www.BarracudaLabs.com

BARRACUDA LABS
ANNUAL REPORT 2009

BARRACUDALABS

FOREWORD

As the Internet continues to expand and mature, new users come online and seasoned users encounter emerging applications and novel platforms. This blend is what fuels the Internet's continued progression towards new uses for business and personal. As we have seen time and time again over the years, this cycle also disrupts traditional security approaches creating a window for opportunistic attackers.

In this report, we highlight some of the shifts in user behavior and the resulting attacker trends. The increased availability of high-speed bandwidth and wireless connectivity, coupled with the recent advances in portable computers and mobile devices, has shattered the traditional concepts of the network perimeter. The growth of the Web in terms of domain names, sites and pages has outpaced the ability of traditional manual URL filtering capabilities. The dominance of user-generated content has surpassed the Web's legacy domain-based approach to trust. The prevalence of Web applications has bypassed the antiquated approaches of file scanning. Indeed, much of the recent success of the Web makes many of the traditional approaches to safety online obsolete.

Much of the work in Web filtering over the years was carried out in an effort to control users. Today, the priority has shifted to protecting users. This requires different deployment approaches for protection technologies in order to protect a user that can reach the Web anytime from any device. This also requires different reputation intelligence that can analyze and understand the trustworthiness of the content creator in addition to the content host. Further, this requires different inspection approaches in order to fully understand the reality of what is happening on a Web site rather than simply what it is intended to do.

Dr. Paul Judge
Chief Research Officer
Barracuda Networks

CONTENTS


TWITTER
TRENDS & TRACKING

TWITTER TRENDS & TRACKING

HOW PEOPLE ARE USING TWITTER

Notably, people are using Twitter more actively. For the purpose of this exercise, we define a True Twitter User as someone who has three main attributes:

- Has at least (≥) 10 followers
- Follows at least (≥) 10 people
- Has tweeted at least (≥) 10 times

Interestingly, our study shows that only 21% of Twitter users fall within our definition parameters and are True Twitter Users.

What do we mean by "more active" on Twitter?

Essentially, this means that:

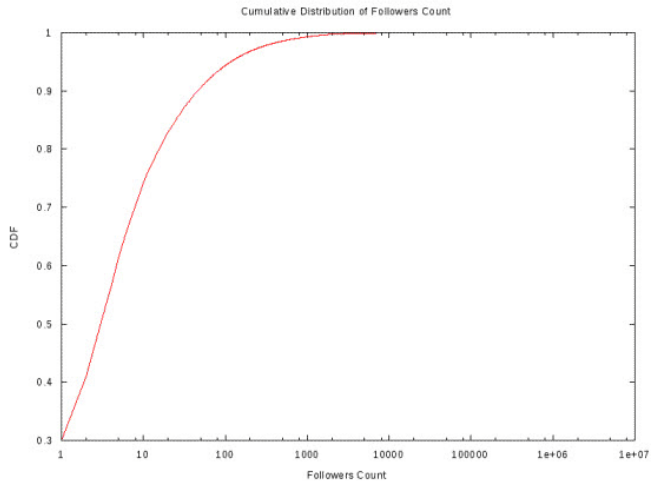
- Users are following more user accounts.
- Users are being followed back by more user accounts and more often.
- Users are tweeting more.

Distribution of Followers

- 17% of Twitter users have zero followers, as compared to 30% in June 2009.
- 61% have less than 5 followers, as compared to 70% in June 2009.
- 74% have less than 10 followers, as compared to 80% in June 2009.

Today, more people have followers on Twitter. Now, 40% fewer people have zero followers compared to mid-2009.

People that have followers now have more followers. There was a 30% increase in the number of users that have 10 or more followers.

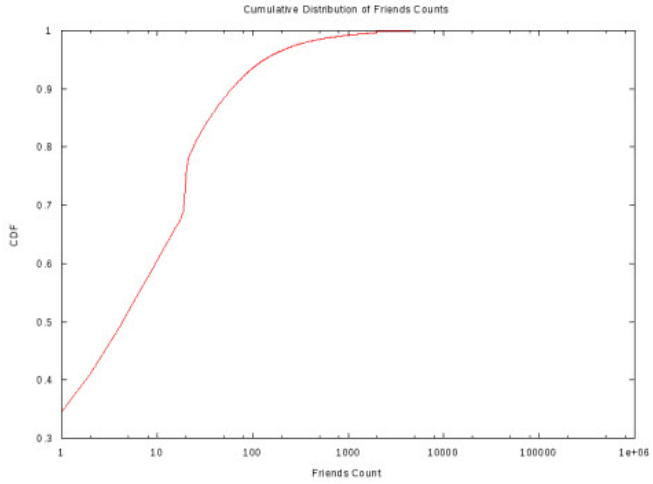


Number of Following (Friends)

- 20% of Twitter users are not following anyone, as compared to 25% in June 2009.
- 51% follow less than 5 people, which is the same count as in June 2009.
- 60% follow less than 10 people, as compared to 66% in June 2009.

The number of Twitter users following no one went from 25% in June 2009 to 20% today, showing a 20% increase in Twitter users that are following at least one person.

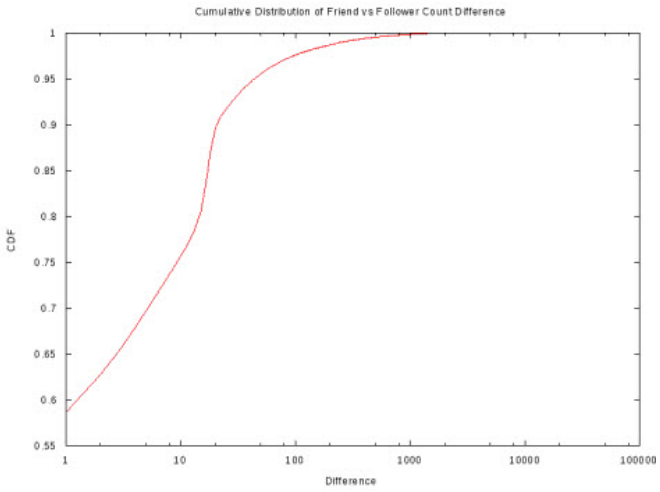
The number of Twitter users following less than 10 people went from 66% in June 2009 to 60% today. The number of Twitter users following more than 10 people went from 34% in June 2009 to 40% today. This shows a 17.6% increase in users following more than 10 people.



Followed or Follower?

- 48% of Twitter users are following more people than they have as followers, as compared to 50% in June 2009.
- 18% of users are following the same number of people that are following them, as compared to 30% in June 2009.
- Combined, 66% of users are following at least ξ) as many people as follow them, as compared to 80% in June 2009.

Today, 34% of Twitter users have more followers than others they are following, showing an 70% increase from 20% in June 2009.

