Report

McAfee Threats Report: First 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: http://www.mcafee.com/us/threat_center/default.asp, or www.trustedsource.org.

In the first quarter of 2009, we have seen many significant changes in the threat landscape compared with what we saw a year or even a few months ago. No one would have predicted twelve months ago that spam volumes would fall, but with the McColo shutdown in November 2008, that is exactly what happened. Spam levels are still 30 percent below their peak levels, and we did not see the increase that historically occurs in March. The question is not *whether* spam will return to previous levels, but rather *when* it will return. There is data regarding new zombie and botnet creation that suggest the time may not be too far in the future.

The creation of malicious websites is increasing, as are sites that host malware—with thousands of new sites appearing daily. New forms of malware are being created every day, and this report details those that have reached the highest levels of prevalence.

The Conficker worm, officially W32/Conficker.worm, has received as much attention as any security threat in recent history. This report will provide some perspective as to whether this attention is hype or reality. We will also focus on threats that do not receive the same level of media attention, but that in fact could be more dangerous than their more popular counterpart.

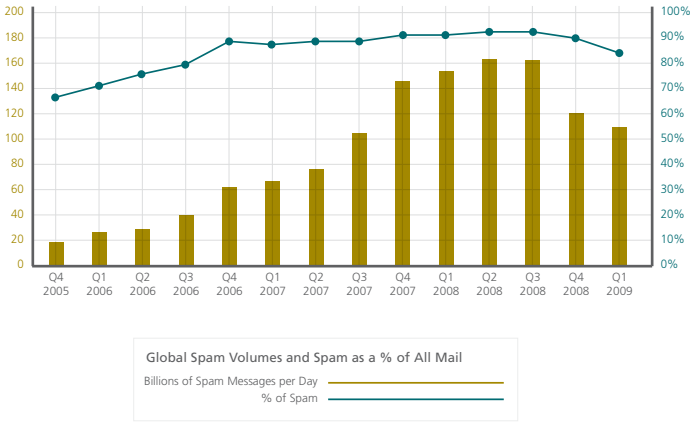
The geography of the threat landscape continues to evolve. This report offers analysis of the geographical contributions to threats—including spam origin, zombie creation, and malware site locations as well as identifying the emerging players in the threat-creation business. The report also provides some interesting details that suggest that countries creating threats do not mind using them against entities within their borders.

Finally, we turn the camera on ourselves and take a look at a few of the predictions we made in our *2009 Threat Predictions* report, published in January, and see whether or how they are materializing. The highlights include the use of current events and social networking sites to propagate threats to unsuspecting users.

Spam: Still a Global Concern

What recession?

Overall email and spam volumes for the first quarter of 2009 are at levels that we have not seen for almost two years. Have spammers followed the rest of the economy and fallen on tough economic times? That's not really the issue. What's actually going on is that spam levels have not yet fully recovered from the McColo shutdown, which took place in November 2008. Compared with the same quarter a year ago, volumes are 20 percent lower in 2009 and 30 percent below the third quarter of 2008, which had the highest quarterly volumes recorded to date. Spam volumes have recovered about 70 percent since the spam host went offline, but they have not yet reached their former levels.



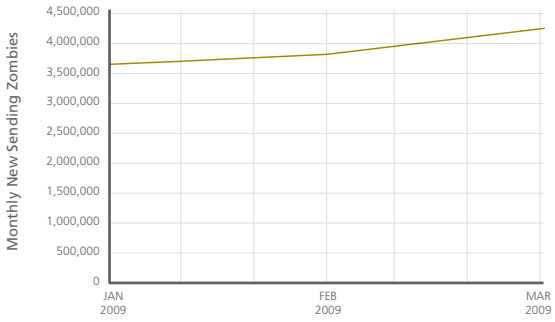
The month of March in recent years has set email volume records, but this March is well off the pace. Last year we saw an average of 153 billion messages per day, while this March averaged only about 100 billion messages per day.

Spam as a percent of total mail has decreased below the 90 percent mark; we've not seen that level since 2006. For all of 2008, we measured spam at 90 percent of total email volume, while the most recent quarter measured 86 percent. Although email accounts and their activity vary greatly, we estimate that individuals are receiving between six and twelve fewer emails per day compared with last year.

