

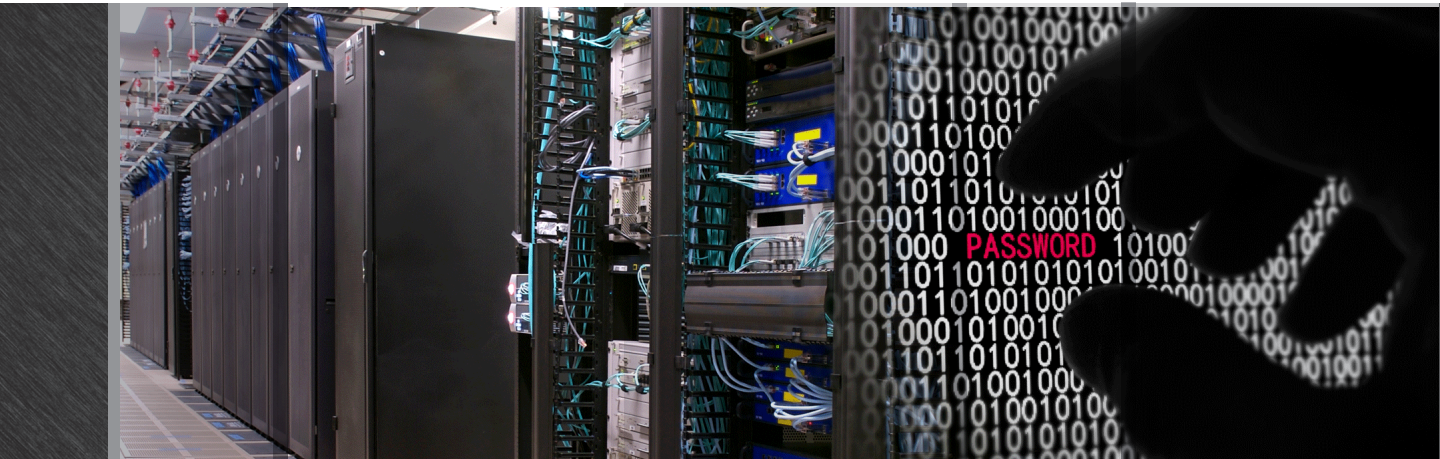


CAROLINA ADVANCED DIGITAL, INC.
IT INFRASTRUCTURE | SECURITY | MANAGEMENT

www.cadinc.com | 800.435.2212

Blue Coat

White Paper



2011 Mid-Year Security Report >

Executive Overview

Innovation breeds opportunity, even for the underground. Web and mobility innovations focus on ease of use, availability, and building large user audiences, but they breed opportunity for cybercrime. Security typically comes later, after a period of breaches and security issues put the issue front and center. Halfway through 2011, we are in the midst of this security period.

The majority of web threats are now delivered from trusted and popular web sites that have been hacked for use by cybercrime. For this reason, reputation defenses become less effective. The once obscure link farm for search engine poisoning now resides within popular web sites. The exception for link farms is now a rogue domain or remote web location. Phishing attacks overwhelmingly come from popular and trusted web sites hacked by cybercrime. The recent large-scale accumulation of user identities and email IDs by cybercrime only raises the concern for phishing attacks and Advanced Persistent Threats (APTs) that target specific organizations and users.

Search engine poisoning (SEP) ranks as the number one web threat delivery method at this point in the year. To be more specific, image searches have passed text searches and are now the top vector for malware delivery. Pirated movies and games and adult content, are top lures as new devices provide a high-definition entertainment landscape for users. Web pages are often dynamically created for SEP attacks, emphasizing the value of real-time web rating and threat-analysis defenses. Spam related to pirated movies and games is also making a comeback, delivering fake-codecs or fake-warez dynamically leading to malware.

The web sites we trust are cybercrime's entry points into our lives. Given that web sites today contain thousands of dynamic web links to various content types and sources, innovations like malvertising now rank as the second most popular web threat delivery method halfway through 2011. Cybercrime resides patiently in multi-tier ad networks and selectively picks targets and assesses exploits and vulnerabilities. When the opportunity is open, it strikes. Patience and selective analysis provide a better return on investment than the mass injection attacks of years past.

Week-over-week analysis shows SEP at a steady volume with a tidal effect of highs and lows. For malvertising, the charts are full of peaks and valleys as attack volume changes dramatically day over day and often within a 24-hour period. Research on dynamic web links shows cybercrime is quickly moving to new domains and IP addresses – faster than in years past. While some long-lived cybercrime sites continue to exist, the trend is speed of transfer to new identities and locations to evade detection.