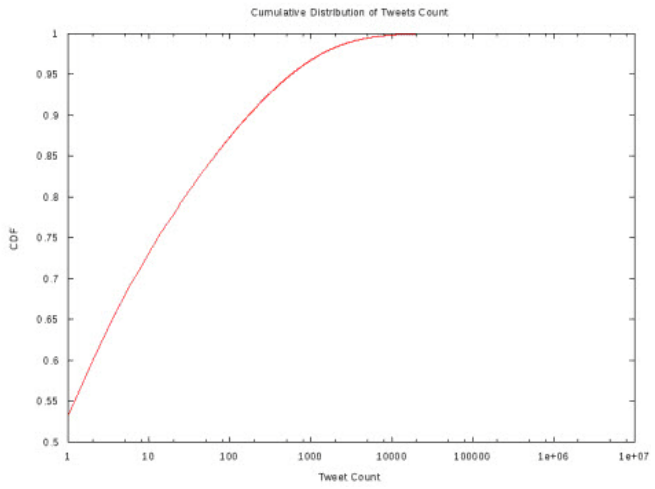


Number of Tweets

- 34% of Twitter users have no tweets, as compared to 37.1% in June 2009.
- 73% of users have less than 10 tweets, as compared to 79% in June 2009.

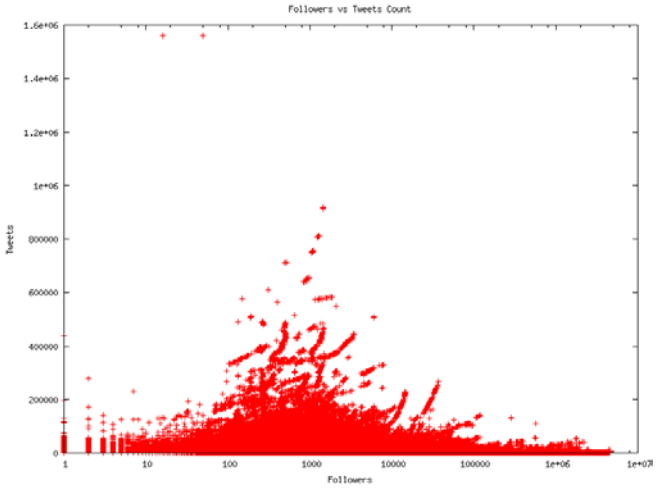
27% of users have tweeted at leas) (10 times, which is a 29% increase since June.

Moreover, today there are 34% of users who have not tweeted since they created an account. While that still seems like a fairly high percentage of inactive accounts, it shows an 8% decrease (down from 37%) since June 2009, demonstrating that people are becoming more active.



Tweets vs. Followers

What's even more interesting is that the most active users on Twitter are not the ones with the most followers. This graph plots the number of followers on the x-axis in log scale and the number of tweets on the y-axis.



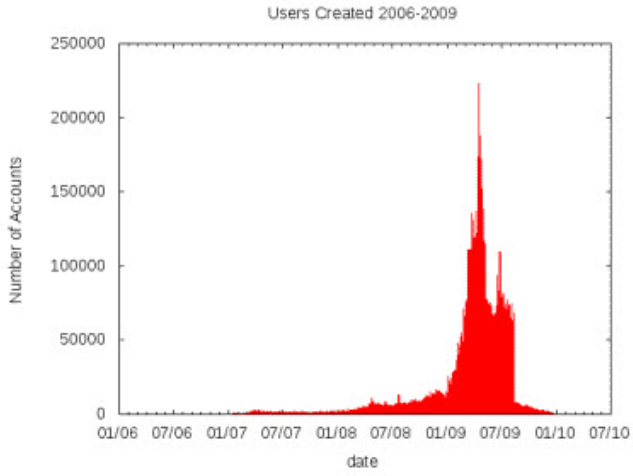
Users with an average of 1,000 followers actually tweet the most, as compared to those with fewer than 100 followers or more than 100,000 followers.

GROWTH OF TWITTER

Further, some remarkable trends emerge as we review how Twitter's growth has taken shape. Based on when a member joined Twitter, we plotted a Twitter growth chart. This chart illustrates a very concentrated growth spurt during the early part of 2009 – a time period that we define as the "Twitter Red Carpet Era."

Twitter User Growth Over Time

Twitter recently reported it had reached approximately 50 million tweets per day. (http://blog.twitter.com/2010/02/measuring-tweets.html)



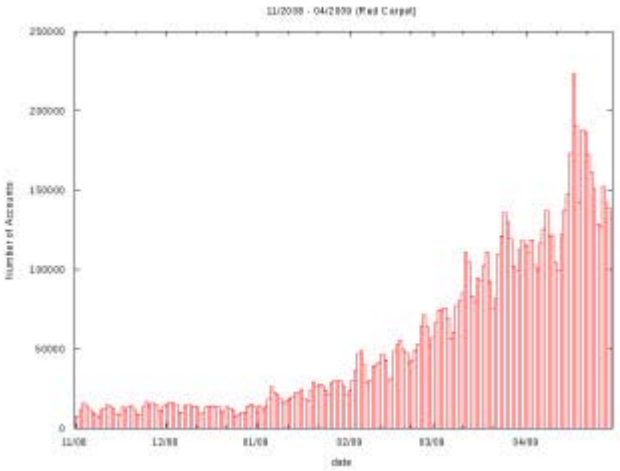
In the beginning of 2008, Twitter was growing approximately 0.31% per month. By November 2008, that growth increased to 1.95% per month.

After December 2008, Twitter's growth exploded from nearly 2% per month, and rising to approximately 4% per month, before finally peaking at nearly 20% per month in April 2009.

At the end of the "Twitter Red Carpet Era," growth appears to have normalized, dropping back to 0.34% by December 2009.

Twitter Red Carpet Era

From November 2008 to April 2009, many "celebrities" – from actors and athletes to musicians and politicians – started Twitter accounts. We call this the "Twitter Red Carpet Era." It was during this time, 27 of the top 50 and 48 of the top 100 most followed Twitter users joined and began tweeting and promoting the service on a daily basis. With the increased visibility of Twitter, the millions of fans of many of these celebrities also joined Twitter, causing the Twitter growth rate to spike – from 2.02% in November 2008 to 21.17% in April 2009.



49% of Twitter accounts were created during the Twitter Red Carpet Era.

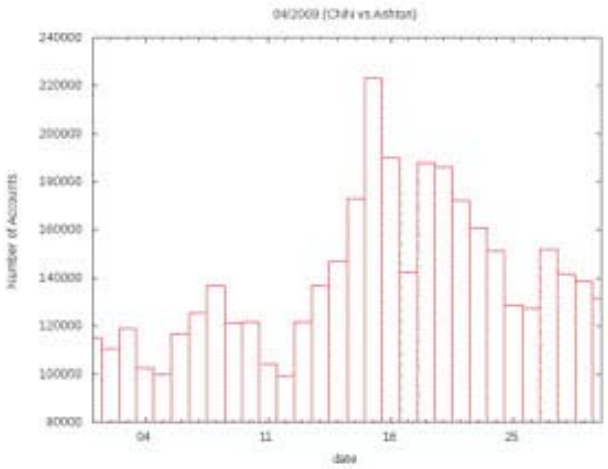
During the famed Twitter Red Carpet Era, 48 of the 100 Most Popular Twitter accounts were created. The following table lists those accounts.

