanted Programs, by Day

Apart from the noise surrounding Conficker, this quarter has been a bit slower than last regarding websites earning our Malicious Web Reputation label. However, this quarter is ending strongly. During the last few weeks we've seen significant activity in SQL and iframe injections, search-engine optimization, downloaders, spoofers, rogue anti-virus (AV) software, and more. For instance, after the death of Michael Jackson we saw an increase in both spam and malware related to the news. Attackers immediately employed search engine efforts to try to redirect users to a rogue AV site or an infected Flash video. Further, we see these servers increasing the breadth of their attacks as they search for one that will successfully infect visitors.

Looking at the types of malware and potentially unwanted programs (PUPs) that are downloaded from web servers, we discovered that there was little change in prevalence between this quarter and last. Generic PUPs make up the lion's share of web-borne downloads.

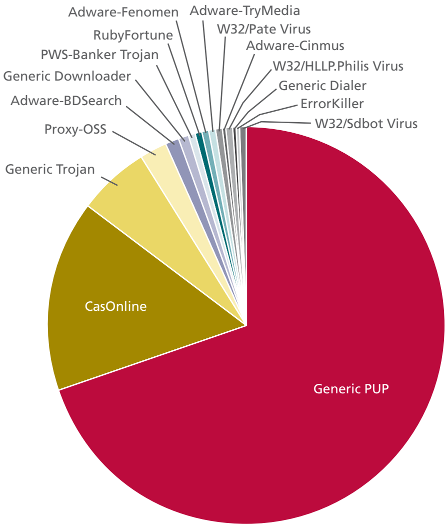


Figure 14: Malware and PUPs Download Prevalence, by Type

Web 2.0 and Twitter

With the events of this quarter—the Air France crash, Iranian elections, the deaths of Farrah Fawcett and Michael Jackson—the world made it known that it is Web 2.0 enabled. The question is whether Web 2.0 is fully ready for the world. Both Facebook and Twitter experienced surges of activity with the announcement of the death of the King of Pop. For once, this activity trumped the security risks associated with the news event. As the world moves further into this new form of communication, malware authors and phishers are actively following along.

There are some distinct security risks that social networking sites present. Many of the risks have to do with the large number of features and applications that so many people run without a second thought. This carefree attitude has allowed various worms, phishing attacks, and other such malicious activity to come into play. For instance, there are many social networking tools that will do all sorts of things for users—from monitoring bank accounts to blocking and hiding from others. The key is that many of these "tools" require users to enter usernames and passwords. It's unfortunate that many people feel so at home with the interactive Web 2.0 experience that they forget the basics of online security. Once attackers gain access to account credentials, they have full access to the victims' friends and can launch all sorts of mischief. This phenomenon gives new meaning to the term "friendly fire."

Since its creation in 2006, Twitter has gained massive popularity worldwide. It is one of the most frequently used applications on the Internet today and has ranked as high as 27th place (by Alexa) in Internet traffic. It was only a matter of time before malware, phishing, and scams— both using and targeting Twitter and its users—began. In addition, Twitter has become commonplace in both business and consumer use; that exposure gives attackers the means to direct followers to various URLs. Due to the limited space associated with "tweeting," many methods, especially TinyURL, are wildly popular for maximizing space. (TinyURL is a web service that takes a long URL and substitutes a short alias that will redirect browsers to the full address.) Although TinyURL is a useful service, users have no clue where they are being redirected to until they attempt to access the page. Therefore, the caution that users usually apply when they view search results and news links disappears behind the obfuscating address, and they are left to the security of their gateway and desktop machines to protect them.

In April, the micro-blogging platform faced various JavaScript worm attacks exploiting a cross-site scripting (XSS) vulnerability to infect other user profiles. The first alert occurred when Twitter profiles began posting messages that encouraged people to visit StalkDaily.com, a competitor for Twitter. Mikeyy Mooney, the 17-year-old creator of this twitter clone, assumed the responsibility: "I am the person who coded the XSS which then acted as a worm when it auto updated a users profile and status, which then infected other users who viewed their profile. I did this out of boredom, to be honest. I usually like to find vulnerabilities within websites and try not to cause too much damage, but start a worm or something to give the developers an insight on the problem and while doing so, promoting myself or my website."[5]

Hours later, after Twitter said it had resolved the problem, a similar worm made its way into the community. Again, once an infected profile was viewed, it executed and injected a code in the viewer's profile that passed along the infection. Two other attacks occurred the next day, forcing the Twitter staff to delete almost 10,000 tweets spreading the worm.

A few days later, Travis Rowland, founder and CEO of exqSoft Solutions, a custom Web applications development company, confirmed that he'd offered—and that Mooney had accepted—a job with his company. This announcement is surprising and regrettable, as the writing of malicious code should serve neither as a job application nor positive credentials for employment.

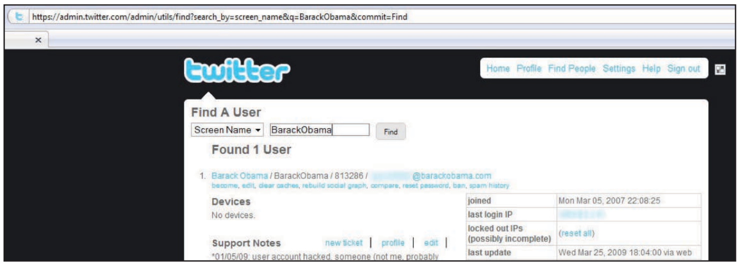
In the meantime, new copycat variants referencing celebrities have appeared.