From a user agent perspective, some Mac users are searching for pirated goods and images and falling into known malware delivery vectors. While exploit kits today focus on Windows users, many Mac users have their noses pressed against the glass of cybercrime. When cybercrime's focus switches to the Mac, these users will be lined up like lambs. Before 2011 ends, it would not be surprising to see Mac users facing web threat issues themselves.

Tracking Malware Networks

Lures are dynamic, and so are payloads. On the other hand, the infrastructure of malware delivery networks requires time and effort to maintain and operate. While a news break or celebrity action catches our attention, using these as lures requires a malware network that is ready to herd web users effectively. Below is an image from Blue Coat WebPulse™ cloud defense, operated by Blue Coat Security Labs, of web sites known to deliver web threats and their correlations to each other. Malware delivery networks are spread out over multiple web sites – many of them popular and trusted – to evade detection by reputation analysis. It is now very common for web threat delivery and phishing attacks to hide within reputable Web sites. Rarely are all the attack elements kept within one web site.

Malware Delivery Networks and Their Correlated Web Sites

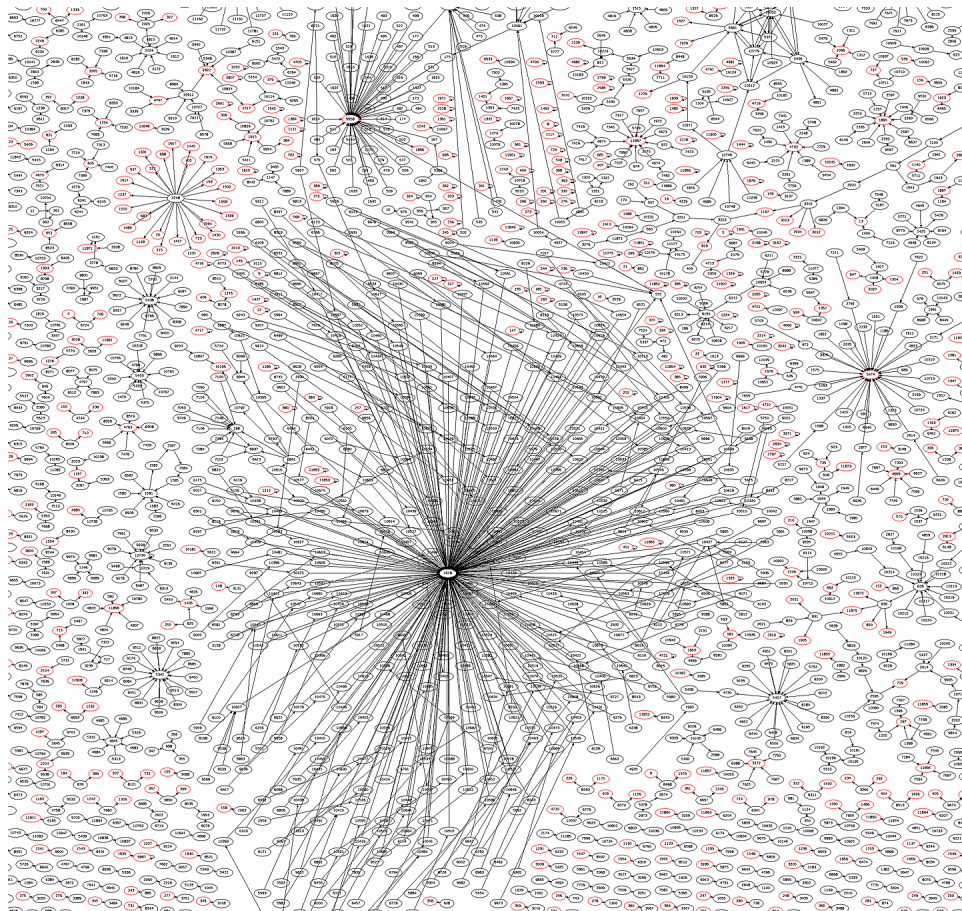


Image 1 - Source: Blue Coat Security Labs

Graphical mapping software makes it easy to see how the large malvertising network in the center of the image above pulls unsuspecting users into the attack. You can also see many other smaller circle correlations of interrelated web sites working dynamically together to herd users and deliver web threats. The vertical lines of ovals (web sites) at top center are pornography ladders.

On any given day, the number of unique malware networks varies. In the first half of 2011, malware networks ranged from just under 100 operating in a single day to fewer than 25 in operation.

