

State of the Web – Q2 2010

A View of the Web from an End User's Perspective

ABSTRACT

Attackers are no longer targeting web and email servers. Today, they are attacking enterprises from the inside out, by first compromising end user systems and then leveraging them to gain access to confidential data. As such it is imperative that organizations have an understanding of what is happening on the web. As a Security-as-a-Service vendor, Zscaler has a unique perspective on web traffic. With millions of end users traversing the web through Zscaler's global network of web gateways, we are able to better understand both how users are interacting with web based resources and how attackers may be targeting end users. In our quarterly 'State of the Web' report, we provide a window into the web from an end user's perspective.

OVERVIEW.....	3
WEB TRAFFIC.....	4
Web Browser Versions.....	4
Top Categories by Country	5
The Wikileaks Saga.....	6
MALICIOUS TRAFFIC.....	8
Malicious Sites.....	8
Malware by Top Countries	9
Top Malicious Domains.....	10
Malware / Botnets	12
Incidents	13
Facebook 'Likejacking'	13
Mass SQL Injection Attacks	13
Malvertising	13
WordPress Hacks	14
Malicious .in Domains	14
SEO Attacks.....	14
Phishing.....	16
iPad Beta Testing Phish	16
Watch World Cup Live Phish.....	16
Twitter Followers Phish.....	16
CONCLUSION	18

OVERVIEW

During the second quarter of 2010, attackers once again took advantage of opportunities just as quickly as they emerged. These opportunities included both the emergence of new vulnerabilities in popular technologies as well as current events that drew the attention of millions around the globe. Q2 included the start of one of the largest global sporting events, the World Cup. It didn't take long for attackers to seize on this opportunity to deliver a variety of World Cup related attacks including poisoning search results with Blackhat search engine optimization (SEO) techniques and phishing for financial credentials. The release of the iPad in April also received no shortage of press and as such was another popular target for attackers.

While we are pleased to see the use of Internet Explorer (IE) 6, a now nine year old web browser, continue to decline, it still commands a concerning proportion of enterprise web traffic. More than one in five employees continue to use IE 6 when surfing the web, despite the continued emergence of Oday threats and a lack of modern security features. In June 2010, only 22% of corporate IE users had migrated to IE 8 – the latest and most secure iteration of the IE browser.

A new attack trend emerged during the quarter thanks based on the deployment of a new Facebook feature - the 'Like' button – on numerous external sites. It allows site visitors to easily provide a referral to external web content, and with bloggers seeing a 50% increase in Facebook referral traffic using the feature¹ it's not surprising to see it also being abused. Known as 'Likejacking', Zscaler has seen numerous instances of attackers tricking users into clicking 'Like' buttons to drive traffic to malicious sites. We have also seen 'Likejacking' combined with 'Clickjacking' to further automate the process. Another social networking inspired attack that we saw increasing over the quarter are – Twitter follower scams – sites set up to trick users into providing their Twitter credentials in exchange for more followers.

While we continue to see growth in malicious web traffic, the players are constantly changing. During the quarter, China moved up to the number two spot overall when comparing the number of unique IP addresses in various countries known to be hosting malicious sites. The jump was a fairly dramatic one, with China moving from an average of only of 2.97% of unique IP addresses in Q1 2010 to 7.24% in Q2. Overall, China, the Netherlands, Russia and Korea all moved up three or more places in the top ten rankings for the quarter. We also noted significant movement among the top malicious IP addresses seen during the quarter, with statistics changing dramatically from month to month. This illustrates just how dynamically attacks are constantly being delivered from alternate locations to bypass static controls such as block lists.

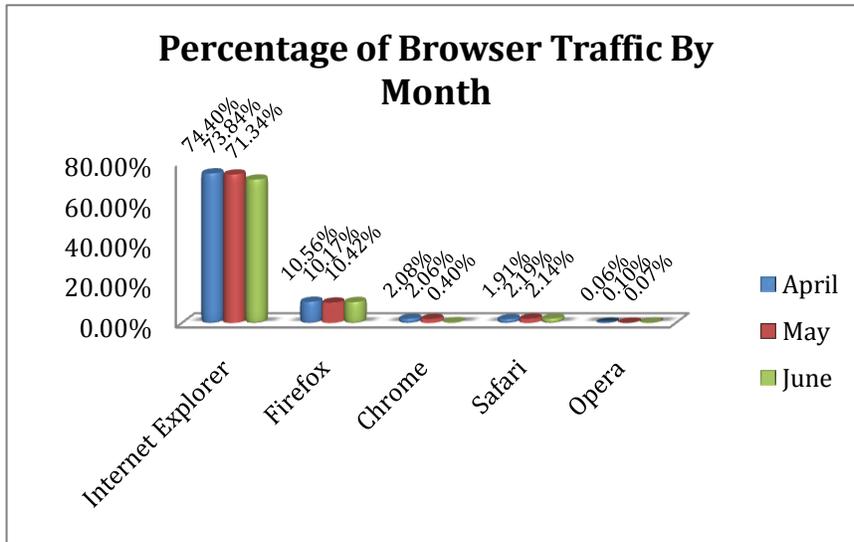
Mass attacks also played a role during the quarter. In June we witnessed yet another mass SQL injection attack, this time targeting Microsoft IIS servers with SQL Server back-ends. As has become common practice for attackers, links to malicious JavaScript files were injected into sites with application vulnerabilities that permitted SQL injection. In this case, thousands of sites were infected with code that ultimately leveraged a known vulnerability in Adobe Flash to compromise PCs. This was not, however, the only instance of mass infection that we tracked during the quarter. WordPress sites, a common target for attackers given the spotty security history of the application, was also saw a surge in attacks during the quarter.

Attackers continue to target end users in the attempt to obtain valuable data or compromise machines to build botnet armies. While the goals have not changed, the techniques continue to evolve. The attacks that we're seeing are increasingly dynamic in nature, continually shifting locations and swapping out payloads to avoid detection. It is clear that security vendors must be able to quickly adapt and inspect web based content on-the-fly in order to identify and secure against emerging threats in this continually evolving environment.