[5] BNOnews, "17-year-old claims responsibility for Twitter worm." http://www.bnonews.com/news/242.html

Twitter hacked

For the second time this year, a hacker claims to have gained administrative access to a Twitter employee's account.[6]

In April, an anonymous French hacker called Hacker Croll posted screenshots to a French online discussion forum. The images were apparently captured while the hacker was logged in to the Twitter account of Jason Goldman, a director of product management with Twitter.



https://admin.twitter.com/admin/utils/find?search_by=screen_name&q=BarackObama&commit=Find

Find A User

Screen Name ▾ BarackObama Find

Found 1 User

1. Barack Obama / BarackObama / 813286 / [redacted]@barackobama.com
become, edit, clear caches, rebuild social graph, compare, reset password, ban, spam history

Devices
No devices.

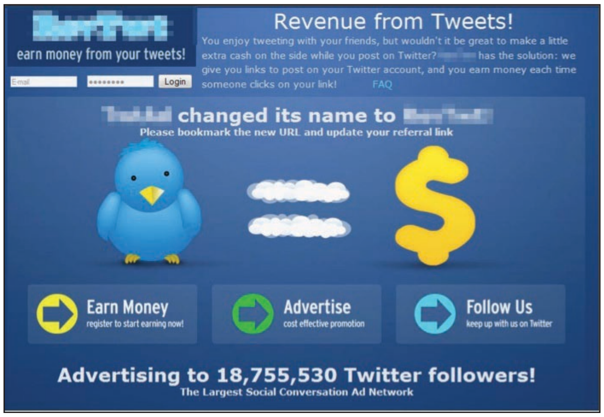
Support Notes new ticket | profile | edit |
*01/05/09: user account hacked. someone (not me, probably

joined	Mon Mar 05, 2007 22:08:25
last login IP	[redacted]
locked out IPs (possibly incomplete)	(reset all)
last update	Wed Mar 25, 2009 18:04:00 via web

Figure 15: Even Twitter Has Suffered From Hackers Gaining Access to Administrators Accounts.

Marketing or spamming tools?

If you doubt the power that Twitter offers both the present and future, you only have to search for some offers appearing on the Internet.



[redacted]
earn money from your tweets!

E-mail •••••••• Login

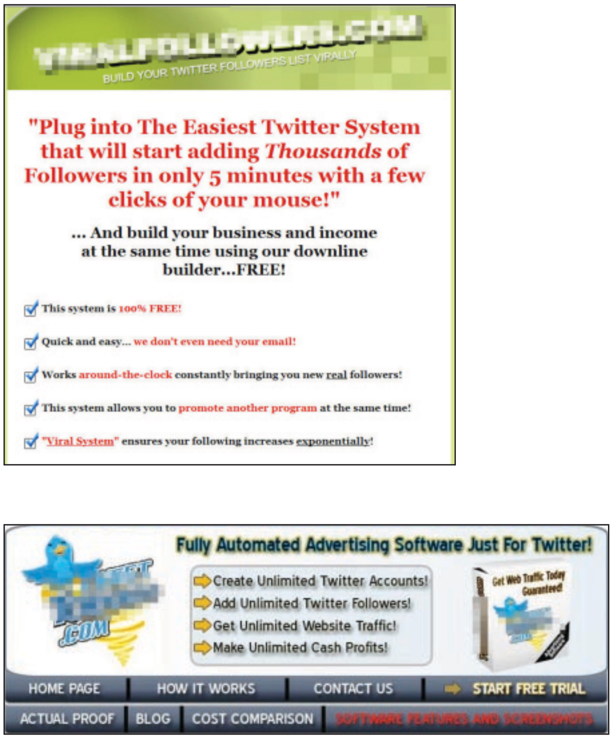
Revenue from Tweets!

You enjoy tweeting with your friends, but wouldn't it be great to make a little extra cash on the side while you post on Twitter? [redacted] has the solution: we give you links to post on your Twitter account, and you earn money each time someone clicks on your link! FAQ

[redacted] changed its name to [redacted]
Please bookmark the new URL and update your referral link

Advertising to 18,755,530 Twitter followers!
The Largest Social Conversation Ad Network

[6] Twitter, "Unauthorized Access: An Update on Security." http://blog.twitter.com/2009/04/unauthorized-access-update-on-security.html



[redacted]

BUILD YOUR TWITTER FOLLOWERS LIST VIRALLY

"Plug into The Easiest Twitter System that will start adding *Thousands* of Followers in only 5 minutes with a few clicks of your mouse!"

... And build your business and income at the same time using our downline builder...FREE!

- ☑ This system is 100% FREE!
- ☑ Quick and easy... we don't even need your email!
- ☑ Works around-the-clock constantly bringing you new real followers!
- ☑ This system allows you to promote another program at the same time!
- ☑ "Viral System" ensures your following increases exponentially!

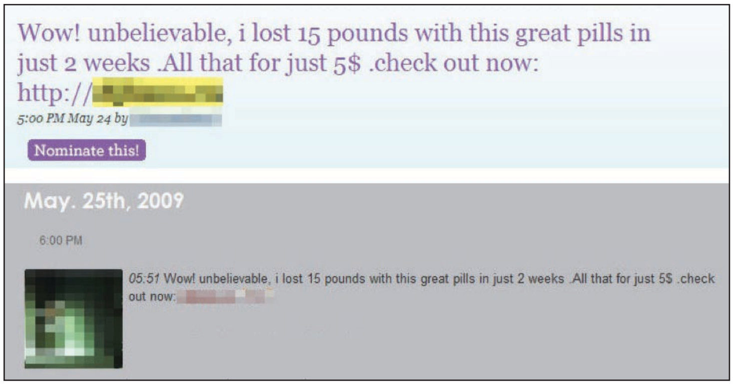
Fully Automated Advertising Software Just For Twitter!

- Create Unlimited Twitter Accounts!
- Add Unlimited Twitter Followers!
- Get Unlimited Website Traffic!
- Make Unlimited Cash Profits!

Figures 16a, 16b, and 16c: Twitter Is Full of Sales Opportunities, but Are They Marketing or Spam? Many of These Services Require Users to Divulge Login Information—That's Never a Good Idea.