Unique Malware Delivery Networks per Day

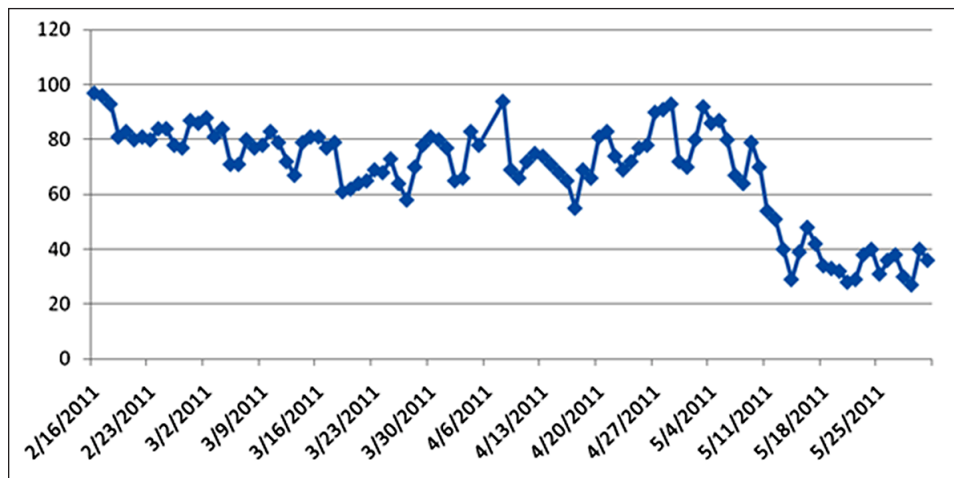


Chart 1 - Source: Blue Coat Security Labs

Chart 1 shows the number of unique malware networks seen each day, with a drop off in mid-May as networks relocated and consolidated. Overall, 395 unique malware networks were under observation as of the end of May. For the last 30 days covered by the chart, an average of 50 unique malware networks was seen each day.

Table 1 ranks malware delivery networks based on the number of attack hosts. The table shows both the average number of nodes as well as the minimum and maximum number of nodes during the first half of the year, which demonstrates the dynamic nature of these networks.

Top 10 Malware Delivery Networks by Number of Unique Host Names

	Malware Delivery Network	Number of Hosts			Primary Malicious Activities
		Average	Min	Max	
1	Shnakule	2001	560	4357	Drive-by downloads, fake anti-virus (AV), fake codecs, fake flash updates, fake warez, fake Firefox updates, and botnet / CnC controls NOTE: Interrelated activities include pornography, gambling, pharmaceuticals, link farming, and work-at-home scams.
2	Ishabor	766	393	1140	Fake AV
3	Cinbric	505	21	1602	Pornography-themed ransomware
4	Naargo	199	58	299	Pornography-themed network NOTE: Not categorically a malware network, but its suspicious nature merits continued tracking and investigation.
5	Vidzeban	156	12	347	Fake warez NOTE: This network has a significant presence of Russian-language pages.
6	Thonaki	99	37	169	Fake AV
7	Kulerib	96	1	325	Drive-by downloads and gambling-themed malware NOTE: Interrelated activities include pornography, gambling, pharmaceuticals, and work-at-home scams
8	Rabricote	72	8	254	Suspicious link farming
9	Ananghee	62	1	106	Fake AV
10	Albircpa	61	43	80	Fake AV and drive-by downloads

Table 1 - Source: Blue Coat Security Labs

While Ishabor, Kulerib, Rabricote and Albircpa were initially believed to be self-contained networks, it has been determined that they are actually components of the larger Shnakule malware delivery network.

For a perspective on how the size of the malware delivery networks fluctuate on a daily basis, Chart 2 shows the number of unique hostnames (or unique attack hosts) generated per day in April and May.

Unique Hostnames per Day for Top 10 Malware Delivery Networks

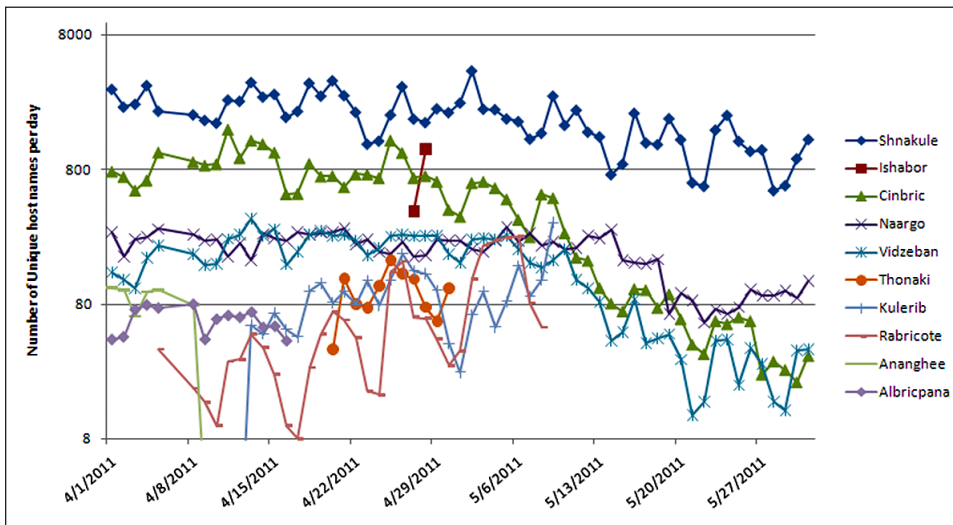


Chart 2 - Source: Blue Coat Security Labs

Shnakule has been the dominant malware delivery network while Cinbric and Vidzeban have declined. Ishabor was short-lived; however, in two days it produced over 1,500 unique host names before becoming part of Shnakule to create a larger malware delivery network.