¹ <http://everything.typepad.com/blog/2010/06/facebook-like-integration-typepad-blog-stats.html>

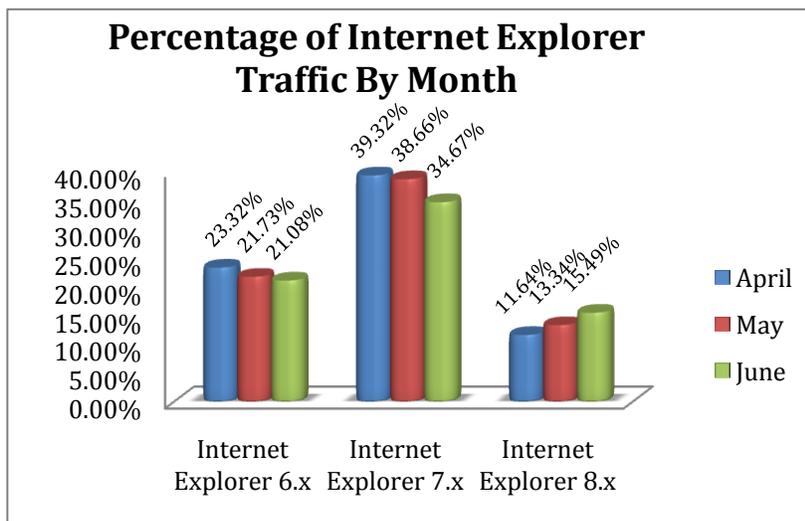
WEB TRAFFIC

Web Browser Versions



As has been the trend over recent State of the Web quarterly reports, Internet Explorer (IE) continues to lose ground in the browser wars. While this same trend has been noted in other public reports, those tend to look at browser traffic statistics from a server point of view – namely, reviewing web server logs to deduce which browsers most frequently visited the site. Zscaler is in the position of viewing traffic patterns from two unique vantage points. First, we see web traffic to not just one web site, but quite

literally millions, as end user traffic flows through the Zscaler cloud regardless of its ultimate destination. Secondly, Zscaler traffic tends to be exclusively from corporations as opposed to the general public. Therefore, we're not only able to get a more accurate picture of web browser statistics, but our stats also reflect *enterprise* web traffic. While groups such as Net Market Share show IE usage among all users at just north of 60%, as can be seen in the chart below, the popular browser actually enjoys a greater advantage by more than 10% in the corporate world, although this lead is rapidly falling².



In Q1, we saw a significant drop in IE6 usage from 33.46% to 26.93%, due in large part to 0day vulnerabilities such as the uninitialized memory corruption vulnerability in iepeers.dll (CVE-2010-0806)³, which served as a catalyst to force enterprises that had been clinging to IE6 for compatibility reasons to finally upgrade. We saw this trend continuing in Q2, although at a less dramatic pace as IE6 usage further slipped from 23.32% to 21.08%. While encouraging, it is concerning that *one in five enterprises still continues to support IE6*, now a

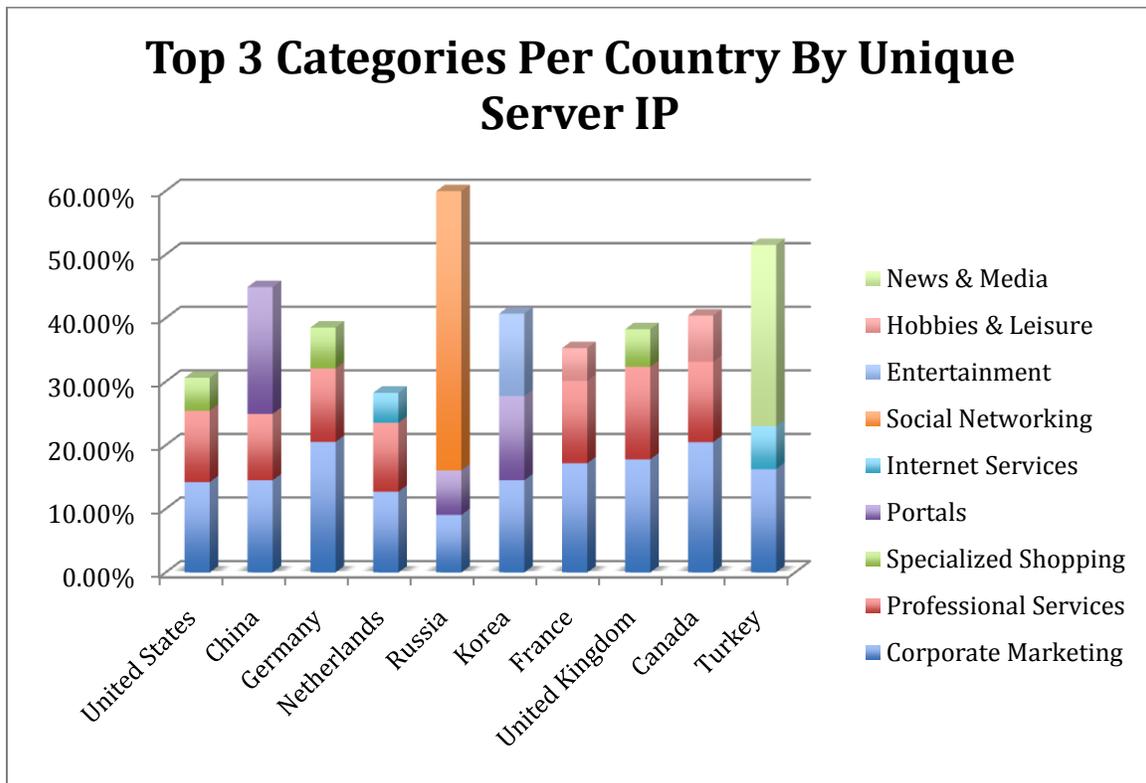
nine year old web browser lacking many of the security features present in the most recent Microsoft browser, IE8. IE7 also saw a decline in usage for the quarter, but remains the most highly used Internet Explorer browser in enterprises, representing over one third of all web browser usage.