We fully expect spam volumes to regain their 2008 levels, but the ability of spammers to reorganize their command centers and botnets after the shutdown has taken longer than many predicted when the takedown first occurred. Ultimately for the spammers, this is an issue of return on investment, as in any business.

New zombies crank up the production line

In this quarter, we detected nearly twelve million new IP addresses operating as "zombies," computers under the control of spammers and others. This is a significant increase over the levels from the last quarter of 2008, with an increase of nearly 50 percent. The third quarter of 2008 also posted a record number of new zombies, but it was exceeded this quarter by one million. And although the spam volume levels have not yet recovered from the McColo shutdown, the activity level of new zombies indicates that the spammers are working hard to regain the infrastructure lost and that volumes will return to previous levels sometime soon.



We can break down the infected systems by country. For the most recent quarter, 63 percent of the new zombies were accounted for by the top 10 countries. This figure represents a small decrease from the prior two quarters. It appears that spammers are reaching out to machines in more countries to fuel their efforts.

Q1 2009		Q4 2008		Q3 2008	
Country	Percent of IPs	Country	Percent of IPs	Country	Percent of IPs
United States	18.0	China	15.8	China	20.4
China	13.4	United States	15.4	United States	16.5
Australia	6.3	Germany	6.5	Germany	6.8
Germany	5.3	United Kingdom	6.0	United Kingdom	6.0
United Kingdom	4.7	Brazil	4.9	Brazil	4.8
Brazil	4.0	Spain	4.3	Spain	3.7
India	3.1	Australia	4.1	India	2.5
Spain	3.0	Italy	3.5	Russia	2.4
South Korea	2.8	Russia	3.1	South Korea	2.4
Russia	2.5	South Korea	2.4	Italy	2.2
Total	**63.3**	**Total**	**66.0**	**Total**	**67.5**

China and the United States have been jostling for the top spot over the past three quarters and dominate in the number of zombie machines under the control of spammers. One notable mover is Australia, which failed to make the top 10 in the third quarter of 2008. In two quarters it has rocketed up to the number three spot, accounting for six percent of all new zombies. The "Land Down Under" is proving to be fertile ground for zombie recruiting.

Q1 2009		Q4 2008	
Country	%of Total	Country	%of Total
United States	35.0	United States	34.3
Brazil	7.3	Brazil	6.5
India	6.9	China	4.8
South Korea	4.7	India	4.2
China	3.6	Russia	4.2
Russia	3.4	Turkey	3.8
Turkey	3.2	South Korea	3.7
Thailand	2.1	Spain	2.4
Romania	2.0	United Kingdom	2.3
Poland	1.8	Colombia	2.0
	70.0		**68.3**

Spam by Country: United States Is Again a World Leader

U.S. automakers may be struggling with manufacturing and sales problems, but spam production from the United States continues to lead the world, accounting for 35 percent of global spam output. Although spam command-and-control operations are an international infrastructure, spammers still favor using computers from the United States to manufacture spam. The top 10 countries dominate in spam production, contributing nearly 70 percent of the total and far outdistancing the other 200-plus countries in the world.

Looking at the last two quarters, we see that India has shown the greatest percentage increase, now contributing nearly seven percent of the global spam. Their spam output has doubled from the previous quarter. Perhaps spam is the latest industry to try its hand at outsourcing to India.

We also welcome Thailand, Romania, and Poland to the top 10. This data supports the notion that spammers are looking high and low for new sources of horsepower for their spam engines.

Q1 2009		Q4 2008		Q3 2008	
Prescription drug	25.0	Prescription drug	37.0	Male enhancement	31.2
Advertising	21.9	Advertising	19.3	Advertising	19.3
Product replica	18.8	Male enhancement	16.8	Prescription drug	10.7
Male enhancement	17.5	DSN	9.5	Storm	8.0
DSN	7.1	Dating	3.9	DSN	7.7
Storm	1.6	Product replica	2.6	Breaking news	6.7
Diploma	1.1	Employment	1.7	Product replica	6.0
Software	1.1	Software	1.5	Debt loan	1.6
Debt loan	1.0	Debt loan	1.2	Banking	1.1
Other	4.9	Other	6.5	Other	7.7
	100.0		**100.0**		**100.0**

Spam by type: sex, drugs, and lots more

Male enhancement, prescription drug, and general advertising spam continue to score near the top among the types of spam sent. These three types alone account for approximately 60 percent of the spam sent during the past three quarters. It seems like the cultural slogan "sex, drugs, and rock 'n' roll" lives on through spam. Well, almost. Perhaps we have grown up to some extent; today the phrase could be "sex, drugs, and economics."