The dynamic nature of web attacks surfaces in the charts and tables very quickly. As Google Earth displays cities, roads and buildings, the Blue Coat WebPulse cloud defense maps out malware delivery networks. Unlike building addresses, however, host names change very quickly.

Table 2 ranks malware networks based on the number of initial requests per day, over a 60-day period, that were made automatically to WebPulse rating servers by Blue Coat ProxySG appliances. Where Table 1 ranked the size of the malware delivery networks, this table ranks their effectiveness in driving users to the networks.

Top 10 Malware Delivery Networks by Initial Ratings Server Requests

	Malware Delivery Network	Number of Requests			Primary Malicious Activities
		Average	Min	Max	
1	Shnakule	21263	4555	51539	See Table 1
2	Ishabor	4303	2717	5888	See Table 1
3	Shangvos	2899	0	5892	Malicious downloads
4	Tonenuro	2105	1766	2444	Fake AV
5	Ostroka	1832	0	11636	Suspicious Facebook surveys and scams
6	Thonaki	1768	911	2919	See Table 1
7	Vidzeban	1637	12	3741	See Table 1
8	Ananghee	1557	0	3613	See Table 1
9	Nakinakindu	1486	799	2507	Drive-by downloads NOTE: Believed to be a component of Shnakule
10	Abewesban	1330	669	1755	Fake AV

Table 2 - Source: Blue Coat Security Labs

For Tables 1 and 2 fifteen unique malware delivery networks are highlighted. This is just a small sample of the nearly 400 unique malware delivery networks under observation by Blue Coat Security Labs during the first half of 2011.

In the below chart, malware delivery networks are ranked by the number of initial requests to ratings servers. The chart sh malware delivery networks is shown in Chart 3 below.

Initial Requests per Day to Rating Servers for Top 10 Malware Delivery Networks

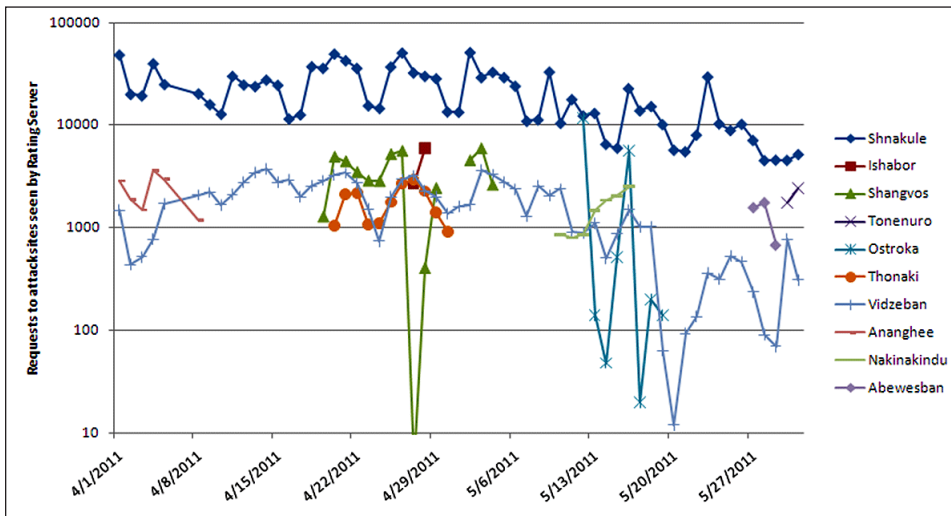


Chart 3 - Source: Blue Coat Security Labs

The chart shows the number of initial web requests to malware sites rated by WebPulse-cloud-hosted rating servers. The rating is provided in real time, and then cached within deployed ProxySG devices. Subsequent web requests are rated locally at customer sites by the ProxySG using the URL rating cache, so the true number of web requests to these malware networks made by users behind ProxySG devices is much greater.

While the charts, tables and malware delivery network descriptions are interesting and show the dynamic nature and volume of web threats, the question of what users are doing to fall into these malware networks remains open. Chart 4 shows the five leading categories (or sources) through which unsuspecting users enter the observed malware networks under observation.