Twitter spam

No doubt we'll find spam in heaven. It's already reached Twitter.



Wow! unbelievable, i lost 15 pounds with this great pills in just 2 weeks .All that for just 5$ .check out now: http://[redacted]

5:00 PM May 24 by [redacted]

May. 25th, 2009

6:00 PM

05:51 Wow! unbelievable, i lost 15 pounds with this great pills in just 2 weeks .All that for just 5$ .check out now: [redacted]

Figures 17a and 17b: Twitter Spam Delivers Familiar Messages, as These Examples Demonstrate.

Twitter a target for vulnerability research

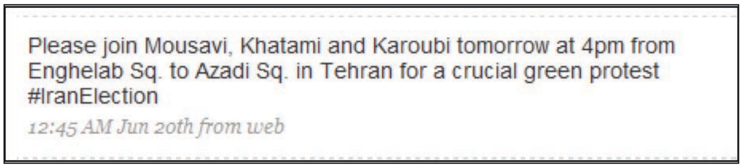
It's been a while since the "Month of Apple Bugs" or the "Month of PHP bugs," so it must be time for the "Month of Twitter Bugs" (MoTB), which is scheduled for July this year. We await the inevitable cross-site scripting (XSS) and cross-site request forgery (CSRF) flaws that put Twitter users at risk for malicious hacker attacks.

Raff Aviv, who is behind this project, wrote on his website, "Each day I will publish a new vulnerability in a 3rd party Twitter service on the twitpwn.com web site. As those vulnerabilities can be exploited to create a Twitter worm, I'm going to give the 3rd party service provider and Twitter at least 24 hours heads-up before I publish the vulnerability."[7]

We're happy to see Twitter get a little push to resolve potential holes and reduce the risk to their large user base, although 24-hours notice does not strike us as responsible disclosure. History shows us that high-traffic sites that heavily use Web 2.0 technologies will be exploited if left unpatched.

Hacktivism Returns

Twitter played a part this quarter in the aftermath of Iran's election. Twitter users transmitted information about protests against the government. Twitter was also the conduit for distributing denial-of-service attack tools and coordinating those attacks against several Iranian news sites.

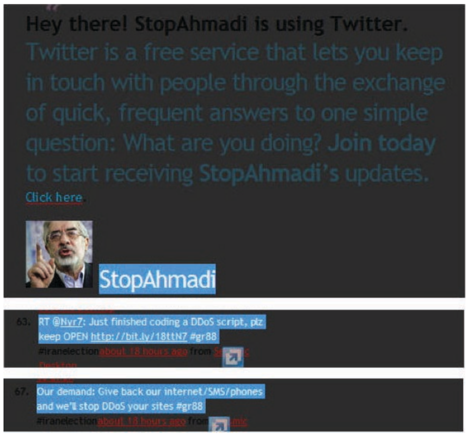


Please join Mousavi, Khatami and Karoubi tomorrow at 4pm from Enghelab Sq. to Azadi Sq. in Tehran for a crucial green protest #IranElection

12:45 AM Jun 20th from web

Figure 18: Iranians Used Twitter to Protest Against Their Regime.

Regardless of one's political leanings, the use of Twitter to disseminate information and coordinate action shows the power of social networking tools generally and of Twitter specifically.



Hey there! StopAhmadi is using Twitter.

Twitter is a free service that lets you keep in touch with people through the exchange of quick, frequent answers to one simple question: What are you doing? Join today to start receiving StopAhmadi's updates.

Click here

StopAhmadi

63. RT @Nyr7: Just finished coding a DDoS script, plz keep OPEN http://bit.ly/18ttN7 #gr88 #iranelection about 18 hours ago from Se[illegible]c Desktop

67. Our demand: Give back our internet/SMS/phones and we'll stop DDoS your sites #gr88 #iranelection about 18 hours ago from [illegible]mic

Figure 19. Twitter and Other Social Networking Tools Are a Powerful Force.

Twitter may be the current social networking darling, but it's not alone. Facebook remains a very popular service with both users and malware writers. Avert Labs continues to see an increase in the leading malware, Koobface, that targets Facebook users. (See Figure 20 below.) This malware is still one of the most prevalent threats that we track.

[7] Aviv Raff On .NET. http://aviv.raffon.net/2009/06/15/MonthOfTwitterBugs.aspx

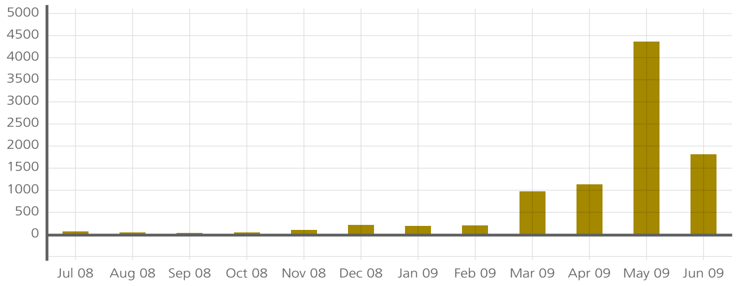


Figure 20: Unique Koobface Binaries Discovered, by Month. May Saw an Immense Jump in Threats.

Phishing

In this quarter we saw an increase in the number of phishing URLs targeting foreign banks and in foreign languages. We also see websites set up en masse that use different kits and methodologies; these kits are multilingual. For example, we found one kit that was used to generate 1,784 phishing web sites. The French version of that kit was used to generate 214 phishing sites. On May 27 we saw a tremendous spike in new phishing URLs. Many of these were spread across geographies and used various kits.

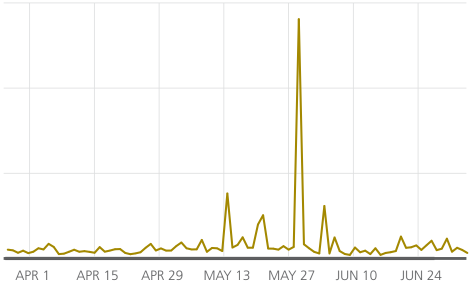


Figure 21: New Phishing Sites Discovered, by Day. On May 28 Phishers far Exceeded Their Usual Efforts.