² <http://www.netmarketshare.com/browser-market-share.aspx?qprid=0>

³ <http://www.microsoft.com/technet/security/Bulletin/MS10-018.mspx>

Top Categories by Country

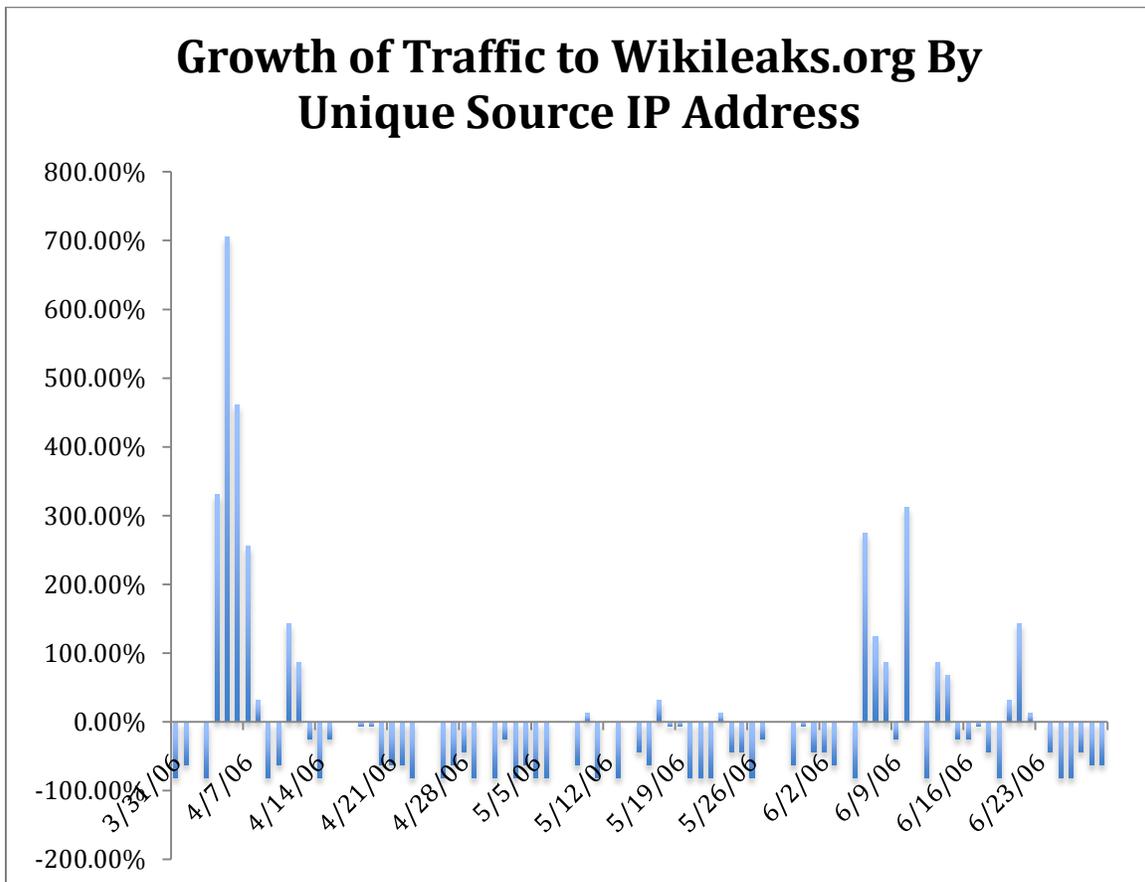
What types of sites are popular in different countries? Do the same categories float to the top regardless of geography? We took a look at the top three categories of web servers for the ten countries receiving the most malicious web traffic and the results were interesting. When looking at Western countries such as the United States, Germany and the UK, the results are almost identical; corporate, professional services and shopping sites consistently take the top three spots, in that order. Canada, France and the Netherlands also had corporate sites and professional services as the top two web destinations. Eastern countries, however, differed significantly. In Russia, we found that nearly 44% of all traffic was destined for social networking sites. This is interesting, given Zscaler's primarily corporate user base. Keep in mind however that in this instance, we're looking at traffic by destination, not source. This does not therefore show that Russian workers are spending an inordinate amount of time on social networks, but rather that Russia receives a higher than average amount of web traffic destined for Russian based social networking sites, with the primary sites being vkontakte.ru, odnoklassniki.ru, and mamba.ru. And, in Turkey the top spot was claimed by news and media sites at 28.5% of traffic.



The Wikileaks Saga

Wikileaks.org has been the subject of several major news stories in mid-2010. The site is best known as a place for people to share important information previously unknown to the public, typically obtained through insider contacts (information leaks from whistle-blowers, disgruntled employees, etc.). Wikileaks rose to public prominence this year due to a series of posts related to the Afghan war.

The chart below details traffic patterns for requests to wikileaks.org from unique client IP addresses over the course of the quarter.



Three distinct spikes can be seen when looking at traffic to wikileaks.org from visiting IPs/organizations on:

- April 5 – 8
- June 7 – 9, 11
- June 22

Unsurprisingly, these traffic spikes coincide with the following major releases of documents on the site:

- April 5, 2010 – Release of “Collateral Murder” video⁴
- June 7, 2010 – Arrest of Army Spc. Bradley Manning
- June 11, 2010 – Dept. of State Press Briefing
- July 25, 2010 – Release of “Afghan War Diary”⁵

⁴ http://en.wikipedia.org/wiki/July_12,_2007_Baghdad_airstrike

The largest spike was on April 6th, where a full 25% of the total unique IPs identified during the quarter visited the site. This spike corresponds to the “Collateral Murder” video release. Comparing the April traffic spike to the days leading up to the event, shows that the initial spike represented roughly a 700% growth in daily visits. The spike follows a similar pandemic pattern: (1) spike at the onset of the event, (2) secondary spike from those coming in contact with, or learning of the event, (3) drop-off from saturation of the population, and (4) return to slightly elevated normal levels.

The spikes in early June are directly related to Manning’s arrest and the corresponding press briefings from the Government on the incident. And the spike on June 22 corresponds to Wikileaks announcement of its plans to release documents related to a U.S. airstrike that killed Afghan civilians in 2009⁶.

The Wikileaks saga is an experiment in “Internet Rubber-Necking” or “Gawking.” In other words, the population hears about the Wikileaks story on the news, from their friends, etc. and they subsequently want to check it out for themselves. From a security standpoint, it is important to identify and research anomalous traffic patterns, as they may be malicious in nature. Take for example a newly promoted phishing site or drive-by download – a page previously receiving little or no traffic is suddenly inundated with requests – however infected machines or users falling prey to a social engineering attacks are driving the traffic. Monitoring for anomalous traffic patterns and being able to distinguish between breaking news and propagating malware is critical to defending against modern web based threats. Fortunately, we’re able to supplement the detection of such traffic with inspection of the web content in order to differentiate between the two scenarios.