Account	Joined Twitter
1. ashton kutcher (aplusk)	14 months ago
2. Oprah Winfrey (Oprah)	13 months ago
3. John Mayer (johncmayer)	13 months ago
4. Kim Kardashian (KimKardashian)	11 months ago
5. THE_REAL_SHAQ (THE_REAL_SHAQ)	16 months ago
6. Ashley Tisdale (ashleytisdale)	15 months ago
7. taylorswift13 (taylorswift13)	15 months ago
8. Demi Moore (mrskutcher)	13 months ago
9. Coldplay (coldplay)	14 months ago
10. iamdiddy (iamdiddy)	15 months ago
11. Mariah Carey (MariahCarey)	13 months ago
12. 50cent (50cent)	15 months ago
13. A Googler (google)	13 months ago
14. Ashlee Simpson Wentz (ashsimpsonwentz)	11 months ago
15. Miley Cyrus (mileycyrus)	11 months ago
16. Al Gore (algore)	16 months ago
17. Tony Hawk (tonyhawk)	12 months ago
18. lilyroseallen (lilyroseallen)	16 months ago

19. Chelsea Lately (chelsealately)	13 months ago
20. People magazine (peoplemag)	11 months ago
21. Martha Stewart (MarthaStewart)	12 months ago
22. Katy Perry (katyperry)	12 months ago
23. Mandy Moore (TheMandyMoore)	12 months ago
24. RainnWilson (rainnwilson)	13 months ago
25. Perez Hilton (PerezHilton)	13 months ago
26. NBA (NBA)	13 months ago
27. Justin Timberlake (jtimberlake)	11 months ago
28. Brooke Burke (brookeburke)	14 months ago
29. John McCain (SenJohnMcCain)	13 months ago
30. John Legend (johnlegend)	15 months ago
31. Tony Robbins (tonyrobbins)	16 months ago
32. Good Morning America (GMA)	12 months ago
33. Giuliana Rancic (GiulianaRancic)	12 months ago
34. Al Yankovic (alyankovic)	12 months ago
35. GeorgeStephanopoulos (GStephanopoulos)	16 months ago
36. Lenny Kravitz (LennyKravitz)	12 months ago
37. twt.fm (twtfm)	13 months ago
38. Larry King Live (kingsthings)	12 months ago
39. Nick Cannon (NickCannon)	13 months ago
40. Women's Wear Daily (womensweardaily)	13 months ago
41. LeVar Burton (levarburton)	14 months ago
42. Serena Williams (serenajwilliams)	11 months ago
43. Denise Richards (DENISE_RICHARDS)	12 months ago
44. NFL (nil)	13 months ago
45. Paris Hilton (ParisHilton)	12 months ago
46. Fred Durst (freddurst)	14 months ago
47. Peter Facilely (peterfacinelli)	10 months ago
48. Selena Gomez (selenagomez)	12 months ago

Ashton Kutcher vs. CNN

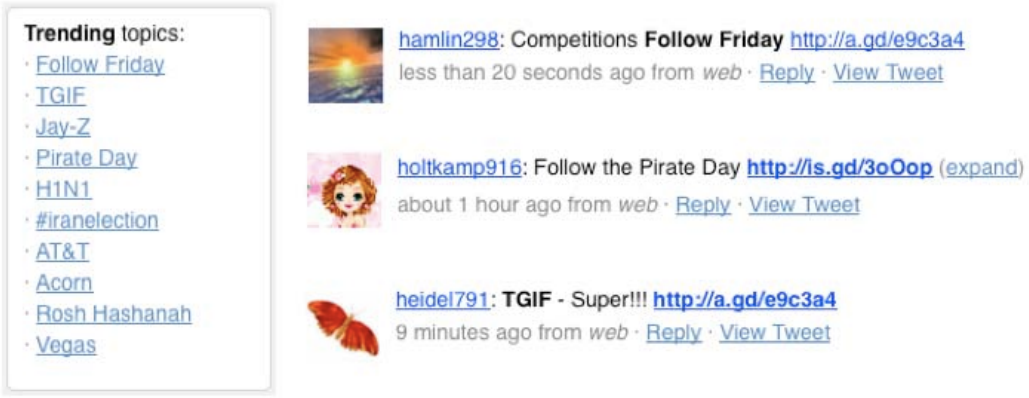
Anyone who follows Twitter remembers well when Ashton Kutcher (@aplusk)challenged CNN (@CNNbrk) to race toward one million followers on Tuesday April 14, 2009. The community responded and the number of new user sign-ups increased tremendously. From April 1 to April 13, there was an average of 0.57% growth in new user sign-ups per day. From April 15 to April 30, there was an average of 0.72% growth in new user sign-ups per day. Twitter's growth rate increased 26.9% in the weeks following Ashton versus CNN challenge. Friday after the challenge saw the largest growth spike in Twitter's history as it grew by 1.03% in a single day.



ATTACKS ON TWITTER

The following section outlines examples of the types of attacks that are carried out on Twitter, followed by a quantitative view of the volume of accounts involved in such attacks.

The figure below shows fake accounts being used by attackers. These accounts are sending tweets that include trending topics and a link. In this case, the link was pointing to a Chinese domain name that served as a distribution point for a Rogue AV operation. Clicking the link starts a series of redirections that end in one of several Rogue AV distribution points.



Throughout 2009, Twitter experienced a number of attacks including the following:

- January: Increase in Phishing Attacks on Twitter
- April: StalkDaily/Mikeyy worm
- June: Guy Kawasaki Account Offers Leighton Meester sex tape
- July: Koobface Increase in Twitter Activity
- July: Fake Retweets Spam
- August: Profile Image Spam
- August: Distributed Denial of Service Attacks
- September: Spam Increase including 'Google is hiring'
- September: Direct Message Worm
- December: DNS records compromised and Web site defaced by "Iranian Cyber Army"

Twitter Crime Rate

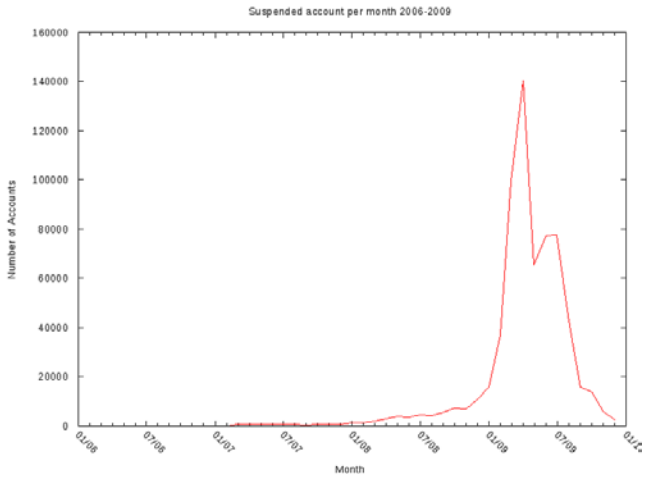
As millions of users flocked to Twitter during the Twitter Red Carpet Era, so too did the criminals. During this time, numerous accounts were used for malicious purposes such as poisoning trending topic threads with malicious URLs (hidden by the ever popular URL shortening services) aimed at luring Twitter users to sites carrying malware or other malicious content.

The Twitter Crime Rate is defined as the percentage of accounts created per month that were eventually suspended for malicious or suspicious activity, or otherwise misused.

- In 2006, the Twitter Crime Rate was only 1.2%.
- By 2007, the Twitter Crime Rate increased slightly to 1.7%.
- In 2008, the Twitter Crime Rate averaged around 2.2%.