The United States continues to host more phishing sites than any other country. Certain nations host more “risky” sites. This lineup is usually the same each time we measure.

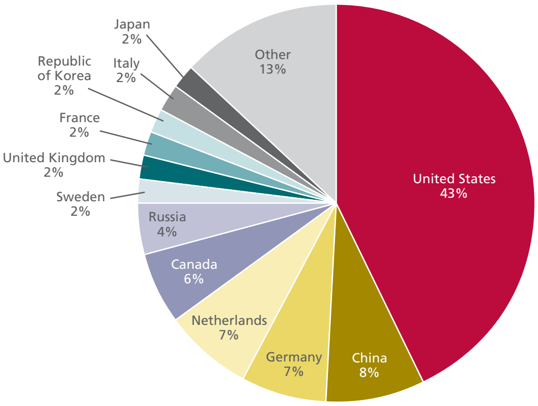


Figure 22: Distribution of Phishing Websites.

Malware: the Face of Cybercrime

In many ways, cybercrime has evolved alongside computers and how people use them. From the earliest stages of both computing and the Internet we saw malware and cybercrime, although we did not use those terms then. Viruses attacked the boot sector, were parasitic, and were distributed mainly by floppy disk. Scams and spam appeared very early as well and had the same goal they have today—to sell something. When Internet usage exploded, malware and cybercrime evolved to keep up with changes in users behavior. Many people's lives are now completely tied computer use. Whether paying bills online, blogging, or interacting with others on Facebook and Twitter, people and their identity data are now digital. Malware authors and cybercriminals fully understand this dynamic and have always kept pace with—some would say expected—this evolution. Their current set of tools and services reflects their understanding as cybercrime more and more becomes a service business.

Password-Stealing Trojans Grow Rapidly

Trojans that steal passwords continue to be one of the favorite tools of cybercriminals. The tools to create these Trojans are commonly available on the Internet and there are many sites devoted to selling them as a service. Their function is simple: They steal passwords. It is the complexity of the Trojan itself that makes it so successful.

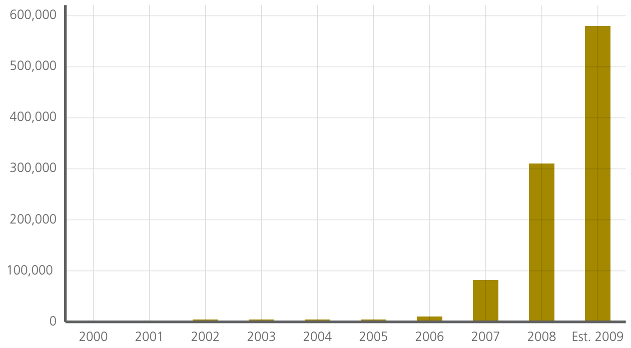


Figure 23: Growth in Password-Stealing Malware

Password-stealing Trojans most often infect users who open an email attachment that downloads malware from a malicious website. Once installed, the Trojans gather usernames and passwords from a large variety of programs, such as Internet Explorer, FTP sessions, and many online games including *World of Warcraft*. The harvested identity data is sent to a server run by cybercriminals, who then sell in a variety of ways—including auction sites or bulk sales—to a buyer.

Avert Labs has observed a growing complexity in these malicious programs. They are stealthier than ever before and often have self-protection mechanisms to insure their survival on a compromised PC. They are also becoming more general in nature. In previous years Trojans were specific to the institution they targeted. Lately, however, they have been gathering more and more data across a larger variety of targets, thus maximizing their effectiveness. Why target one bank or game when you can gather all of them?