Top Five Categories for Entering into Malware Delivery Networks

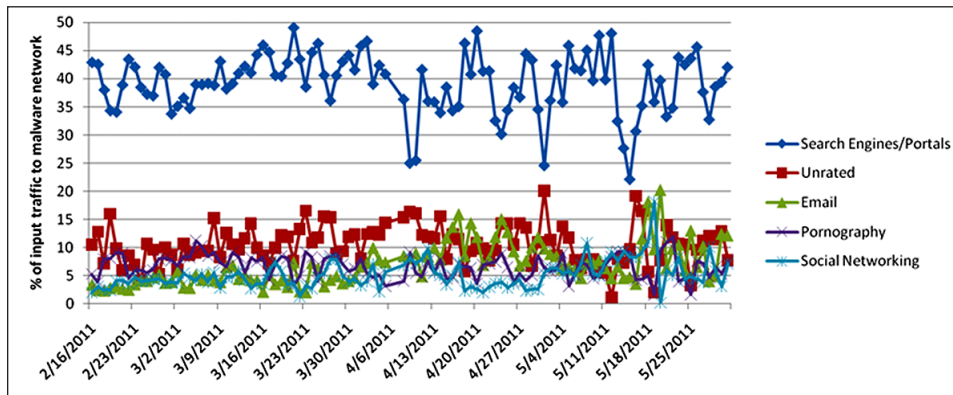


Chart 4 - Source: Blue Coat Security Labs

Search engine poisoning ranks as the leading malware delivery vector for the first half of 2011. Malvertising is not category-specific and is not shown on chart 4, but it ranks as the number two malware delivery vector based on research analysis. Conservative or high-security networks may opt to block unrated web requests knowing they rank third for inducing users into malware delivery networks. Social networking, pornography and email are in a tie for fourth place. Table 3 below shows how the categories compare as entry points to the malware delivery networks under observation.

Top Five Categories for Entering Malware Networks by Percentage of Requests

	Average	Min	Max
Search Engines/Portals	39.20%	22.07%	49.11%
Unrated	10.53%	1.16%	20.10%
Email	6.90%	2.04%	20.19%
Pornography	6.70%	1.59%	11.85%
Social Networking	5.16%	0.21%	18.19%

Table 3 - Source: Blue Coat Security Labs

Correlation of these topics shows that searches for adult or pornographic images rank as an important web request to block. People like to look at other people and human nature is unlikely to change. As noted in the 2011 Blue Coat Web Security Report (February 2011), pornography was third in terms of malware delivery and web threats. The report also noted spikes of up to 110,000 new pornography sites in a single day. This emphasizes the importance of a real-time web defense that can rate new web content and uncover dynamic web links to known malware delivery networks or entirely new web threats.

Botnet Analysis – Evidence of Sharing

In the first half of 2011, the news of numerous breaches, stolen identities, possible source code theft and financial fraud has made security issues top of mind and will drive changes in defenses, policies and risk profiles. The trends toward shared resources among cybercriminals and mass market malware are both serious developments that are also driving an evolution in web security.

For the first five months of 2011, the most-detected botnets, command-and-control (CnC) networks, trojans and worms are shown in Table 4. ZEUS is well known in financial fraud cases for key-logging access credentials to online financial accounts. SALITY has been associated with the Daprosy worm, one of the most destructive in the past decade. KOOBFACE (an anagram of Facebook) is propagated within social networking sites and infects Windows and Mac systems, and even Linux systems to a limited extent.

Most Prolific Botnets / C&C Networks / Trojans / Worms

1	TROJAN-REGISTRY-DISABLER/Gen:Trojan.Heur.VB.dm0@gWscL@gj
2	ZEUS/MUROFET/SPYEYE
3	SALITY
4	Trojan-Downloader.Win32.Agent.eckq
5	A Specific Suspected Spamming Trojan (calculated via Web Reputation)
6	WALEDAC*
7	MEBROOT/SINOWAL/TORPIG
8	DELSNIF
9	HILOTI
10	TROJAN-PROXY/Trojan.Win32.Agent.didu/Win32/SpamTool
11	KOOBFACE
12	TDSS
13	PUSHDO/CUTWAIL/PANDEX
14	CARBERP
15	KAZY*
16	BREDOLAB*

Table 4 - Source: Blue Coat Security Labs

*Many of these botnets' infected nodes share similar "botnet space." (That is, end-user systems appear to be infected with multiple botnet-producing trojans. Each exploit is making phone-home requests with respect to its own functionality). The quid pro quo, the sharing of the botnet space, exists.

Many botnets are known to intersect and share their compromised nodes in a symbiotic relationship (which they do with more monetizable malware, such as ransomware, pharmacy spam, scams, and a variety of other exploits). The samples analyzed, sandboxed, researched and studied by Blue Coat Security Labs exhibit this characteristic.