Product replica spam (mostly counterfeit watches) made a large jump this quarter, contributing nearly 19 percent of total spam. This type of replica spam has been popular for the past year, but has also shown significant growth this quarter. This suggests that in tough economic times spammers are helping us extend our buying power by finding some nice bargains on cheap knockoffs.

Delivery status notification spam continues to steadily account for eight percent of total spam. These messages are almost always associated with phishing attacks and occur as an apparent bounce notification after the victim's email addressed has been spoofed. Clearly phishing is still alive and well. Many of these message are financially related and an attempt to get a person's personal information.

Spammers respect no country's sovereignty—including their own

There is a myth in the cybersecurity community that online criminals, a significant number of which are believed to reside in Eastern Europe, prefer to focus on targets in Western countries and shy away from attacking people or companies in their local jurisdiction. We are starting to see data that belies this myth. The Internet knows no geographical boundaries. It is now apparent that cybercriminals will attack any target of opportunity they can find. We have seen evidence that cybercrooks have deeply compromised some key Russian and Eastern European government agencies and corporations, as well as top officials at those entities.

McAfee TrustedSource™ recently has observed malware-laden email and spam originating from a variety of government agencies and banking institutions in Russia. According to our analysis, the compromised Russian banks include:

- Rusfinance Bank
- OGO Bank
- Tusarbank
- Link Capital Investment Bank
- The Maritime Bank
- Vladivostok Alfa Bank
- Bank Eurotreid
- Bank Voronezh
- Bashcreditbank
- Enisey's United Bank
- Inter-Svayz Bank

Our data also suggests that computer systems in the following Russian government offices are controlled by cybergangs:

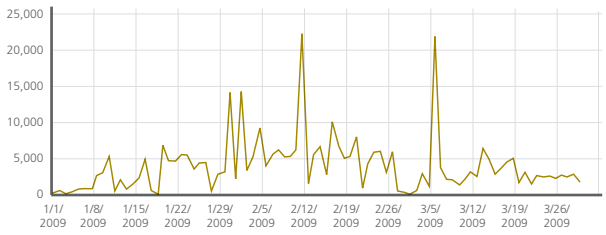
- Ministry of Taxation, Nazran region
- Russian State Internet Network
- Regional Finance & Economy Institute
- Joint Institute for Nuclear Research
- Medical Center of Russian Federation President's Department
- Pension Fund of the Russian Federation
- Personal Network for the Russian Federation Justice
- JSC Chechen Cellular Communication

This data for Russia suggests online criminals are largely indiscriminate about their targets and will attack any organization of financial or other interest to them. Although Russia clearly leads the way in this type of activity (and the sheer volume of spam they produce), our analysis shows the same type of activity other former Soviet Union countries, including Ukraine, Belarus, Armenia, Azerbaijan, Georgia, Kazakhstan, Kyrgyzstan, Moldova, Tajikistan, Turkmenistan, and Uzbekistan.

Web: New Sites with Malicious Reputations Appear Daily

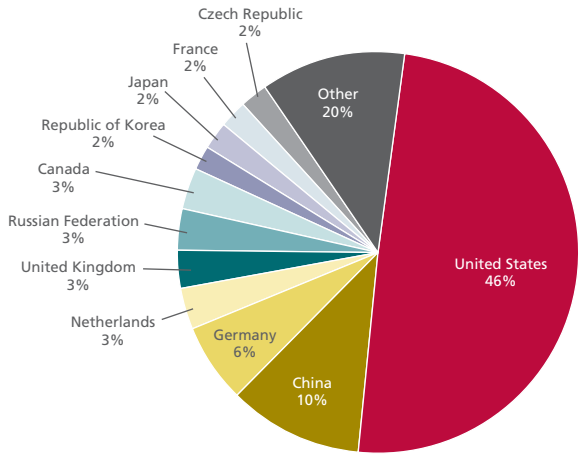
During the course of this quarter we have seen the continuation of many of the threats that presented themselves during the last quarter of 2008—but with greater intensity. Although most of the media hype and attention has been on Conficker, it was by no means the only prevalent threat during this quarter. Even if we overlook Conficker activity, we still saw a slight increase in activity year over year and a definite increase from previous quarters. Rogue anti-virus applications were an issue that caused quite a bit of concern on the web as well as increases in scams and phishing activity.