During the Twitter Red Carpet Era, the Twitter Crime Rate increased from 2.02% to 3.36%, showing a 66% increase in the overall Twitter Crime Rate.

As more users joined Twitter in 2009, the Twitter Crime Rate continued to escalate reaching 12% in October 2009. This means that one in eight accounts created was deemed to be malicious, suspicious or otherwise misused and was subsequently suspended – clearly showing that the criminals do, in fact, follow the users online.

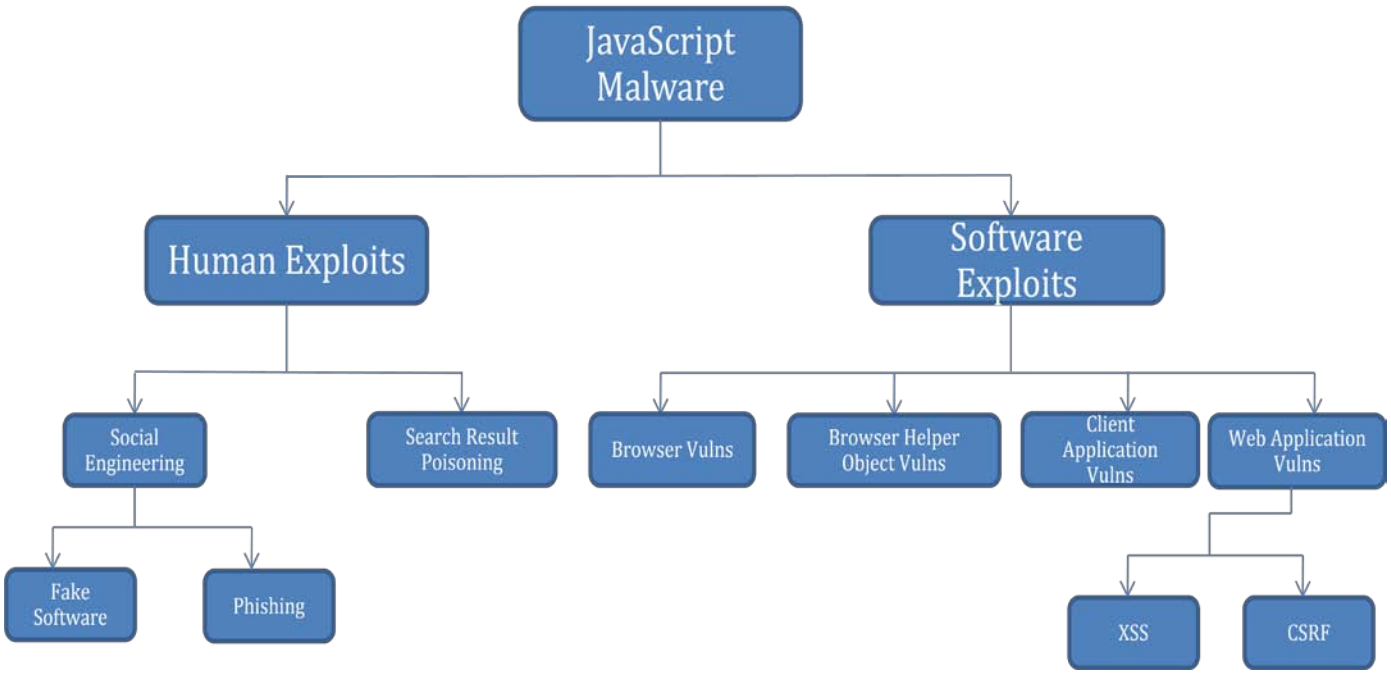



WEB & MALWARE
TRENDS

WEB & MALWARE TRENDS

WEB MALWARE TAXONOMY

The year 2009 proved to be a busy one for Web malware. At Barracuda Labs, we saw attackers shifting their attention to different product groups, innovating their propagation methods and exploiting social engineering means to monetize client side weaknesses. Based on the weakness or vulnerability targeted, we created a classification of these attacks that leads to a better understanding of the types of JavaScript attacks in use.



The distribution of human versus software exploits is shown in the following table.

Software Exploits	69%
Human Exploits	31%

Human exploits are attacks that target a person's understanding and trust on the Internet. These attacks convince people to perform an unintended action. These include social engineering and search result poisoning. Social engineering is widely used in the form of Rogue AV distribution. Attackers convince users that their computers are infected by viruses and then offer a free evaluation version of the fake antivirus software. However, once the user installs, the attackers demand money to make the "antivirus" work or even remove the software from the system. Many users fall prey to this attack, thus successfully monetizing a social engineering attack.

ROGUE AV

Below is an example of Rogue AV software being distributed from a page that belongs to the University of Arkansas Web site. When users accessed a particular page from the university Web site, it opened a window warning them that their computer was infected with viruses and then subsequently downloaded fake anti-virus software.

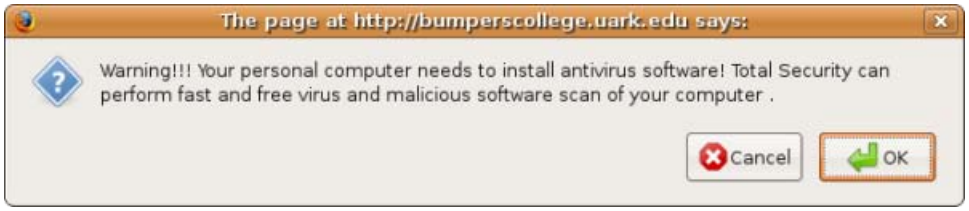
A forensic analysis of the attack revealed that the user requested the following:

> hxxp://bumperscollege.uark.edu/ssp_director/inc/html/d/georgia-inmate-query.html

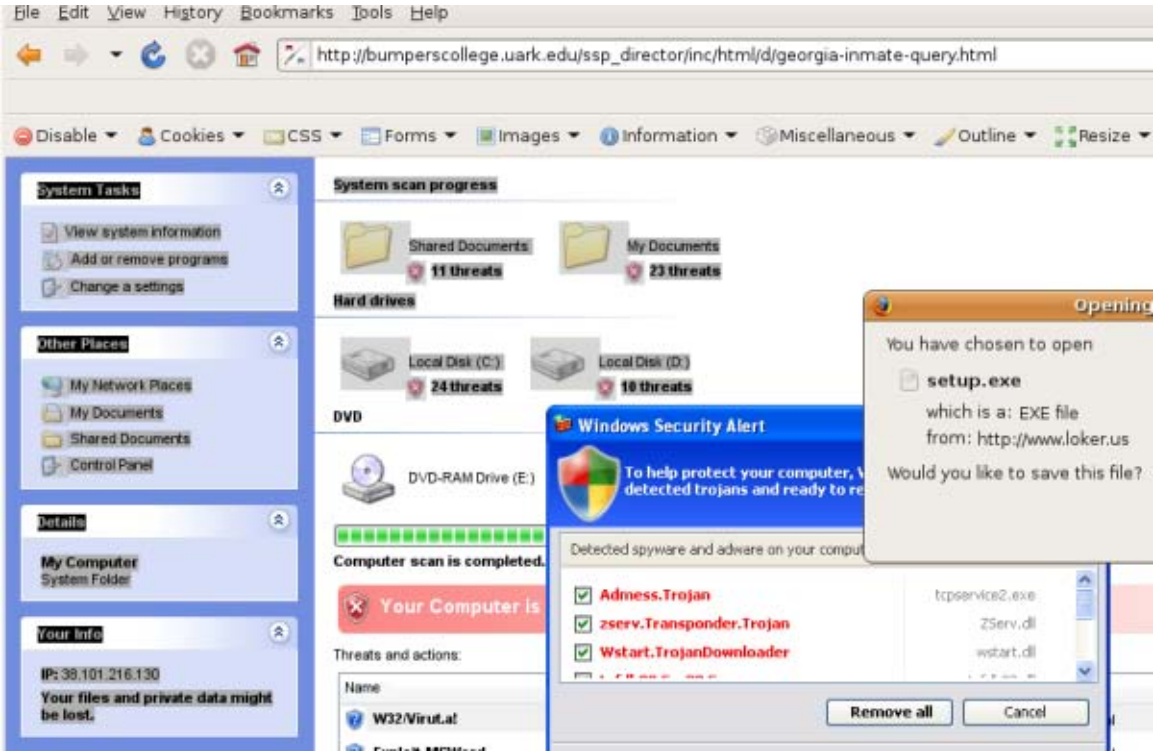
which in turn requested a JavaScript from a malicious domain via script include:

> hxxp://xrusx.com/counter.php?sref=bumperscollege.uark.edu/ssp_director/inc/html/d/georgia-inmate-query.html

which contained further malicious JavaScript includes that generated fake warning messages on the user's computer.



And ultimately attempted to download setup.exe:



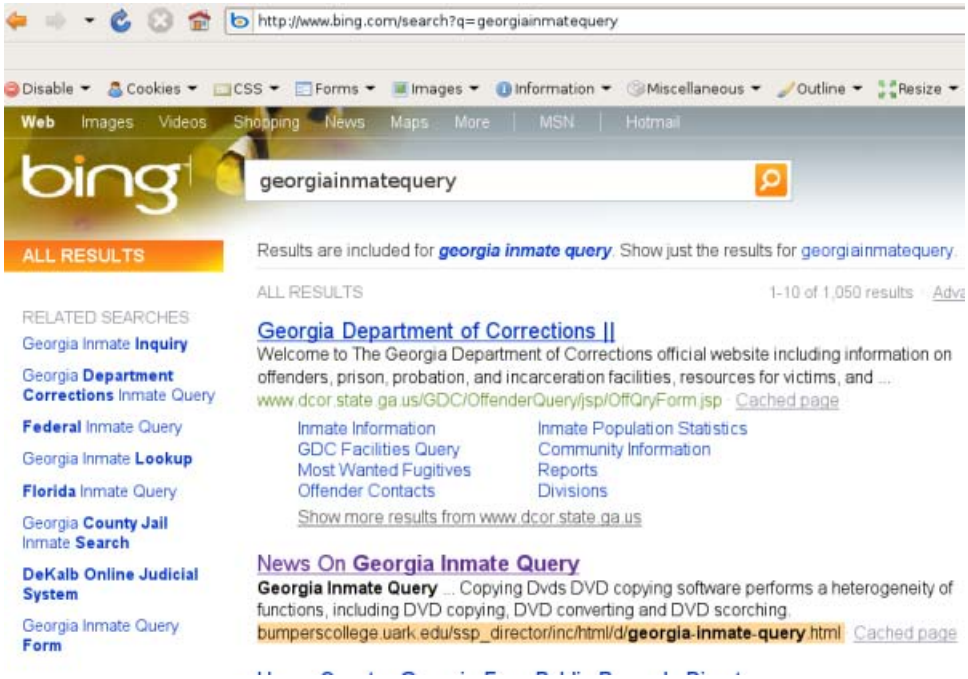
setup.exe was linked off another malicious domain:

hxxp://www.loker.us/forum/attachments/setup.exe

While investigating deep into the tracks of the user to determine how the user got to this page, we made yet another interesting discovery. Our investigation could not find a user browsing page that linked directly off the University of Arkansas site linking the malicious page that was distributing the Rogue AV. Instead, it was a Bing search result that lead user to this page. Specifically, one customer using the Barracuda Purewire Web Security Service searched for 'georigainmatequery' on Microsoft Bing search engine.

hxxp://www.bing.com/search?q=georgiainmatequery

Which yielded following results:



This example also illustrates how attackers are using SEO poisoning techniques to spread malware. As you can see, the malicious link from uArk.edu shows up in the Bing search results — and in the number two spot. The page is leveraging uArk.edu's reputation ranking in what we consider SEO poisoning. This is becoming increasingly more popular as hackers are targeting vulnerabilities in legitimate Web sites since it makes the malicious page more likely to be visited. While search engines have been proactively adding malware scanning in their arsenal, legitimate Web site owners also need to take proactive steps to keep their site free of such malicious content.

GOOD SITES GONE BAD

Here we explore an example of a good site that was compromised to host malicious code. Specifically, attempts to access certain PBS Web site pages yielded JavaScript that serves exploits from a malicious domain via an iframe.

A forensic analysis of this attack revealed that the user requested the following:

hxxp://www.pbs.org/parents/curiousgeorge

which in turn requested:

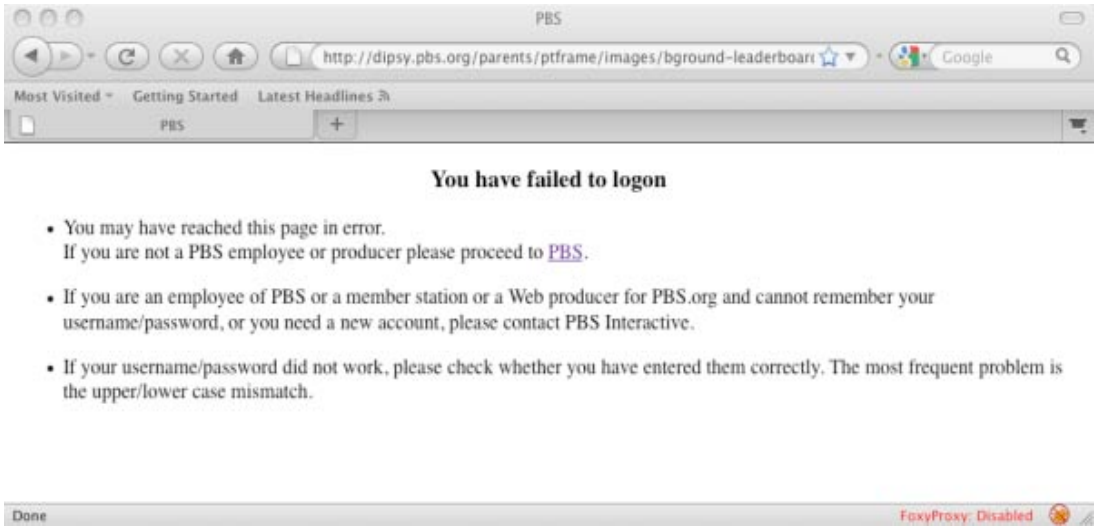
hxxp://dipsy.pbs.org/parents/ptframe/images/bground-leaderboard.jpg

instead of:

hxxp://www.pbs.org/parents/ptframe/images/bground-leaderboard.jpg

Accessing the image off of dipsy.pbs.org requires login credentials, as shown in the following screenshot.