It's a good idea to validate web sites by checking certificates and to warn users about sites without authorized certificates. VirusTotal, used by many professionals and end users for checking files or URLs against 40+ anti-malware engines for threats, had a fake site as of early June 2011, according to Kaspersky Lab. The fake site delivers a worm that recruits user systems into a botnet for distributed denial of service (DDoS) attacks. It also communicates to command-and-control (CnC) servers with host characteristics, according to reports from Net-security.org published in late May. According to reports, VirusTotal was also impersonated in February 2010 to distribute 'scareware' to visiting users.

Web Filtering Category Analysis

At the mid-year point for 2011, analysis of the 15 most requested categories, based on analysis from the WebPulse community of over 75 million users, shows that most rankings are similar to those in the 2010, with a few exceptions.

The Top 15 Most Requested Web Categories

	January-May 2011	2010
1	Search Engines/Portals	Search Engines/Portals
2	Computers/Internet	Web Advertisements
3	Social Networking	Computers/Internet
4	Web Advertisements	Social Networking
5	Content Servers	Content Servers
6	Audio/Video Clips	Audio/Video Clips
7	Open/Mixed Content	News/Media
8	News/Media	Shopping
9	Non-viewable	Reference
10	Shopping	Open/Mixed Content
11	Reference	Business/Economy
12	Business/Economy	Chat/Instant Messaging
13	Entertainment	Entertainment
14	Personal Pages/Blogs	Non-viewable
15	Chat/Instant Messaging	Personal Pages/Blogs

Table 5 - Source: Blue Coat Security Labs

The first exception is Social Networking, which has climbed up the rankings to edge Web Advertisements out of the third. This is quite an accomplishment, given that the top three requested categories are the pillars of web traffic categorization and request volume and rarely change.

Social Networking is becoming its own web communication ecosystem. Blue Coat WebFilter provides up to four category ratings per web request and provides over 45 secondary category ratings within the Social Networking category. This allows policy controls on Games, IM/Chat, Email and other categories within Social Networking, or on specific social networking domains such as Facebook.com. New web application and operation controls go a step further and enable policy controls by specific web application name and operation. Examples of operations are upload video or picture, upload or download attachments, post a message, or send an email.

The other interesting exception for the first half of 2011 is the climb of Open/Mixed Content up three positions to seventh. The concern here is that Open/Mixed Content had the highest growth rate for hosting malware – up 29 percent year over year from the 2010 analysis. Examples of Open/Mixed Content web sites are image sites (for example: istockphoto.com, fotosearch.com, imagebarn.com) plus video hosting sites (for example: google.video.com and youtube.com). In general, Open/Mixed Content sites have random non-offensive content not organized to be placed into a specific category. However, they may have objectionable content.

K9 Web Protection is a free home consumer web defense product provided by Blue Coat. While the user population is less than five percent of the total WebPulse community, the K9 population provides over 15 percent of web threat and unrated content samples to WebPulse and is by far the most interesting user population from an analysis perspective.

Top 15 Most Requested Web Categories for K9 Web Protection Users

	January – May 2011	2010
1	Computers/Internet	Computers/Internet
2	Software Downloads	Search Engines/Portals
3	Non-viewable	Audio/Video Clips
4	Online Storage	Online Storage
5	Search Engines/Portals	Software Downloads
6	Social Networking	Non-viewable
7	Chat/Instant Messaging	Education
8	Web Advertisements	Reference
9	Content Servers	Open/Mixed Content
10	Unrated	Shopping
11	Open/Mixed Content	Social Networking
12	News/Media	Content Servers
13	Audio/Video Clips	News/Media
14	Online Games	Pornography
15	Shopping	Financial Services

Table 6 - Source: Blue Coat Security Labs

Interestingly, Software Downloads and Online Storage are the second and fourth most requested categories for K9 consumer and home users. Online Storage had 13 percent year-over-year growth for malware hosting based on 2010 data analysis. Non-viewable sites are often tracking and web analytic sites with content that is not viewable in web browsers; however these web requests are tracked by WebPulse.

On average, users at work are more interested News/Media, Business/Economy, and Reference categories than K9 consumer or home users, which is not a surprise. Interestingly, pornography shows up in the top 20 categories for business user analysis but not for K9 home users. Of course, K9 Web Protection may have been used to block pornography at home, so users may be making an effort to view it at work instead.

K9 Web Protection can be downloaded from www.k9webprotection.com and runs on IOS devices (iPads, iPhones), Mac and Windows systems (PC or tablet).

Malware Hosting

As mentioned earlier, malware delivery networks are now hiding in legitimate sites that are typically allowed by acceptable use policies. Table 7 shows the leading categories for hosting malware (versus delivery) for the first half of 2011.