The malicious domains that Conficker was to contact are not included in any of the daily charts or data in this section, except for within the chart "Distribution of Websites with Malicious Reputations." Although the Conficker data is an important part of the threat picture, it dilutes the full story of malicious activity. There are many other threats present that are growing in prevalence. Malware authors and scammers are taking advantage of economic concerns and our worries to push a variety of scam sites. Their pitches include avoiding mortgage foreclosure and phishing sites on everything possible; they even offer store rewards cards. Rogue anti-virus sites continue to prey upon unsuspecting users. And the methods of attracting users to websites continue to evolve. Even discounting all of the Conficker activity, URLs crossing the line into "malicious" (or "red") reputation levels have noticeably increased as compared with the final two quarters of 2008.



Daily New Websites with Malicious Reputations

Where are these URLs with bad web reputations located? Not where most people think.



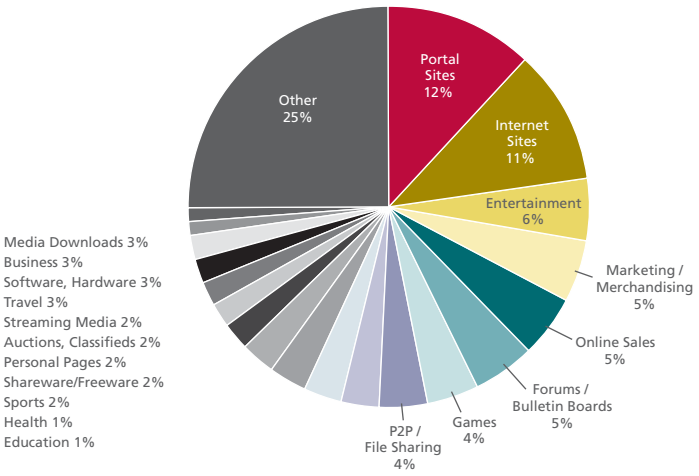
Distribution of Websites with Malicious Reputations

Why the sudden shift in what we have previously considered the "norm" (a top three of the United States, China, and Russia) regarding malicious web activity?[1] This does not mean that some of these countries have fewer URLs with malicious reputations. Rather, we see increased growth within other countries. Much of this growth relates to where Conficker has hosted some of the domains that it is planning to contact or has contacted. In fact, the Conficker contribution alone brought the Netherlands into a tie for fourth place. Although the Netherlands has long been a popular choice for hosting phishing URLs, Conficker provided a significant jump in malware-infected websites and other malicious content. However, the shift cannot be entirely attributed to Conficker. Canada has worked its way into the top 10 of hosting malicious web servers due to the variety of malware and spyware available from these sites.

One important lesson is that these same countries show up across multiple attack vectors—malicious sites, sites hosting spyware/adware, phishing, and spam. The top seven countries hosting websites with a malicious reputation are also in the top 10 hosting phishing, spam, and malware/spyware sites.

Sites with malicious reputations vary considerably in their aims, whether legitimate, shady, or scams. You'll still run a higher risk when visiting a porn or gambling site that is not associated with a recognized and legitimate business. However, any site is vulnerable, and any type of content that a user may want to access is an opportunity for malware distributors to exploit.

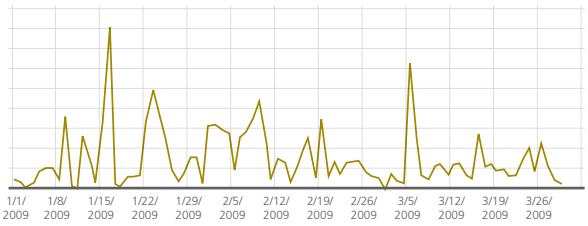
1. In the third quarter of 2008, the ranking order was the United States with 41 percent, China with 12 percent, Russia with 7 percent, Germany and the Netherlands with 5 percent, South Korea with 4 percent, Hong Kong with 3 percent, Taiwan, Canada, and the Czech Republic with 2 percent, and others with 17 percent.