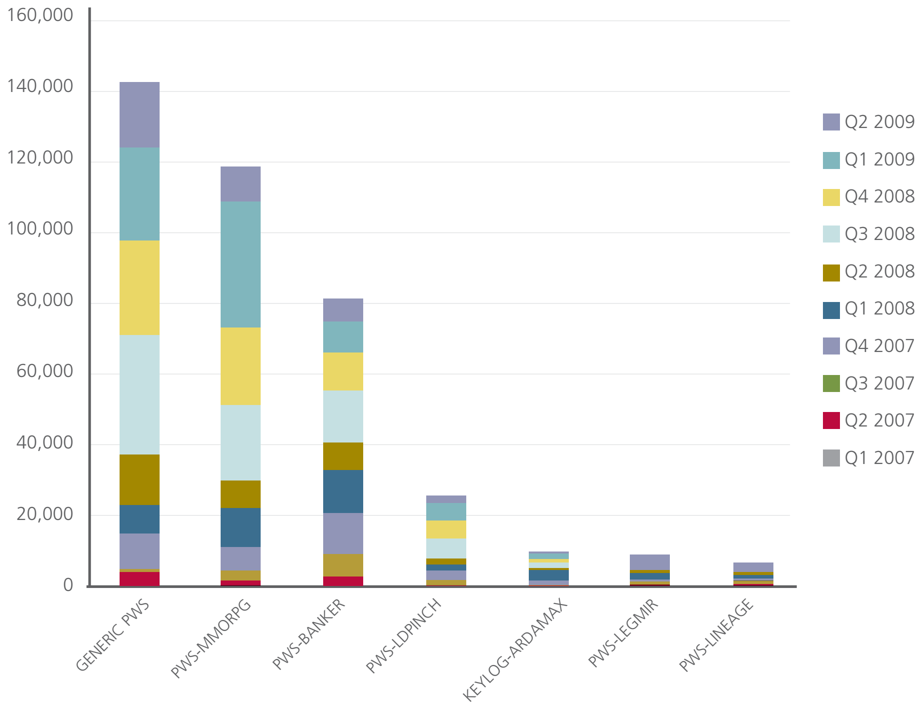


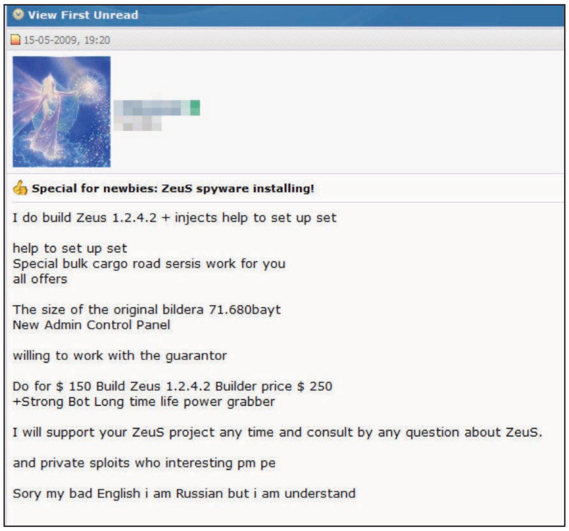
Figure 24: Leading Password-Stealing Variants, by Name and Quarter

Zeus

This god must be angry. Zeus (also known as Zbot and WSNPoem) is a builder application for creating password-stealing Trojans. It includes a control panel based on the web scripting language PHP and a Windows executable to build the malware. The produced file can steal data and credentials, capture HTTP and HTTPS traffic, capture screenshots, send its logs to a remote location, and work as a proxy server. Logs, which are encoded, can be decrypted by the builder. Zeus users can find various options, such as exploit packages and an advanced command and control interface.

Zeus enjoyed an eventful quarter:

- Version 1.2.4.x went on sale in April
- Its Russian authors increased their services for beginners. (See Figure 25.)



View First Unread

15-05-2009, 19:20

[redacted]

Special for newbies: ZeuS spyware installing!

I do build Zeus 1.2.4.2 + injects help to set up set

help to set up set
Special bulk cargo road sersis work for you
all offers

The size of the original bildera 71.680bayt
New Admin Control Panel

willing to work with the guarantor

Do for $ 150 Build Zeus 1.2.4.2 Builder price $ 250
+Strong Bot Long time life power grabber

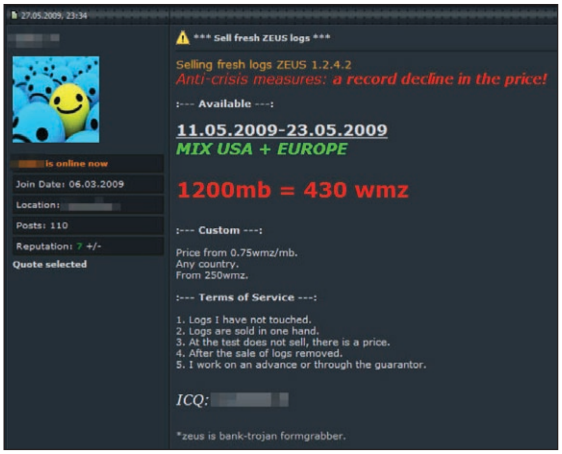
I will support your ZeuS project any time and consult by any question about ZeuS.

and private sploits who interesting pm pe

Sory my bad English i am Russian but i am understand

Figure: 25: Zeus' Authors Offer Extra Incentives.

- Roman Hüssy is a 21-year-old Swiss IT expert who runs Zeustracker, a website that lists Internet servers that use Zeus.[8] Hüssy noticed the unexpected "suicide" of 100,000 infected systems mostly located in Poland and Spain. A botmaster used the "kill operating system" routine to knock the infected machines off their Internet connections. Was this rival warfare or voluntary action to eliminate some traces? Both possibilities are plausible.[9]



27.05.2009, 23:34

[redacted]

[redacted] is online now

Join Date: 06.03.2009

Location: [redacted]

Posts: 110

Reputation: 7 +/-

Quote selected

*** Sell fresh ZEUS logs ***

Selling fresh logs ZEUS 1.2.4.2
*Anti-crisis measures: **a record decline in the price!***

:--- **Available** ---:

11.05.2009-23.05.2009
MIX USA + EUROPE

1200mb = 430 wmz

:--- **Custom** ---:

Price from 0.75wmz/mb.
Any country.
From 250wmz.

:--- **Terms of Service** ---:

1. Logs I have not touched.
2. Logs are sold in one hand.
3. At the test does not sell, there is a price.
4. After the sale of logs removed.
5. I work on an advance or through the guarantor.

ICQ: [redacted]

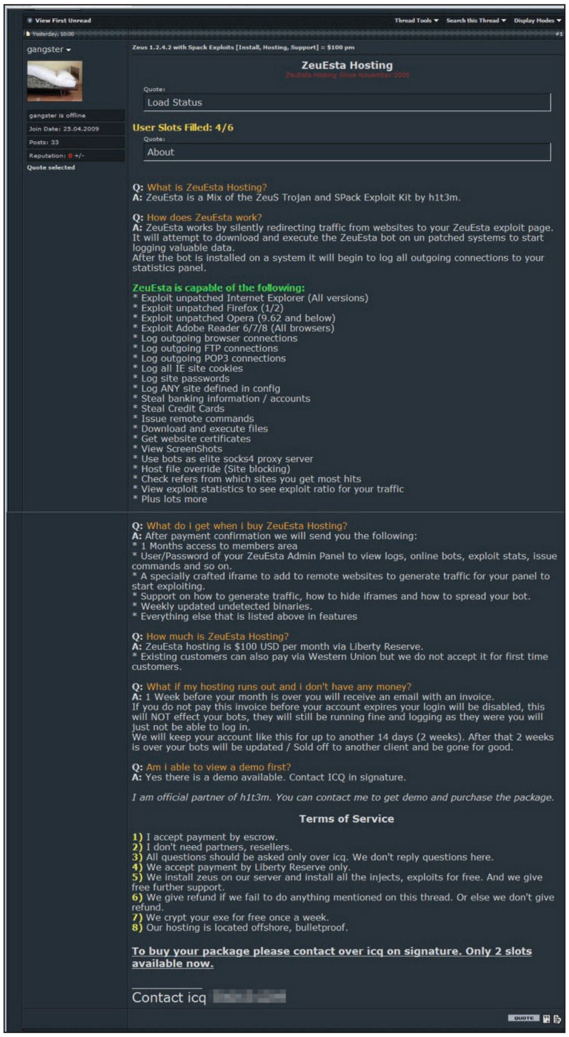
*zeus is bank-trojan formgrabber.