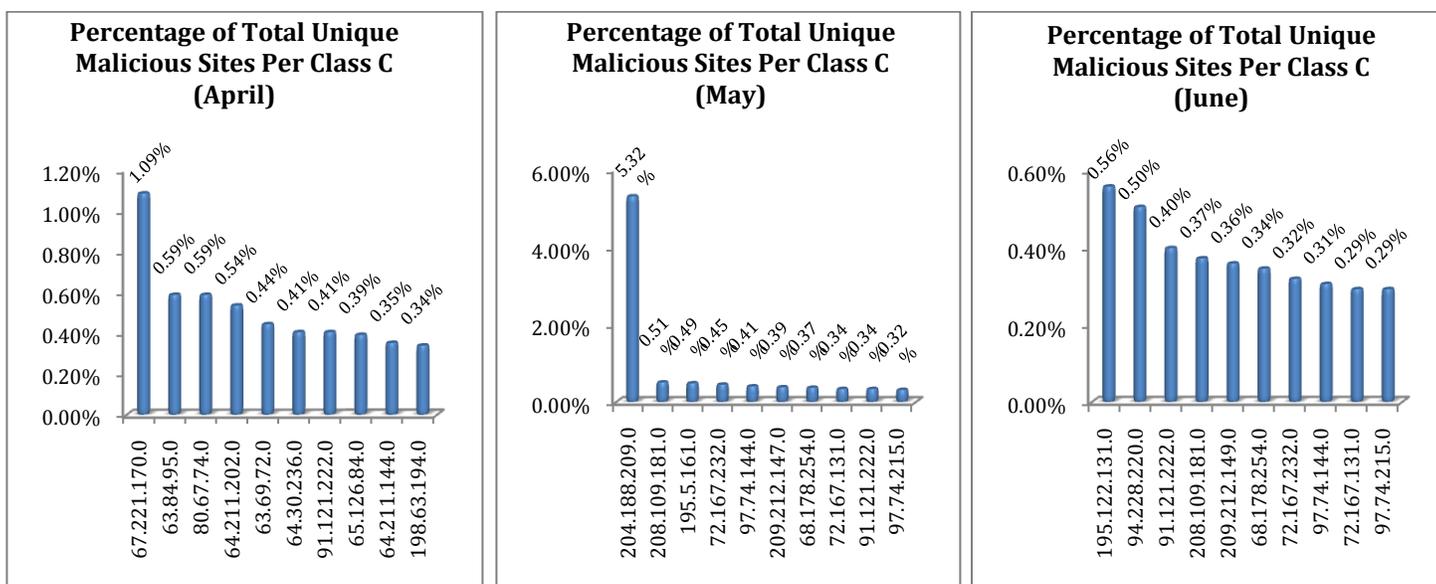
⁵ http://en.wikipedia.org/wiki/Afghan_War_Diary

⁶ <http://www.washingtonpost.com/wp-dyn/content/article/2010/06/21/AR2010062104670.html>

MALICIOUS TRAFFIC

Malicious Sites

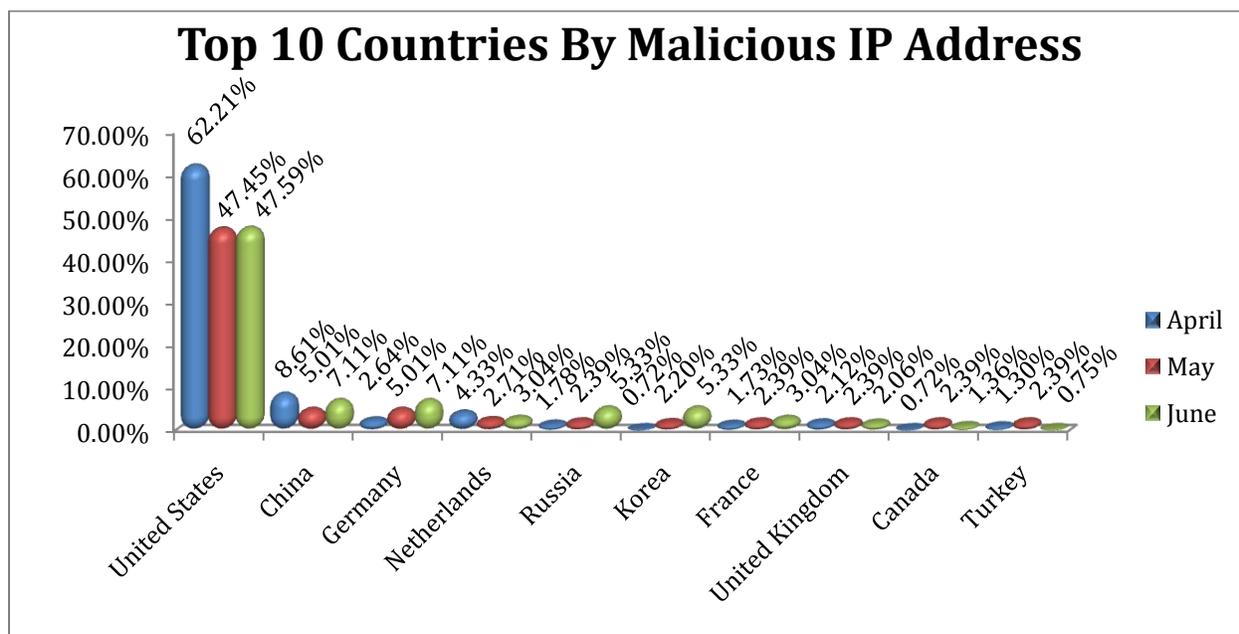
Looking at the top unique Class C addresses hosting malicious content this quarter, one thing stands out: On a month-by-month comparison, the top sites vary dramatically. Namely, a given block of addresses from one month only occasionally shows up in the top ten for the next month. It is clear that attackers are quickly moving content to different locations in order to ensure that enterprises cannot simply protect themselves by blocking a specific range of IP addresses. Techniques such as fast-flux, which quickly rotates DNS resolution among a variety of IPs for specific domains, contributes to these findings.