Top 20 Legitimate Categories Earning Trusted Source's 'Malicious Website' Reputation

This quarter, content servers have increased in popularity with malware distributors as a tool for malicious and illegal content. We've seen this trend across sites that are located and run by reputable and highly respected providers as well as those that are lesser known and more questionable. Combining this threat with the widespread use of blogs and search engine optimization, it is more critical than ever for every computer to have full web security.

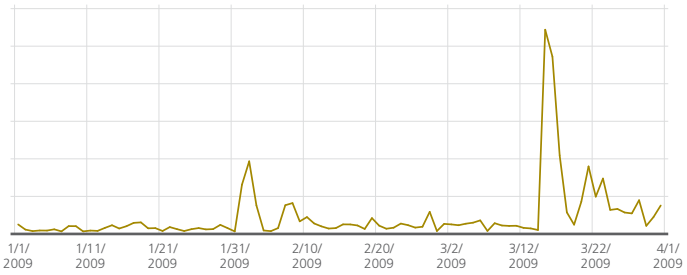
We have touched on the *where*, now let's discuss the *types* of threats we've seen. Beyond Conficker, this has been a busy quarter for new malware and exploits available on the web.



New Websites Delivering Malware and PUPs

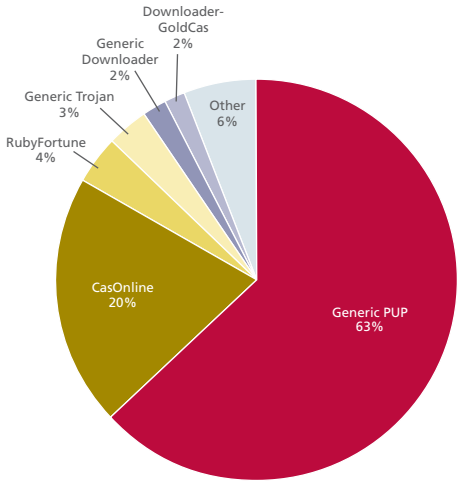
The chart above provides a picture of the number of websites delivering malware and potentially unwanted programs (PUPs) that were detected this quarter by the McAfee TrustedSource network. (The chart shows sites that actually host malware and reflects user traffic to those sites. The chart does not include legitimate sites that are exploited into directing users to malware sites. Also, in this chart we have removed our proactive research to provide a true picture of the unique, new threats available during the course of standard browsing—whether at school, work, or home.)

In contrast, the charts below illustrate what our proactive methodology has found regarding unique, new malware downloads that were being served by various websites. We have some interesting spikes from new exploits or when we found "gold mines" of malicious downloads and PUPs.



Malware and PUPs Downloads, Identified Proactively by Day

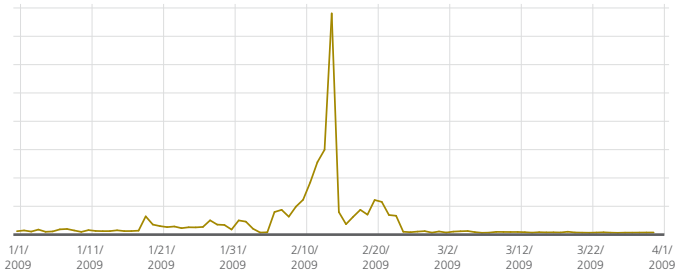
Our proactive observations—regular crawling and verification of websites plus unique methods for mining for further malicious information—showed a huge spike in new casino-related malware downloads around the end of January and beginning of February, as well as a spike in generic PUPs around the end of the quarter. This activity accounted for the top four malware download types during the quarter. (See the next chart.) Another malware of interest is the ongoing presence of the Vundo Trojan, which became more active in the past three months.



Malware and PUPs Download Prevalence, by Type

One of the amorphous web threats we face is the *exploit*, a term that can mean many, and often differing, things to researchers and users. Avert Labs tracks new pages that host browser exploits as we crawl and monitor the web, and we regularly identify new browser security vulnerabilities. When browsers (and their plug-ins) are not kept up to date, these "sandboxes" can easily become a malware author's playground. Once this author becomes king of the hill, the user's computer may receive programming code that allows adware infections, keystroke spying, and other malicious activities.