Figure 26: "Fresh" Zeus Logs for Sale.

- ZeuEsta came back online. Subscribers to this service receive a specific iframe that they can add to booby-trapped websites they compromise or know about. The iframe will redirect their victims to a ZeuEsta page to infect them with malware. Subscribers also gain password-protected access to a personal administration panel to view logs, online bots, exploit stats, issue commands, etc. Liberty Reserve hosts ZeuEsta for US$100 per month.

[8] https://zeustracker.abuse.ch/monitor.php?filter=online

[9] Security Fix, The Washington Post. http://voices.washingtonpost.com/securityfix/2009/05/zeustracker_and_the_nuclear_op.html



Zeus 1.2.4.2 with Spack Exploits [Install, Hosting, Support] = $100 pm

ZeuEsta Hosting

ZeuEsta Hosting Since November 2008

Quote:

> Load Status

User Slots Filled: 4/6

Quote:

> About

Q: What is ZeuEsta Hosting?
A: ZeuEsta is a Mix of the ZeuS Trojan and SPack Exploit Kit by h1t3m.

Q: How does ZeuEsta work?
A: ZeuEsta works by silently redirecting traffic from websites to your ZeuEsta exploit page. It will attempt to download and execute the ZeuEsta bot on un patched systems to start logging valuable data.
After the bot is installed on a system it will begin to log all outgoing connections to your statistics panel.

ZeuEsta is capable of the following:
* Exploit unpatched Internet Explorer (All versions)
* Exploit unpatched Firefox (1/2)
* Exploit unpatched Opera (9.62 and below)
* Exploit Adobe Reader 6/7/8 (All browsers)
* Log outgoing browser connections
* Log outgoing FTP connections
* Log outgoing POP3 connections
* Log all IE site cookies
* Log site passwords
* Log ANY site defined in config
* Steal banking information / accounts
* Steal Credit Cards
* Issue remote commands
* Download and execute files
* Get website certificates
* View ScreenShots
* Use bots as elite socks4 proxy server
* Host file override (Site blocking)
* Check refers from which sites you get most hits
* View exploit statistics to see exploit ratio for your traffic
* Plus lots more

Q: What do i get when i buy ZeuEsta Hosting?
A: After payment confirmation we will send you the following:
* 1 Months access to members area
* User/Password of your ZeuEsta Admin Panel to view logs, online bots, exploit stats, issue commands and so on.
* A specially crafted iframe to add to remote websites to generate traffic for your panel to start exploiting.
* Support on how to generate traffic, how to hide iframes and how to spread your bot.
* Weekly updated undetected binaries.
* Everything else that is listed above in features

Q: How much is ZeuEsta Hosting?
A: ZeuEsta hosting is $100 USD per month via Liberty Reserve.
* Existing customers can also pay via Western Union but we do not accept it for first time customers.

Q: What if my hosting runs out and i don't have any money?
A: 1 Week before your month is over you will receive an email with an invoice.
If you do not pay this invoice before your account expires your login will be disabled, this will NOT effect your bots, they will still be running fine and logging as they were you will just not be able to log in.
We will keep your account like this for up to another 14 days (2 weeks). After that 2 weeks is over your bots will be updated / Sold off to another client and be gone for good.

Q: Am i able to view a demo first?
A: Yes there is a demo available. Contact ICQ in signature.

I am official partner of h1t3m. You can contact me to get demo and purchase the package.

Terms of Service

1) I accept payment by escrow.
2) I don't need partners, resellers.
3) All questions should be asked only over icq. We don't reply questions here.
4) We accept payment by Liberty Reserve only.
5) We install zeus on our server and install all the injects, exploits for free. And we give free further support.
6) We give refund if we fail to do anything mentioned on this thread. Or else we don't give refund.
7) We crypt your exe for free once a week.
8) Our hosting is located offshore, bulletproof.

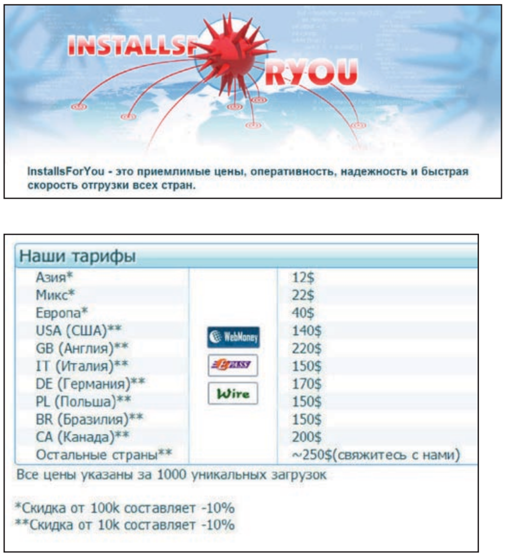
To buy your package please contact over icq on signature. Only 2 slots available now.

Contact icq [redacted]

Figure 27: The ZeuEsta Service Makes It Easy for Cybercriminals to Get Into the Business.

Crimeware as a Service

The Zeus story demonstrates the evolution toward more service in cybercrime. "If you have the malware, they have the vulnerable computers!" Some cybercriminals will install malware written by others on compromised machines they control.