The significant spike in malicious traffic in June resulted from attacks using the then Microsoft Oday iepeers.dll (CVE-2010-0806) vulnerability mentioned previously. In May, Zscaler blocked a significant amount of exploit traffic of this nature coming from 204.188.209.194.

The code used in the attack was well obfuscated, being split between several files, using eval() statements, DOM references, and exceptions (try ... catch). The exploit page appeared to have been written by Chinese hackers and was targeting Chinese users, based on the fact that part of the intermediate code was written with Chinese characters. Samples of the exploits had also been reported in a few Chinese forums. Victims were typically redirected to the exploits from other websites, mainly though hacked web pages. We have also previously seen other malicious campaigns using domain names (e.g. d.360360.co.cc and 46603.com) that once resolved to this IP address.

Malware by Top Countries



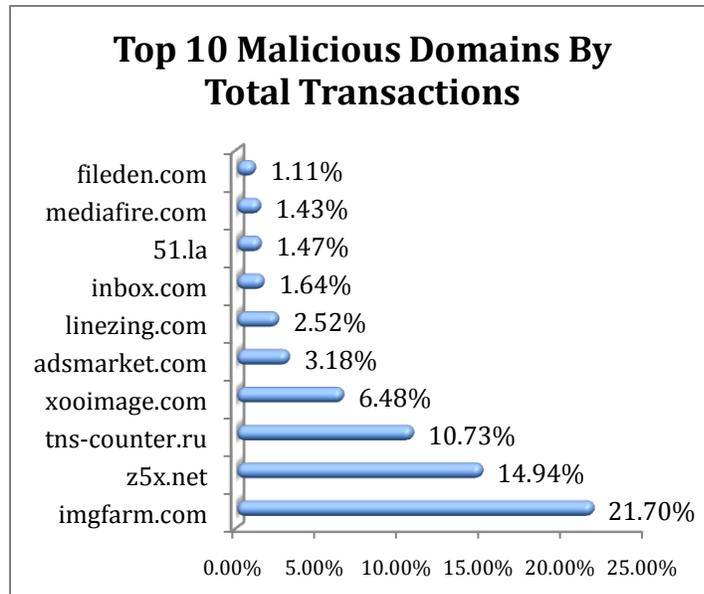
While the majority of malicious traffic originates from servers in the United States, this is to be expected, given that the majority of web traffic in general (good and bad) comes from US based servers. China accounted for the second highest percentage of malicious traffic, while other industrialized countries rounded out the top ten. This quarter, we witnessed a large jump in the rankings for China, which moved up from 5th place overall in Q1, with a quarterly average of 2.97% to 2nd in Q2 with 7.24% of all malicious sites. Overall, China, the Netherlands, Russia and Korea all moved up three or more places in the top ten rankings for the quarter.

Country	Q2 2010		Q1 2010	
	Rank	Avg.	Rank	Avg.
United States	1	54.95%	1	53.56%
China	2	7.24%	5	2.97%
Germany	3	4.18%	2	4.88%
Netherlands	4	3.87%	11	1.38%
Russia	5	2.64%	12	1.35%
United Kingdom	6	2.56%	4	3.69%
France	7	2.51%	8	2.55%
Turkey	8	1.42%	N/A	N/A
Korea	9	1.27%	14	0.92%
Canada	10	1.04%	8	2.58

Note: Turkey was not included in the top 25 countries for the Q1 2010 report.

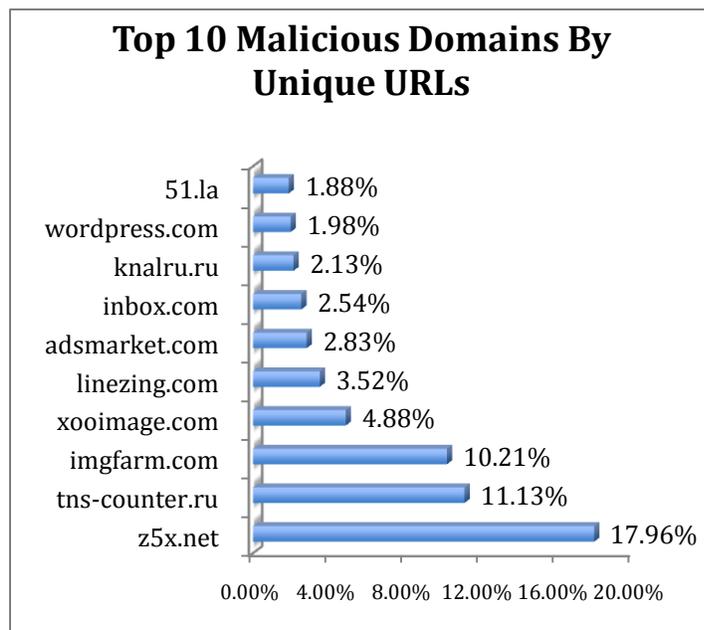
Top Malicious Domains

- Most blocked advertising network: **z5x.net**
- Most blocked adware site: **imgfarm.com**
- Most blocked web counter service: **tns-counter.ru**
- Most blocked hosting service: **xoimage.com**
- Most blocked affiliate network: **adsmarket.com**
- Most blocked malicious domain: **host127-0-0-1.com**



During Q2 2010, the domain *z5x.net* accounted for approximately 18% of the blocked URLs and 15% of the blocked transactions for the quarter. This domain was the number one advertising-related site blocked for the quarter. The reason for the blocks stemmed from past abuse by Trojan "Clicker" software installed on infected systems to monetize advertisement click throughs on the domain. An example of one such artifact can be seen on ThreatExpert, which indicates that the Trojan potentially originated in Russia⁷. In addition, other sources such as WOT⁸ show the site has previously also been used for fake Greencards.

Similar to past quarters, the top adware site blocked is related to the "FunWeb" adware.



The domain *imgfarm.com* accounted for over 10% of the malicious URLs and 21% of the malicious transactions blocked for the quarter. While the FunWeb applications are not necessarily considered malicious, they remain in the unwanted category and are often installed without the user's knowledge or consent. For additional information on this domain and adware, see the adware section of our Q1 2010 State of the Web report.