When browsers (and their plug-ins) are not kept up to date, these "sandboxes" can easily become a malware author's playground.

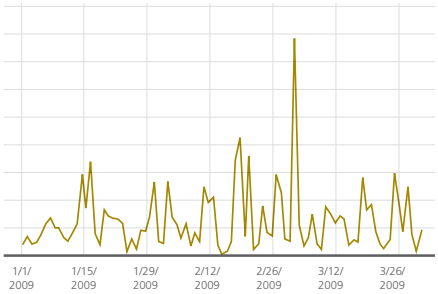


Websites Discovered Hosting Browser Exploits

Anonymizer activity

Malware authors are boosting their use of redirected-URL attacks, whether via an anonymizer or a Web 2.0 interface using a content server. This may be to avoid standard detection (by acting as an embedded URL instead of a source URL) or to benefit from the reputation of the site that appears to deliver the malware.

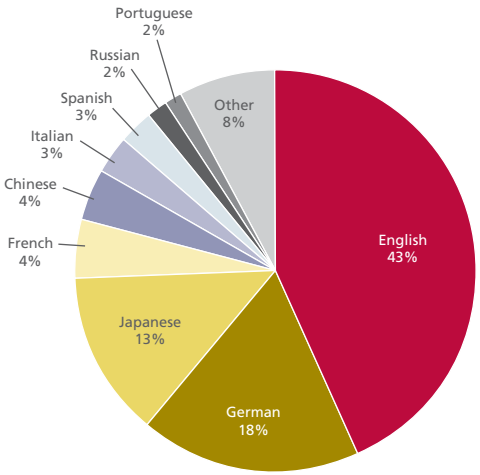
An anonymizer is a tool that hides a user's identity while online. Most anonymizers are not malicious and thus are not included in our previous discussions of security risks. However, using one may open the door to a "man in the middle" attack, in which a malicious or hijacked anonymizer injects code into messages traveling, in either direction, between user and server. This not only puts the user at risk but also endangers hosts and networks that would otherwise be protected. Overall, anonymizer activity has increased this quarter compared with last quarter. There was also a slight increase in year over year activity for this quarter.



New Anonymizers per Day

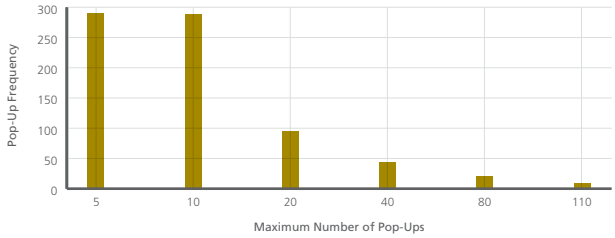
General web trends

The web is a global community. Just look at the connections across any professional- or social-networking site. Web pages continue at a steady pace to support more languages. The same blog attacks that show up on high-profile sites in the United States are also distributed via Chinese blogs, Brazilian blogs, and many others. And today's attacks employ a widespread net. In addition, as malware distributors take advantage of brand awareness such as leading sports events and the use of malware embedded in tournament brackets and player JPGs, they are using global brands to hit audiences across all languages.



Distribution of Languages in Web Content

The annoyance factor of pop-up screens has not diminshed. It is interesting that despite pop-up blockers and similar tools most websites still use them. The maximum number of pop-ups we saw on one website was 116.



Distribution of Pop-Ups in Sites With at Least Five

We continue to see widespread use of legitimate Web 2.0 and business-related URLs for spreading malware. Ten or more years ago, it seemed you could remain safe by simply staying away from certain content, but today threats seem to find us regardless of where we browse. Any website that can be exploited (via any of numerous vulnerabilities) will be. Administrators routinely see scans looking to exploit their servers. What is interesting is the high prevalence of these scans coming from sites and servers associated with everything from illegal software to malicious sites to anonymizers. If a high-traffic website is vulnerable, then it is not a matter of whether it will be exploited, but when.

Businesses on the web need to be treated with the same scrutiny as one would apply to a door-to-door salesman.