InstallsForYou - это приемлимые цены, оперативность, надежность и быстрая скорость отгрузки всех стран.

Наши тарифы

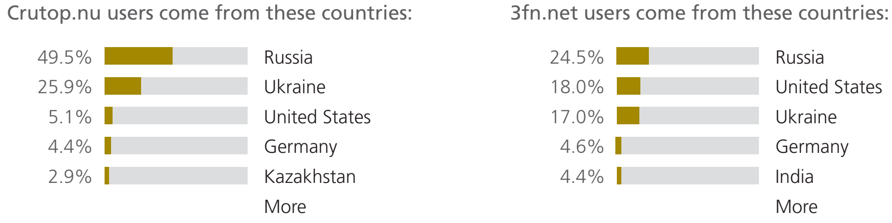
Азия*		12$
Микс*		22$
Европа*		40$
USA (США)**	WebMoney	140$
GB (Англия)**	EPASS	220$
IT (Италия)**	Wire	150$
DE (Германия)**		170$
PL (Польша)**		150$
BR (Бразилия)**		150$
CA (Канада)**		200$
Остальные страны**		~250$(свяжитесь с нами)

Все цены указаны за 1000 уникальных загрузок

*Скидка от 100k составляет -10%
**Скидка от 10k составляет -10%

Figures 28a and 28b: Just $140 Will See Your Malware Installed on 1,000 Computers.

The Federal Trade Commission has successfully stopped another cybercriminal. The rogue internet service provider Pricewert LCC, using many names including 3FN.net, Triple Fiber Network, and APS Communications, has been shut down by FTC. According to the feds, this company recruited, knowingly hosted, and actively participated in the distribution of spam, child pornography, and other harmful electronic content. Searching at the Oregon Secretary of State's Corporate Division website, we found that Pricewert was registered in Portland in September 2003, with two Belize companies listed as members. In its memorandum, the FTC itemizes the illegal contents hosted by 3FN: malicious botnet software, child pornography, fake anti-virus products, illegal online pharmacies, and pirated music and software.[10] The FTC explains how the 3FN staff used the crutop.nu forum to recruit new customers. Querying Alexa.com shows us that Russians and Ukrainians are the main visitors to these sites.



Figures 29a and 29b: The FTC Shut Down a Rogue ISP Whose Illegal Activities Attracted Interest Primarily From Russia and Ukraine.

[10] United States District Court, Northern District Of California, "Memorandum of Points and Authorities in Support of Plaintiff's Motion for an *ex parte* Temporary Restraining Order and Order to Show Cause." http://www.ftc.gov/os/caselist/0923148/0906043fnmemotro.pdf

AutoRun Malware

USB and flash memory–based malware (also called AutoRun malware) continue to be one of the most prevalent families of malware that Avert Labs sees each day. Users love their handy devices and malware writers love user data. When we take into account the types of devices that AutoRun malware can infect—USB sticks, digital picture frames, and larger storage devices—the danger to both consumer and enterprise user data cannot be understated. To learn more about AutoRun infections and how to combat them, read our report *The Rise of AutoRun-Based Malware*, by Avert Labs researchers in our Bangalore, India, offices.[11]

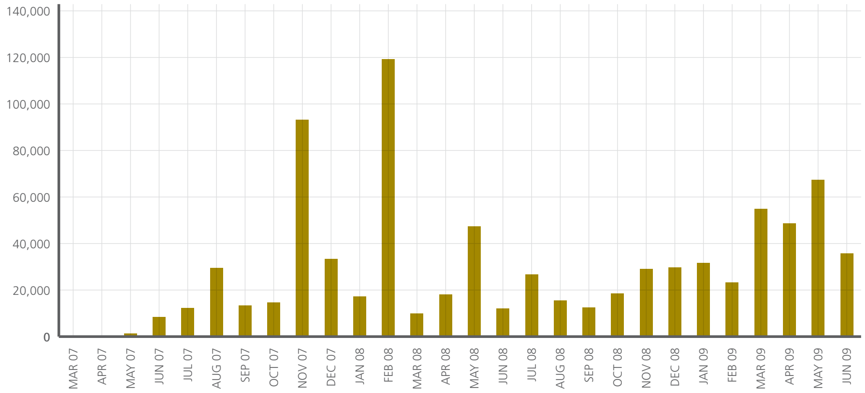


Figure 30: Unique AutoRun Malware Binaries Discovered, by Month.

In Figure 30 we can see that in some months there are large jumps in new AutoRun malware versions. In spite of the up and down, the overall trend is on the rise. AutoRun functionality provides malware writers with significant convenience. (It saves a couple of clicks.) This Windows feature has single-handedly revived the 1980s model of hand-carried malware propagation. Prevalent Trojan families such as PWS-OnlineGames and PWS-Gamania, which previously required a user to click an executable, now use the AutoRun vector to spread via removable drives. Parasitic virus families such as W32/Sality and W32/Virut have also incorporated this infection vector with some success.

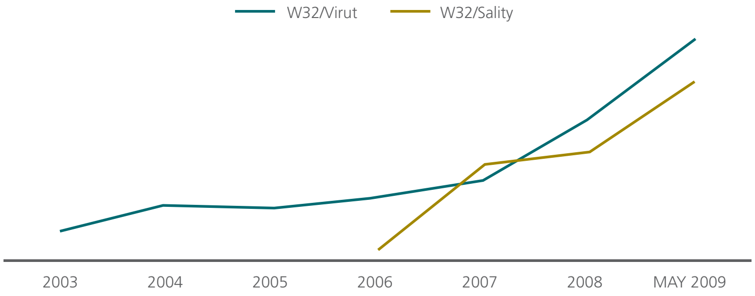
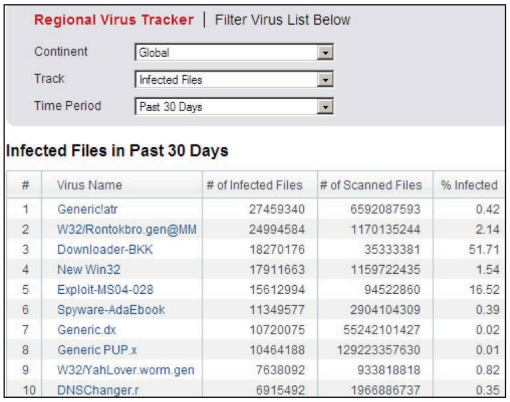


Figure 31: Parasitic USB Growth for the W32/Sality and W32/Virut Viruses.