The *tns-counter.ru* domain is another that is reoccurring quarterly on the "top blocked" list. This domain accounted for about 11% of malicious URLs and transactions for the quarter. It is a web counting/statistic site that has been reported in the past as being abused to spread malware. While the service itself may not be malicious, its past history of abuse has deemed it to be an untrustworthy domain for users to visit.

⁷ <http://www.threatexpert.com/report.aspx?md5=6d1e330bbc964534e79df2c86edfd80e>

⁸ <http://www.mywot.com/en/scorecard/z5x.net>

xooimage.com is a French image hosting service that has made the top of Zscaler's list for the most URLs (4.9%) and transactions (6.5%) blocked to a hosting provider service. This service has been abused in the past to spread a variety of Trojan programs, including Zeus. A simple Google query for "xooimage.com and malware"⁹ reveals a variety of the examples that we saw throughout the quarter.

The domain host *127-0-0-1.com* is tied to Trojan Swizzor. This, along with a number of other related Trojan Swizzor domains, has been resolving to the 66.220.17.X Class C address space (Hurricane Electric)¹⁰. Trojan Swizzor is a small Trojan downloader that is used to download other Trojan downloaders. This specific Trojan Swizzor domain accounted for about 1% of blocked malicious URLs for the quarter.

adsmarket.com is an affiliate network—in other words they pay advertisers to advertise for a number of their customers. It made up about 3% of the blocked malicious URLs and transactions. Often, criminals monetize affiliates by spamming, conducting Blackhat Search Engine Optimization (SEO), or spreading malware to increase visits/purchases/installs for a particular customer.

Wordpress.com provides the WordPress website software as well as a hosting platform for users with WordPress sites. Zscaler saw approximately 2% of its malicious traffic to this domain. This is likely due to the series of attacks witnessed against WordPress sites throughout Q2 2010, in which the compromised WordPress pages would be used to host/redirect visitors to malware. In the below "Incidents" section of this report the WordPress attacks are discussed in more detail.

These numbers in general show that large percentages of "malicious sites" are not necessarily malicious in the classic sense of the word, but rather include a variety of unwanted activities such as advertising and affiliate networks, untrustworthy web counter/stats sites, abused free hosting services, and various flavors of adware. It is imperative, therefore, that these various aspects of unwanted Internet activity are appropriately managed/blocked within an organization.

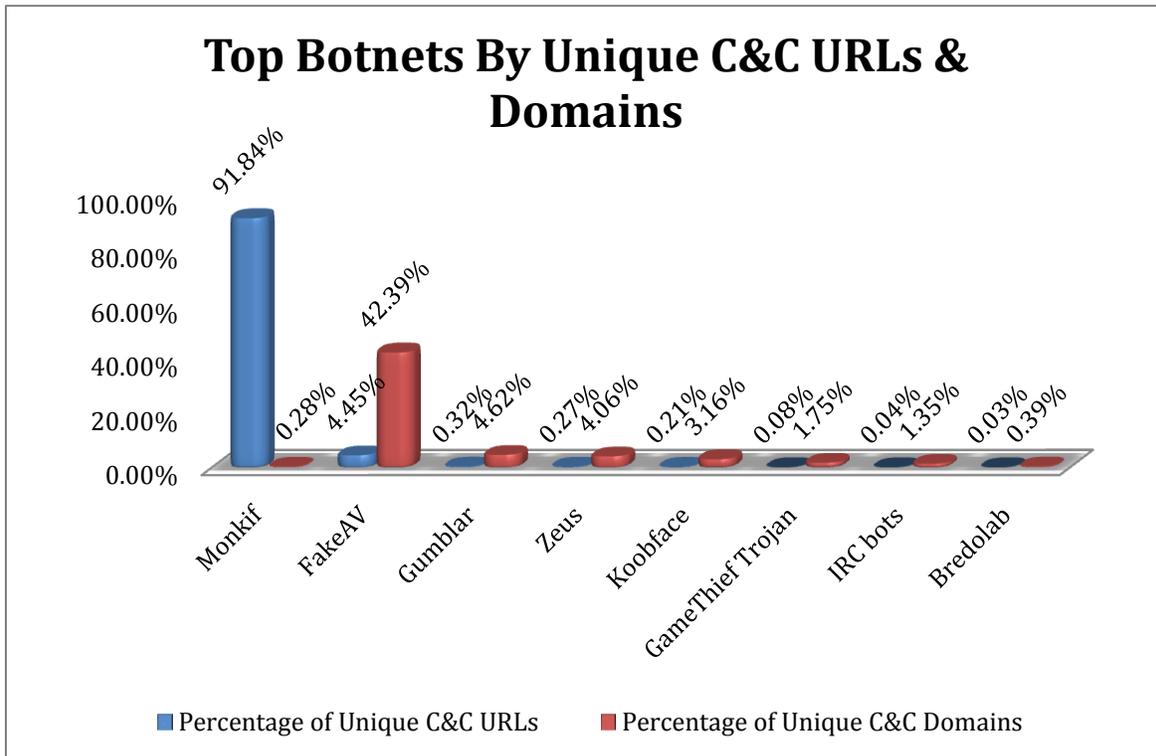
⁹ <http://www.google.com/search?q=xooimage.com+malware>

¹⁰ <http://www.malwareurl.com/listing.php?domain=66.220.17.200>

Malware / Botnets

From the perspective of unique URLs associated with a given botnet, Monkif appears to be off the charts, with nearly 92% of the traffic. This stat is somewhat misleading however, as Monkif tends to leverage a variety of parameters within GET requests, sent to C&C (command & control) servers, which magnifies the volume of unique URLs from this perspective.

Looking instead at the number of unique domains associated with a particular threat, we get a very different picture, with Fake AV campaigns easily taking top spot with over 40 percent of registered malicious domains. This is not surprising given the increasing activity that we have seen with Blackhat SEO attacks, which commonly leverage Fake AV as their social engineering attack vector of choice.



Compared with Q1, the volume of Gumblar domains has increased, going from about 1% to 4.62%, while Torpig/Sinowal has slowed somewhat, not even making the top 10 this quarter with only a small handful of unique domains as opposed to approximately the 1% witnessed in Q1.