We've seen a marked increase in scams on the web. We expect this will increase as the con artists feed on the worries of the global population via spam email and the web. It is often very hard to discern whether an organization is legitimate. Businesses on the web need to be treated with the same scrutiny as one would apply to a door-to-door salesman. Users need to know that once they provide a scammer with credit card information for an online donation or fake service—that data is gone.

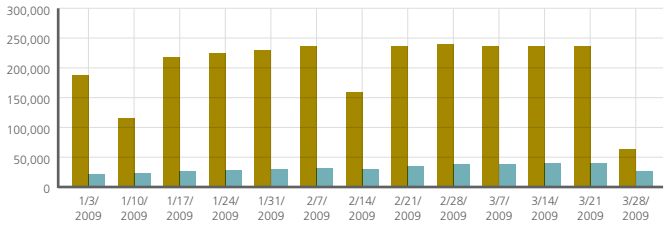
However, our research does show some hope for the economy. Real estate sites have shown a marked increase in growth this quarter, cracking the top 10 categories of content available to users (and pushing sports out of the top group).

Malware: Conficker Hype versus AutoRun Realities

The last several months have been full of stories about Conficker. You would imagine it was the only threat worth worrying about. However, when we look at the numbers, we see a different picture. Conficker is not exactly doomsday.

Conficker has indeed been an important piece of malware for many reasons. It has infected numerous hosts. It has been actively developed, maintained, and discussed. But the actual detections are not as great as one would assume from a malware that has received this much attention.

On the other hand, we have seen malware this quarter that is worrisome. It is a different story for AutoRun-based malware, which uses predominantly USB drives or flash memory to replicate itself and has been seen in far greater numbers than Conficker this quarter. Let's look at both side by side:



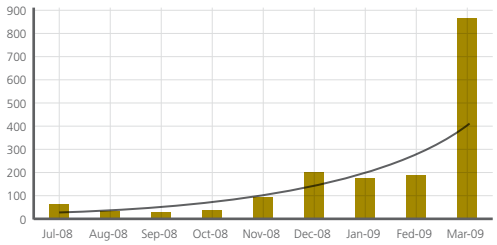
During the past 30 days, less than 10 percent of all reported detections have been AutoRun worms. Conficker started at about one percent and has increased 12 fold, but it still represents less than 15 percent of the amount of AutoRun worm detections at the latter's peak.

Predictions Update

At the beginning of this year, McAfee Avert Labs released its *2009 Threat Predictions.*[2] Several of our educated guesses materialized this quarter.

Friendly fire results in casualties

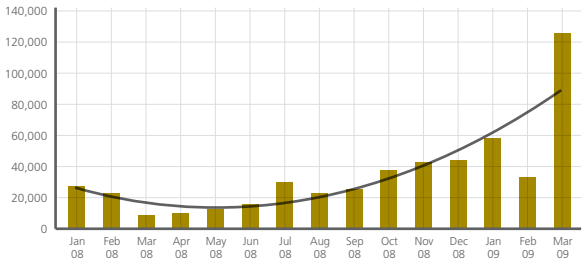
Over the past decade, the popular threat vector of receiving viruses from your friends largely fell by the wayside. Web 2.0, however, has revitalized this old-school method of attack. During this quarter, Koobface variants took thousands of users by surprise as they received the virus from their friends on Facebook. Without the victims' awareness, the links associated with the virus-sent messages led to websites that distributed the worm. Shortly thereafter their computers contracted the virus and sent infected messages to their circle of friends. Social networks continue to offer attackers a popular vector for social-engineering attacks.