Top 10 Categories Hosting Malware

January – May 2011		2010
1	Online Storage	Suspicious
2	Software Downloads	Online Storage
3	Pornography*	Pornography*
4	Open/Mixed Content	Computers/Internet
5	Computers/Internet	Search Engines/Portals
6	Placeholders*	Open/Mixed Content
7	Phishing*	Personals/Dating
8	Hacking*	Web Hosting
9	Online Games*	Software Downloads
10	Illegal/Questionable*	Phishing*

Table 7 - Source: Blue Coat Security Labs

The categories marked with an asterisk should be blocked to follow best practices for web filtering and security.

Four of the top five categories for typically considered acceptable usage and are allowed by most corporate IT policies. Year-over-year growth in the Open/Mixed Content and Online Storage categories is a major concern as reported in the 2011 Blue Coat Web Security Report.

Summary

We can summarize these findings with a few key points:

Malware hosting is often found within categories that users are allowed to visit.

->SEP ranks No. 1 for malware delivery, followed by malvertising and unrated sites. Social Networking, Pornography and Email are tied.

Pornography remains as the last 'old school' lure. New adult web sites are generated daily, which makes real-time web content analysis and threat detection a requirement.

->Users searching for images and pirated media are a prime concern. Their activity ranks at the top of the list for possible malware delivery. Stolen user identities put phishing near the top of the list, plus spam for rich media, fake codec updates, and fake-warez.

The overriding conclusion is that a single defense layer is insufficient, and that real-time web defenses are needed. The analogy with Google Earth holds: it provides a map of cities, streets and buildings, while a real-time web defense maps malware delivery networks and correlates dynamic lures with delivery paths and dynamic payloads.

As it stands, users often face the web with no more than anti-virus software and simple URL filtering of known static sites. In the midst of some of the most significant cybercrimes in history, real-time web defenses should be added in a multiple-layer defense scheme. Cloud-hosted defenses can expand and adapt more quickly to new web threats than on-box defenses, and they benefit from collaborative real-time user inputs to generate great awareness of new web threats and content. Cloud security intelligence can be added to web gateways and remote users in a real-time hybrid architecture, or provided as a Cloud Security SaaS.

One click opens the door to cybercrime. The single dynamic web link needs real-time analysis to protect your users, your resources and your reputation.

Credits

This report was authored by Tom Clare and edited by Craig Kensek.

Security research contributions were from Roger Harrison, Chris Larsen, Tim van der Horst, Tyler Anderson, Patrick Cummins and Ben Hanks.

Appendix – The New Threat from Malvertising

Virtually all of the free web services we use regularly – from searches to email, maps to social networking, and even gaming and video sites – are free only because they are funded by online advertising. Online advertising is a huge multi-billion dollar business, supported by a large multi-layer ad network infrastructure. And it is effective not only for legitimate advertisers, but also for cybercriminals. Indeed, in security vendor Blue Coat Systems' 2011 Web Threat Report, malvertising (as in malware advertising) has come from nowhere to arrive at the No. 3 position in their Top 10 methods for web attack in 2010. Let's look at how this new phenomenon works, and draw some conclusions about how best to confront it.

Online Advertising and Malvertising

Ad networks operate on an Affiliate Marketing model, where advertisers place campaigns with a large number of publishers – large and small – that are paid media fees by referral on some measurable action that tracks traffic to the advertiser. The complex affiliate network acts as an intermediary between publishers and affiliate programs – B2B arrangements that pay according to the number of people who visit the page containing the merchant's online ads, see it or click-through to the call-to-action in the ad itself.

This infrastructure is large and complex, with huge numbers of tiny transactions, huge numbers of business relationships, and huge numbers of linked connections between ads and click-through destinations. Larger, well-known trusted ad network domains may outsource to smaller, newer and perhaps not-so-trusted ad domains. With many degrees of separation and automation between the merchant placing the ad and the space where the ad ends up being placed, reputations and trust are often assumed or inherited through the layers of the affiliate network.

Cybercrime loves to leverage other people's trust and reputation – as well as their infrastructure – to deliver malicious software to as many people as possible. Injecting a malicious ad into a legitimate ad network enables the cybercriminal to cast a very large net without necessarily making a splash that can be detected.

Anatomy of a Malware Attack

The following is a typical malware event observed by Blue Coat Security Labs that recently hit India.