Incidents

Facebook 'Likejacking'

In the past quarter, Zscaler has noticed the emergence of Facebook 'Likejacking' – “a malicious technique of tricking users of a website into posting a Facebook status update for a site they did not intentionally mean to 'like'”¹¹. Zscaler first blogged¹² about this problem in June. Of all the Likejacking sites this past quarter, the one that appears to have had the greatest success (highest number of blocked attempts from Zscaler end users) was 101hottestwomen.com.

This Likejacking incident hides an invisible button on the page, leveraging a technique known as clickjacking, so that if the visitor clicks anywhere on the page, the user is unknowingly telling Facebook that they 'like' the page. This and other 'Likejacking' incidents that we have seen are designed to direct traffic to CPALead or other advertising networks in order to generate revenue for the perpetrators behind the incident. CPALead is an affiliate, or advertising network, where their customers pay for its advertising/marketing services. However, its services are essentially 'out sourced' to individuals and groups that are compensated usually in a pay-per-click fashion. Spammers, SEOers, malware authors and others monetize their victims through these services (which are sometimes complicit in the illegal activities). Likejacking is a quick and easy way of increasing traffic volume to a site through an affiliate network.

Mass SQL Injection Attacks

Beginning June 7, 2010 there was a massive SQL injection attack against IIS web servers running vulnerable web applications that interface with a backend Microsoft SQL Server. Zscaler published a blog post¹³ and security advisory¹⁴ on this incident to notify customers.

In the first wave of attacks associated with the incident, affected sites included content from ww.robint.us, which hosted malicious JavaScript that attacked systems vulnerable to CVE-2010-1297, affecting Adobe Flash. Zscaler blocked over 1000 customer transactions to robint.us, in the first 72 hours. Fortunately, the domain was quickly sinkholed, preventing further infection from occurring when users visited the hacked sites.

The next week, the same attack occurred, but redirected users to 2677.in/yahoo.js. Since approximately mid-June, this style of attack has continued, for example with malicious JavaScript hosted at 4589.in/yahoo.js. The continuation of this attack shows the prevalence of web applications vulnerable to SQL injection and the success attackers achieve when infecting visitors.

Malvertising

Zscaler detected and blocked a number of malvertising sites this past quarter, including adnet.media.prananc.com. A large number of these adnet.media.*.com and other related “advertising” domains were registered and injected into hacked web servers. These advertising domains would then act as intermediaries, which would direct victims to drive-by download attack sites.

Many of the fake advertising domains were registered and hosted on the following netblocks:

- 188.72.192.0/24
- 95.143.193.0/24
- 89.248.174.0/23

¹¹ <http://en.wikipedia.org/wiki/Likejacking>

¹² <http://research.zscaler.com/2010/06/likejacking-what-is-it.html>

¹³ <http://research.zscaler.com/2010/06/robintus-case-study-in-mass-website.html>

¹⁴ http://www.zscaler.com/sec_advisory_june10_2010.html

And the drive-by download domains were hosted on:

- 194.8.250.0/24

This subject and these netblocks have been followed closely in MalwareDomainList forum threads¹⁵.

WordPress Hacks

Zscaler first blogged about a number of WordPress hacks in April 2010¹⁶. Since that post, a number of hosting providers: Network Solutions, GoDaddy, Bluehost, Dreamhost, and Media Temple have seen large scale attacks against their WordPress sites.

Using SANS ISC as a timeline, we see the bulk of the attention paid to these attacks occurred in mid-May:

- May 10, 2010 'Another round of WordPress Attacks' (SANS ISC)¹⁷
- May 19, 2010 'WordPress blog attacks ... again' (SANS ISC)¹⁸

These attacks have been ongoing since about mid-April. Recently (mid-June) Rackspace was a target¹⁹. Pointing to a single vulnerability responsible for the increase in compromised WordPress sites is difficult given that it is a popular attack surface with a number of potential weaknesses. WordPress can and has been compromised in a variety of ways: vulnerabilities in the software package (e.g., SQL injection), weak administration credentials, exposed/weak database credentials, misconfigurations and exposure of the site within a shared hosting provider.

Malicious .in Domains

This past quarter, we detected and blocked a number of transactions to malicious .in (India) top-level domain (TLD) sites. Zscaler recently posted a blog on this particular campaign²⁰. A large portion of the malicious .in sites were hosted on the ATECH-SAGADE netblocks (e.g. 91.188.60.0/24). This campaign is ongoing, and the .in domains are being bulk-registered by the criminal(s). The malicious sites host exploit kits to known vulnerabilities on client browsers and applications. Exploit kits are commonly sold in the underground and essentially package a number of known exploits and provide criminals with a point-and-click interface to easily build and deploy malicious web content without the need to fully understand the exploits and how they work. If compromised, the victim downloads and installs various wares/payloads. The purpose of these installs appears to primarily be pay-per-installs that the criminals are able to monetize.

SEO Attacks

We have blogged extensively about the plague of Blackhat SEO attacks that we see each and every day. This problem is growing as search engines fail to tackle it, and AV signatures simply cannot keep pace with the ever-changing binaries used in the attacks. Blackhat SEO involves leveraging SEO techniques to ensure that malicious websites show up in the top results for particular search engine queries. As we have demonstrated through our past research, all major search engines, including Google, Bing and Yahoo!, are targeted and all are struggling to filter the malicious results.

Fake AV has been the most common attack that we've seen tied to Blackhat SEO. Others include various types of software upgrades, such as for Flash Player, codecs required to play videos, and web browser updates, and the overall approach is always the same: convince the victim that they must install a malicious executable.

¹⁵ <http://www.malwaredomainlist.com/forums/index.php?topic=4077.45>

¹⁶ <http://research.zscaler.com/2010/04/wordpress-sites-hacked-again.html>

¹⁷ <http://isc.sans.edu/diary.html?storyid=8770>

¹⁸ <http://isc.sans.edu/diary.html?storyid=8818>

¹⁹ <http://blog.sucuri.net/2010/06/mass-attack-of-wordpress-blogs-on-rackspace.html>

²⁰ <http://research.zscaler.com/2010/07/atech-sagade-badness-malicious-in.html>

The creativity used by attackers is impressive and sadly, the average end user is often fooled. The content used is polished and convincing. We're also seeing the attacks becoming more selective, whereby the victim machine is first probed to ensure that the right attack is delivered. For example, we saw an attack recently that delivered alternate payloads depending upon the web browser involved. If Internet Explorer was detected, the attacker could be confident that the request was coming from a Windows based machine and therefore a Fake AV payload was delivered. If however, the request came from a Firefox browser, a fake Firefox update was instead delivered.