If correct credentials are not provided, dipsy.bps.org serves an error page that looks normal:



… until you look under the hood. The end of the error page's source:

contains obfuscated JavaScript placed there by a malicious third party. Once deobfuscated, this code writes an iframe that loads malicious JavaScript from the following malicious URL:

hxxp://qxfcuc.info/f.cgi?jzo

The above URL serves exploits that target a variety of software vulnerabilities, including those in Acrobat Reader (CVE-2008-2992, CVE-2009-0927, and CVE-2007-5659), AOL Radio AmpX (CVE-2007-6250), AOL SuperBuddy (CVE-2006-5820) and Apple QuickTime (CVE-2007-0015).

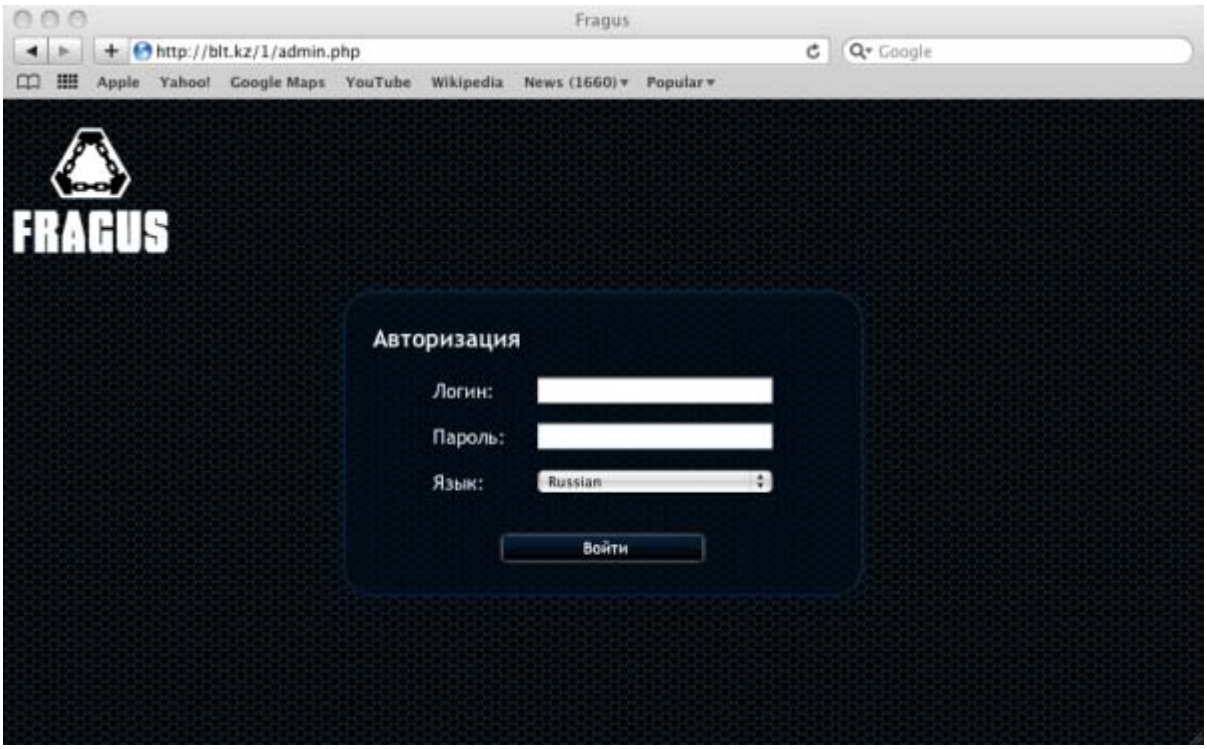
The domain qxfcuc.info is part of a malware campaign that includes tens of similar Web sites hosted off of a handful of common IP addresses. Similar exploit code was served from most of these domains, although a handful (e.g., yyoqny.info) display a message that suggests the criminal behind this campaign is compromising systems to build a botnet that will likely be leased later. Translated from Russian, that message tells prospective leasers to "Send a message to ICQ #559156803; stats available under ststst02."

WEB EXPLOIT KITS

Web Exploit Kits are increasingly used by attackers to host exploits on compromised sites. These kits embed small portions of code that will be accessed by visitors to the otherwise legitimate site. The exploit page typically tries several exploits based on a range of vulnerabilities in the client's browser, machine and software. The exploit kits typically also host an administration page that allows the attacker to configure the kit and view statistics about infected clients. These exploit kits are created by skilled programmers and then sold so that other attackers can easily carry out attacks. These kits are offered at prices that range from $300 to $1,000.

Some of the exploit kits in use include LuckySploit, UniquePack, NucPack, Liberty, Fragus, Tornado, Fiesta, IcePack, FirePack, MPack and Eleonore.

Below, we explore Fragus as an example of the capabilities of a Web Exploit Kit. The image below is a screenshot of the log in screen:



Below is a list of exploits that are part of the Fragus kit.

•directshow(): Performs heap spraying, then serves hxxp://blt.kz/1/directshow.php, which targets the Microsoft Video (DirectShow) ActiveX control vulnerability (a.k.a., MS09-032).

•pdf(): Serves hxxp://blt.kz/1/pdf.php?eid=3, which targets Acrobat Reader vulnerabilities in util.printf, Collab.getIcon, and Collab.collectEmailInfo (a.k.a., CVE-2008-2992, CVE-2009-0927, and CVE-2007-5659, respectively).

•flash(): Serves hxxp://blt.kz/1/swf.php?eid=4, which targets the Adobe Flash Player integer overflow vulnerability (a.k.a., CVE-2007-0071).

•aolwinamp(): Performs heap spraying, then attempts to exploit the AOL Radio AmpX (AOLMediaPlaybackControl) ActiveX control vulnerability (a.k.a., CVE-2007-6250).

•snapshot(): Targets the Microsoft Access Snapshot Viewer ActiveX control vulnerability (a.k.a., MS08-041) in an attempt to have hxxp://blt.kz/1/load.php?e=6 executed.

•spreadsheet(): Performs heap spraying, then attempts to exploit the Microsoft Office Web Components ActiveX control vulnerability (a.k.a., MS09-043).