2. McAfee Avert Labs Threat Center. http://www.mcafee.com/us/local_content/reports/2009_threat_predictions_report.pdf

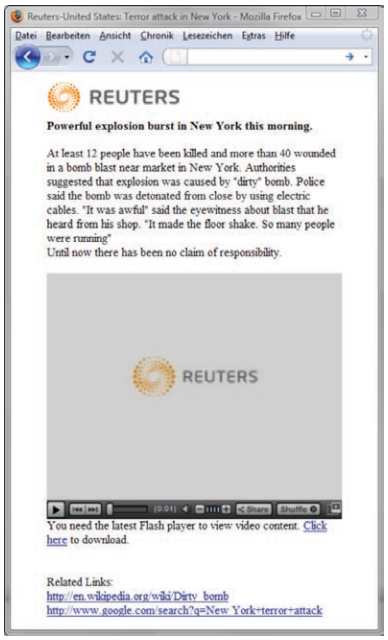
Worldwide rogue web

In February, Facebook was exploited by attackers who created rogue applications using the Facebook platform. Many users took the bait and installed these applications. The events gained media attention, which led McAfee Avert Labs to uncover a massive search engine–optimization ring that targeted the top Google search terms. The attackers not only stole copyrighted materials from popular sites, but they also abused other popular sites, such as Democrats.org, to bump up their Google rankings. The goal of the attackers in optimizing search results was to install rogue anti-virus software. This was a case of a rogue Facebook application, leading to rogue search results, leading to rogue security software. These incidents point out the need for users to surf safely.



Unique Rogue Anti-Virus Binaries Discovered

Threats speak your language



Attackers know that the more relevant and in-context an attack is, the more likely a person is to take action: click a link, enter a username and password, and install an application. Stories about events occurring in our backyards are more likely to grab our attention than the same event happening halfway around the globe. In February and March, the cybercrooks behind the Waledac virus exploited this concept. Unsuspecting victims were lured to websites that were customized based on their location, adding a sense of authenticity. While users read about "local news," the website attempted to silently install the virus via drive-by exploit code.

McAfee Avert Labs Blog

Google and search engine abuse

Google. The name alone means many things to many people. For job searchers, it is a way to find the latest listings. For employers, it is a way to find qualified people online. For shoppers, it is an effective tool for locating attractive prices on the goods they need. And for malware writers and cybercriminals, it is an increasingly effective tool for distributing malware and engaging in cybercrime. When you consider that search engines account for so much Internet activity today, it seems logical that malware writers would look to abuse its power as a way to distribute their wares. For a sampling of our blogs on this topic, have a look at these McAfee Avert blog entries:

- http://www.avertlabs.com/research/blog/index.php/2009/03/15/democratsorg-cans-the-spam/
- http://www.avertlabs.com/research/blog/index.php/2009/03/10/democratsorg-blog-spam-contributes-to-google-search-poisoning/
- http://www.avertlabs.com/research/blog/index.php/2009/02/27/google-bucking-the-trend/
- http://www.avertlabs.com/research/blog/index.php/2009/02/25/google-trends-abused-to-serve-malware/
- http://www.avertlabs.com/research/blog/index.php/2009/01/07/google-code-project-abused-by-spammers/
- http://www.avertlabs.com/research/blog/index.php/2009/01/17/do-not-worry-obama-di-not-refuse-to-be-a-president/

Considering the combined power of indexing and popular keywords with the incentive of easy money for cybercriminals, we expect this type of abuse to continue.

The economy and fear

The global economic problems continue to trouble many people. Issues of safety and terror continue to plague others. Malware writers and cybercriminals can easily turn these fears into profit. This economic trend, which was one of our 2009 threat predictions, has certainly been leveraged throughout this quarter in many troubling ways. Fear is a powerful motivator when used as a social engineering lure by cybercriminals:

- http://www.avertlabs.com/research/blog/index.php/2009/03/16/breaking-news-waledac-terror-attack-in-a-city-near-you/
- http://www.avertlabs.com/research/blog/index.php/2009/02/23/malware-riding-on-the-tides-of-the-economic-crisis/
- http://www.avertlabs.com/research/blog/index.php/2009/02/06/cybercrime-online-threats-and-the-recession/
- http://www.avertlabs.com/research/blog/index.php/2009/01/05/one-hacker-may-conceal-another/
- http://www.avertlabs.com/research/blog/index.php/2009/01/20/fake-antivirus-and-a-real-threat/
- http://www.avertlabs.com/research/blog/index.php/2009/01/29/hoax-or-not-treat-it-the-same/

Scams, spam, and phishing work well enough in good times—let alone in bad. Always remember that the bad guys read the same news that we do and will use headlines and events against us unless we remain vigilant.

About McAfee Avert Labs

McAfee Avert Labs is the global research team 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. http://www.mcafee.com.

McAfee®

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

5395rpt_avert_quarterly-threat_0409