We continue to observe an alarming increase in malware using AutoRun as an infection vector. Here's an example of how rampant the problem of AutoRun malware is: Figure 32, below, is data from the McAfee global virus map, which tracks statistics of detections observed on computers running McAfee anti-virus software.

[11] http://www.mcafee.com/us/local_content/white_papers/wp_autorun_malware_v8_en.pdf



Regional Virus Tracker | Filter Virus List Below

Continent: Global

Track: Infected Files

Time Period: Past 30 Days

Infected Files in Past 30 Days

#	Virus Name	# of Infected Files	# of Scanned Files	% Infected
1	Generic!atr	27459340	6592087593	0.42
2	W32/Rontokbro.gen@MM	24994584	1170135244	2.14
3	Downloader-BKK	18270176	35333381	51.71
4	New Win32	17911663	1159722435	1.54
5	Exploit-MS04-028	15612994	94522860	16.52
6	Spyware-AdaEbook	11349577	2904104309	0.39
7	Generic.dx	10720075	55242101427	0.02
8	Generic PUP.x	10464188	129223357630	0.01
9	W32/YahLover.worm.gen	7638092	933818818	0.82
10	DNSChanger.r	6915492	1966886737	0.35

Figure 32: McAfee's Global Virus Map Puts AutoRun Malware (Called Generic!atr in This List) at the Top of the Heap.

Last quarter the Conficker worm attracted lots of interest from the press. But its significance paled when compared with AutoRun detections, as we reported in our last issue. Although there has been a slight increase in Conficker activity this quarter, it can't touch AutoRun's prevalence.

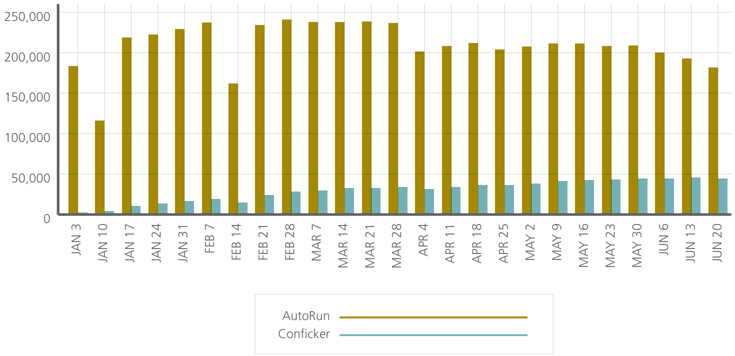
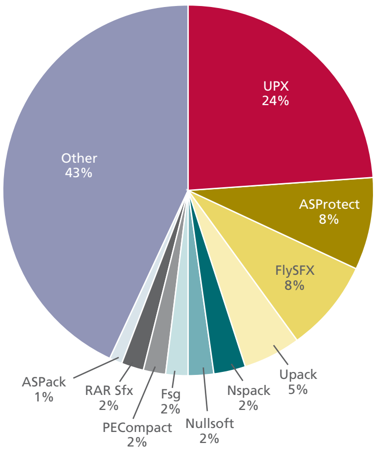
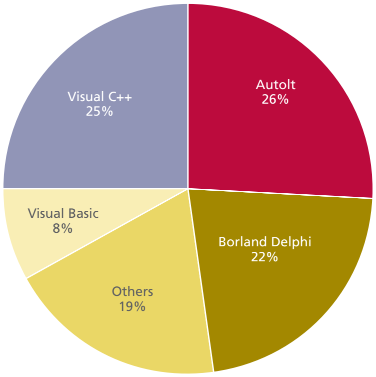


Figure 33: AutoRun Infections Continue to Dwarf Those of the Conficker Worm, in Spite of the Latter's Heavy Media Coverage.

We found AutoRun malware in more than 27 million infected files during a 30-day period this quarter, making it the number-one piece of malware detected globally. Given the millions of computers on the Internet and other security vendor detections of AutoRun-based threats, one can understand how rampant the problem is. The compilers and packers used to create the vast percentage of this family of malware are readily available, and are often the same tools that legitimate software producers use.





Figures 34a and 34b: The Prevalence of Legitimate Packers (top) and Compilers (bottom) During the Quarter Makes It Easy for Attackers to Prepare AutoRun Worms for Distribution.

What conclusions can we draw from the popularity of UPX and AutoIt for creating AutoRun malware? The short answer is that they are free, open-source programs. The source code for creating AutoIt-based worms, for example, is widely available on the Internet; furthermore, files compiled with AutoIt Versions 3.2x and earlier can be easily decompiled to the original script. That's very handy for making new and updated malware versions.

Microsoft has addressed many prevalent infection vectors in the past—such as spreading via boot sectors, office macros, scripts, and email clients—through enhanced security features. With AutoRun-based infections on the rise, Microsoft could make a world of difference by fixing this exploited convenience feature in future Windows updates.

About McAfee Avert Labs

McAfee Avert Labs is the global research group of McAfee, Inc. With research teams devoted to malware, potentially unwanted programs, host intrusions, network intrusions, mobile malware, and ethical vulnerability disclosure, Avert Labs enjoys a broad view of security. This expansive vision allows McAfee researchers to continually improve security technologies and better protect 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®

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