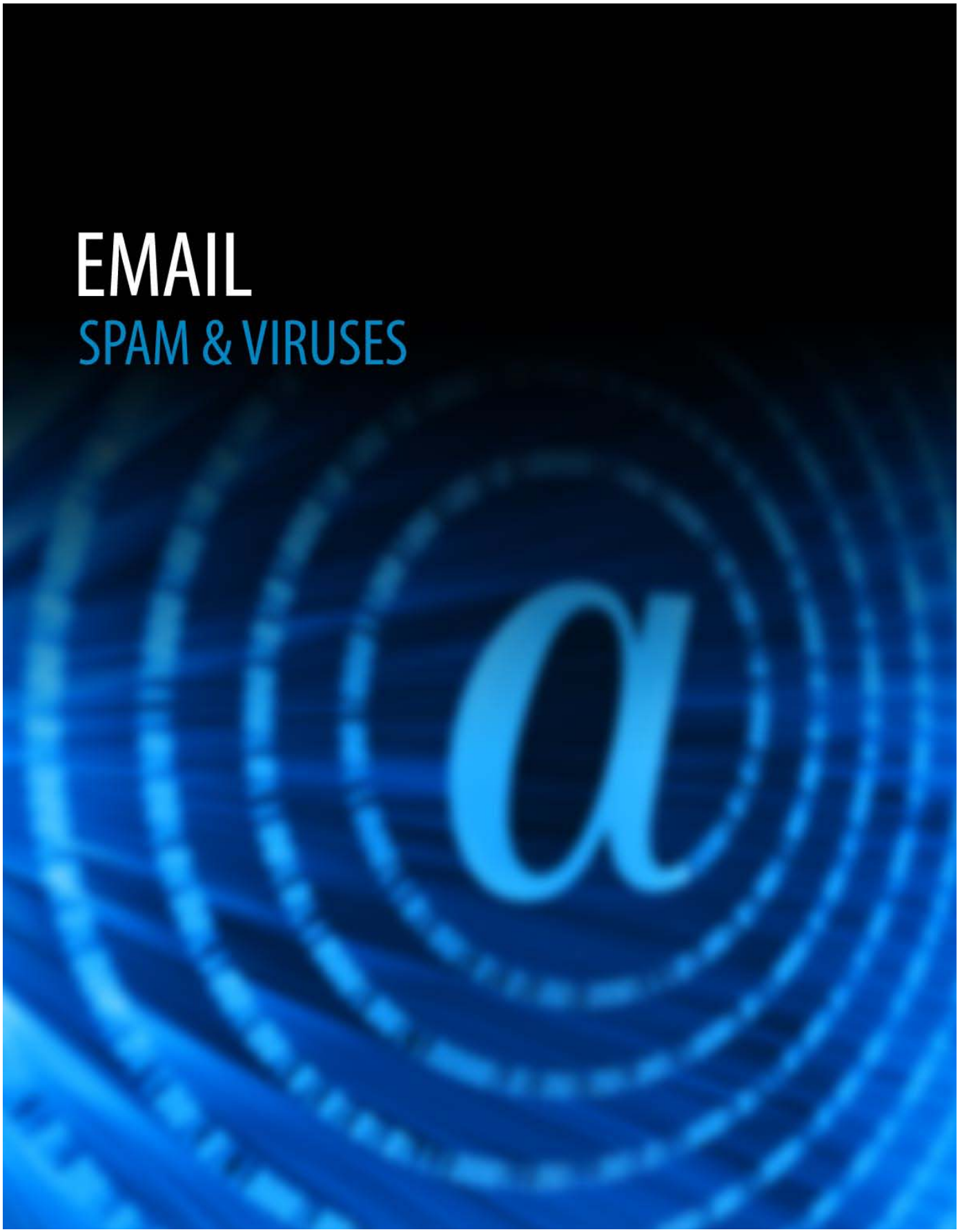
•ms09002(): Performs heap spraying, then attempts to exploit the Microsoft Internet Explorer 7 memory corruption vulnerability (a.k.a., MS09-002).

The top five vulnerabilities that these exploit kits targeted in 2009 are as follows:

	Attack	CVE listing
1.	Adobe Malicious PDF	CVE-2008-2992 CVE-2009-0927 CVE-2007-5659
2.	Microsoft Internet Explorer Memory Corruption	CVE-2009-0075
3.	Adobe Flash Player Integer Overflow	CVE-2007-0071
4.	Microsoft Video DirectShow ActiveX Control Vulnerability	CVE-2008-0015
5.	Microsoft Office Web Components ActiveX control Heap Spray	CVE-2009-1136

The following tables show the top client infections that we tracked based on “phone home” traffic.

Top Phone Home Web Infections for 2009
Adware.Toolbar.MySearch.MyWebSearch
Adware.180Solutions.Zango
Adware.Toolbar.Mysearch.Myway
Adware.FunWebProducts
W32.Gaut.A
AdWare.Win32.Agent.bjx
Adware.MouseHunt
Adware.ZenoSearch
Trojan.Win32.Zbot.gen
Adware.Toolbar.NeoToolbar


EMAIL
SPAM & VIRUSES

EMAIL THREATS

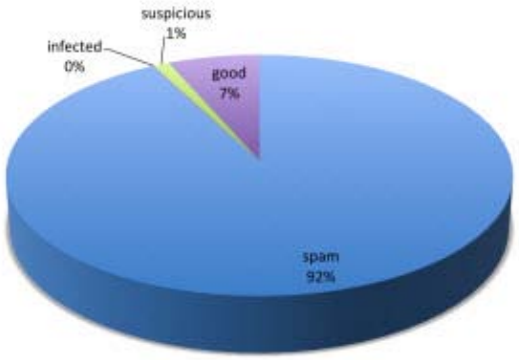
EMAIL SPAM

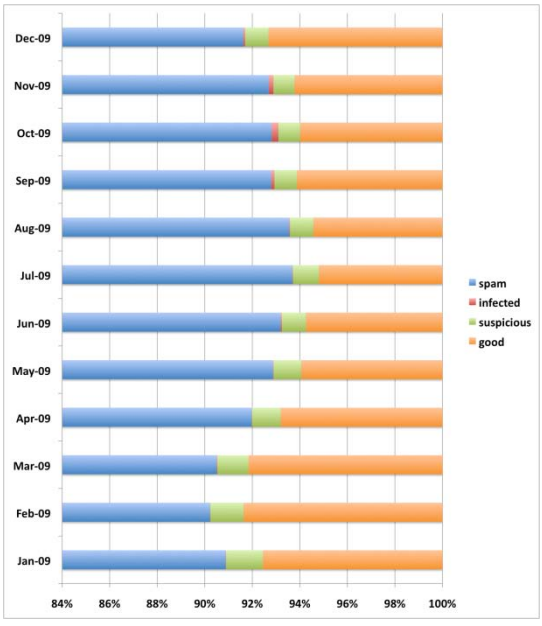
Barracuda Labs examined more than 700 billion email messages in 2009. Of those:

- 92.24% were spam
- 0.07% were infected
- 1.12% were suspicious
- 6.57% were legitimate email

This means that about one in every 1,400 email messages contained a virus; about one in every 100 emails were suspicious; and only one in every 15 emails were legitimate.