Perhaps most concerning is the fact that anti-virus vendors are failing to combat this threat. We typically find that the binary files associated with attacks are detected by fewer than a quarter of AV vendors at the time of the attack.

While there are literally hundreds, if not thousands, of search terms targeted each day, below are some of the more significant events and news stories that we identified throughout the quarter. Be sure to follow up on our related blog posts if you'd like further detail on a particular attack.

Topic	Search Terms	Notes
Events	"tax day freebies" ²¹	Fake AV campaign
Calendar Events	April Fool's Day ²² - "Google april fool" - "Google Topeka" - "april fools 2010 wiki" Mother's Day ²³ - "Mother's Day 2010"	Advertising scams
Celebrity Rumors	"beyonce pregnant confirmed" ²⁴	Numerous malicious links in top 100 results
News Stories ^{25,26}	"Camden 5" "Tri Energy" "american idol top 2" "american idol top 3"	Google, Bing and Yahoo! all affected
Sporting Events	"2010 nba draft order" ²⁷ World Cup - numerous ²⁸	Fake codecs

²¹ <http://research.zscaler.com/2010/04/video-first-link-on-google-leads-to.html>

²² <http://research.zscaler.com/2010/04/search-engines-need-to-protect-their.html>

²³ <http://research.zscaler.com/2010/05/elaborate-scam-for-mothers-day.html>

²⁴ <http://research.zscaler.com/2010/04/search-engines-need-to-protect-their.html>

²⁵ <http://research.zscaler.com/2010/04/search-engines-need-to-protect-their.html>

²⁶ <http://research.zscaler.com/2010/06/spam-seo-trends-statistics-part-i.html>

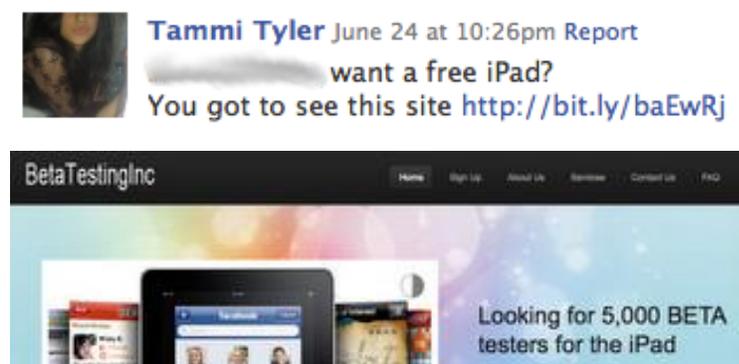
²⁷ <http://research.zscaler.com/2010/06/spam-seo-trends-statistics-part-i.html>

²⁸ <http://research.zscaler.com/2010/06/world-cup-black-hat-seo-list.html>

Phishing

While phishing may have one of the lowest barriers to entry from an attack perspective (requiring only a clever social engineering attack), it remains a highly profitable enterprise. We are constantly impressed with the level of creativity that we see in such attacks. Modern phishing attacks are far broader than their predecessors that largely targeted financial credentials. Phishing attacks today are going after social networking credentials (i.e. Twitter and Facebook), MMORPG games with established after markets (e.g. World of Warcraft) and attacks tied to current events.

iPad Beta Testing Phish



The world saw the release of the iPad this past quarter, and needless to say it immediately became a popular and coveted tech gadget. That popularity attracted a number of fraudsters who jumped at the chance to offer iPads to gullible victims that were willing to provide their personal credentials (email, financial, etc.). One such scam seen was the *iPad beta testing* scam.

Watch World Cup Live Phish

Toward the end of the quarter was the start of World Cup – arguably one of the most popular international sporting events. Given the date and times of many of the games, many North American fans had to turn to the Internet to stream their team’s games while they were at work. Searching for sites that offered streaming of World Cup games turned up a large number of shady sites. Many of these sites linked to an affiliate site (for example, tvprocessing.com). Those advertising/spamming World Cup streaming sites profited from their traffic volume to the affiliates, and it appeared that in some cases these sites would also harvest financial credentials. Examples of such sites can be seen in a June Zscaler blog post²⁹ on this subject.

Twitter Followers Phish

Zscaler first blogged about “Twitter follower” phishing sites that harvest Twitter credentials from people seeking to boost their number of followers back in November 2009³⁰. While these sites are not new, their prevalence has increased. Zscaler blocked a number of customer transactions to such sites this past quarter. Below is a small sample of domains seen and blocked this past quarter:

- mytweetfollowers.net
- freetwitterfollowers.net
- followwizard.com



²⁹ <http://research.zscaler.com/2010/06/watch-live-world-cup-fraudscams.html>

³⁰ <http://research.zscaler.com/2009/11/twitter-follower-scams.html>

- twitterfollowerspro.com
- superfollows.com
- fastfollowers.net
- followmaker.com
- followerparty.com
- followpit.com

From the harvested Twitter credentials, the fraudster can use or sell the compromised accounts to further spam this and other frauds or malicious sites.

CONCLUSION

One thing that is abundantly clear as we research threats for our quarterly reports is that – attackers adapt almost instantly to adopt popular web functionality or leverage breaking news to target victims, and further to stay one step ahead of defenses designed to protect corporate users. Attacks are also dynamic in nature, delivering customized content designed to maximize the likelihood of success. As such, static protections that either pre-screen content or simply block known bad destinations are sure to fail. Only by inspecting traffic in real-time, even when encrypted, can these attacks be detected.

As a SaaS vendor, Zscaler is in the unique position to not only inspect traffic inline, but also has access to vast volumes of historical traffic that can be analyzed to uncover anomalous patterns which regularly leads to the discovery of previously unknown threats. The ever-changing threat environment makes for fascinating research insofar as attackers never fail to impress us with their creativity. We've come to a point where it's not a question of *if* breaking news will be leveraged in a SEO attack or *when* a new social networking feature will be abused, but rather identifying the first attack, understanding it and anticipating its evolution. What will attackers have in store for us next quarter? Time will tell, but we know we won't be disappointed.