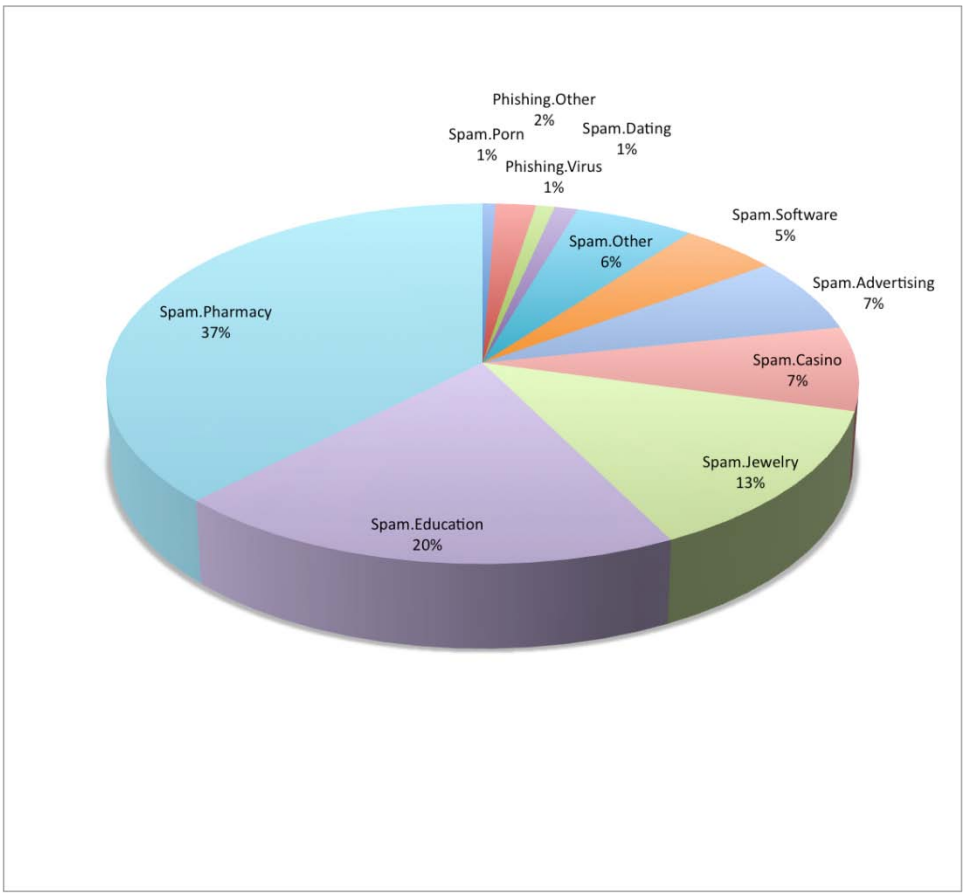
July was the worst month for spam with 93.69% of email being spam.





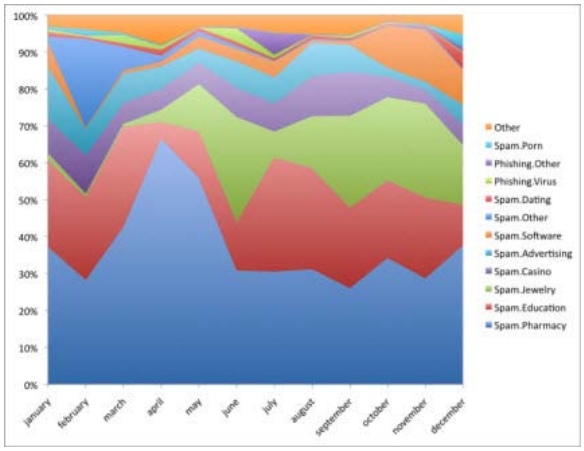
Spam Types

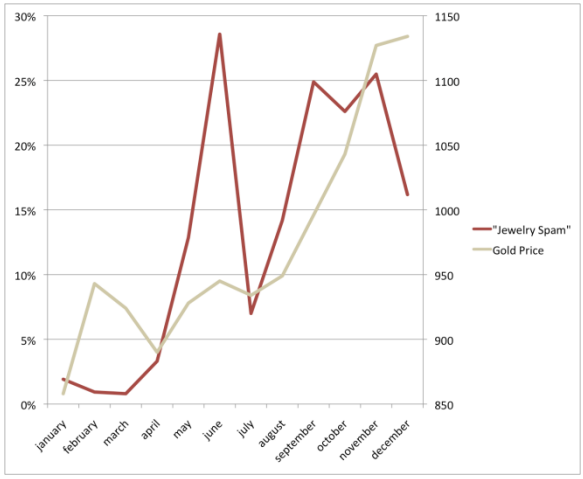
This graph shows the spam percentage by category for 2009. Pharmaceutical spam represented 37% of all spam received in 2009.



The Growth of Jewelry Spam

This graph shows the monthly changes in the types of spam in 2009. One notable shift is the change in jewelry spam. During the first three months of the year, jewelry spam averaged 1.2% of all spam, which grew to 3.3% in March and 12.9% in April. This averaged 19.8% for the remainder of the year. One possible cause for this is the rapidly increasing price of gold that led to many campaigns that offered to "buy your old gold." The below graph compares the growth in jewelry spam to the price of gold. We see that they experienced a similar growth rate during 2009.

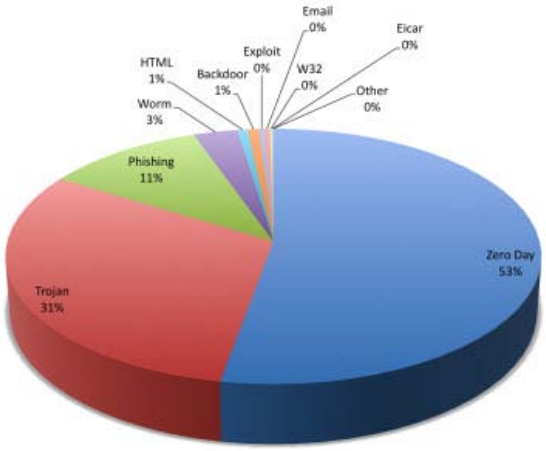




EMAIL MALWARE

Top 10 Malware Types for 2009

Trojans and phishing attacks were the dominant types of malware sent via the email vector. 31% of the email-borne malware detected were Trojans and 13% were phishing. 47% of the email-borne malware were detected by signature-based approaches and 53% were detected Barracuda's Zero-Day protection.

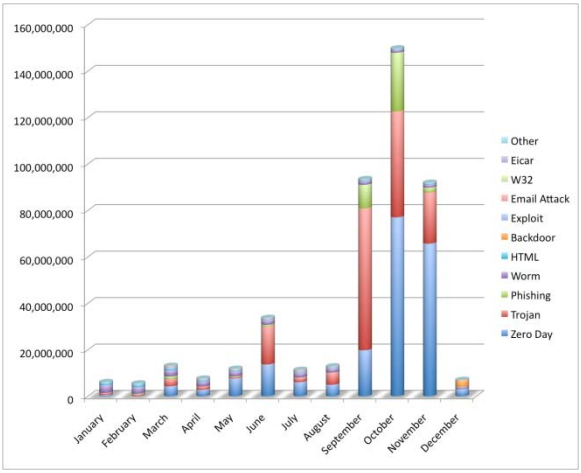


Virus Outbreaks for Year by Month

September through November were the worst months for email-borne viruses, with a tenfold increase from August to October. In October, one in every 344 emails contained a virus. The majority of this malware traffic was trojans such as Trojan.Downloader, Trojan.Agent and Zbot.

From January through August, there were an average of 12 million malware blocks per month. From September through November, there was almost a tenfold increase to 111 million malware blocks per month.

For the first five months of 2009, 13.8% of email-borne malware were Trojans. From June through September, Trojans were 40.2% of email-borne malware.



ACKNOWLEDGMENTS

This report represents several highlights of the work performed in 2009 by Barracuda Networks in protecting our more than 100,000 customers. This includes the efforts of our engineering, support and research teams in the Americas, Europe and Asia. We would like to acknowledge our customers for trusting us with the responsibility of keeping their users and networks safe. We also would like to acknowledge our data sharing partners and research affiliates.

For ongoing updates, please visit BarracudaLabs.com.