- Like most free news sites in the world, one of India's primary entertainment news sites – screenindia.com – is supported by ads.
- One of the third-party links for ads led to doubleclick.net, a well-known, well respected large ad domain. The ad in this case was an infected trusted ad.
- From doubleclick.net some JavaScript led to daniton.com, which appeared to be a trusted part of the affiliate network.
- On the initial visit to daniton.com the ad site did nothing, but a subsequent visit delivered a heavily encrypted piece of JavaScript.
- The JavaScript from daniton.com resulted in an iFrame tag injection into the original host page.
- The iFrame silently requested the user's web browser to call the true malware host (which, interestingly, was observed to change location each day) to download a PDF exploit file.
- Also interesting: one of the functions of the iFrame was to find the user's version of Acrobat Reader so it could leverage the "exploit" that matched that version to give it the best possible shoo-in.

Cybercriminals will either:

- > Create a harmless new ad or ad domain that – once trusted, reputable and allowed by most defenses – transforms into something nasty, or
- > Infect someone else's trusted web ad, using the same kind of injection or poisoning methods they use to infect trusted, reputable websites

A criminal malvertising campaign is run like any real ad campaign, but in both cases the point is to suddenly and silently rewire the ad itself or its click-through to deliver a malware payload. The payload then infects the user's computer, steals logins and passwords, or steals money or data from their employer.

Let's look first at how ads get from the affiliate network to the web page, and how cybercriminals take advantage of the affiliate network infrastructure that characterizes the world of online advertising.

Typically, a web property owner offers ad space to a primary ad vendor – the one the owner has a relationship with. It's all automated so when a page is populated by, say, a new news article, keywords in the article are made available to the primary ad vendor's software. For example, with keywords "Golf" "Florida" and "Luxury", we'd want to target people interested in upscale fly-drive golfing holidays to the Florida Keys. The software figures out whether it has a highly relevant ad that it can use. If the primary ad vendor does not have an ad that targets those people, or hits a cost threshold about placing an ad there on behalf of its client, it's programmed to fall back to placing a less targeted ad (at a lower rate) from one of its affiliates. If the affiliate doesn't have an appropriate ad or is unwilling to pay even the secondary rate to serve a generic ad, they may opt to serve a cheap/generic ad from one of their affiliates. And so on down the chain.

Clearly, this mesh of affiliate/partner/sub-affiliate agreements and fuzzy responsibility between ad networks provides a tremendous opportunity for a rogue ad – or a rogue ad domain – to slip through.

Now, like all web advertising, malvertising ads may be targeted (by keywords like "clearing house" or "data protection") to maximize their effectiveness, and themselves create a kind of dynamic but targeted linkage between sites, all designed to attract and draw a particular type of viewer.

Transformation and Timing Tactics to Circumvent Security

A key feature of malvertising attacks is that the bad ad or the bad ad domain will start off innocently, allowing itself to be checked many times by security software to develop clean ratings and a good reputation.

Like a sleeper cell in a spy novel, patience pays. Taking time to develop clean reputations within ad networks, and passing multiple sweeps for malware, cybercrime develops valuable and trusted positions within Web advertising structures before launching attacks leads to a very successful campaign. When the sleeper awakes, routing behind the ad is transformed to take the view or the click-through to a malware host, and the malware connections are able to do their worst in their targeted campaign. Then the next day, they're gone.

Cybercrime's malvertising tactics tend to launch attacks over the weekend when IT resources are low, defense updates are waiting to be applied and an attack is less likely to be noticed. Remember, classic web defenses are geared towards updates – a new database has to be applied before the security systems can act on the new threat.

Essential Techniques and Technology to Take the Sting Out of Malvertising

Cybercrime waits often months to establish legitimate ad infrastructures to bite users at a selected optimal time and penetrate past reputation-based defenses. So it is clear that, when faced with malvertising, your security systems can't rely on reputation to decide which ads to block. Instead, we need to look to advanced security systems that rate web properties and the ads they depend on in real-time.

Similarly, we can't rely on waiting for a "security update" to be applied to the user's computer. It's probably going to be too late. If your security system has any kind of regular "Click here to update definitions file" requirement, it will likely fail to protect your users, especially on the weekend. Protecting users at home or on the road – or even at the office – has to be provided on-demand, and you should look to security systems that are based on some kind of cloud-based security model that offers on-demand protection.

Appendix Credits

The Appendix was authored by Dave Ewart with contributions from Chris Larsen.



CAROLINA ADVANCED DIGITAL, INC
IT INFRASTRUCTURE | SECURITY | MANAGEMENT

www.cadinc.com | 800.435.2212



Blue Coat Systems, Inc. • 1.866.30.BCOAT • +1.408.220.2200 Direct
+1.408.220.2250 Fax • www.bluecoat.com

Copyright © 2011 Blue Coat Systems, Inc. All rights reserved worldwide. No part of this document may be reproduced by any means nor translated to any electronic medium without the written consent of Blue Coat Systems, Inc. Specifications are subject to change without notice. Information contained in this document is believed to be accurate and reliable, however, Blue Coat Systems, Inc. assumes no responsibility for its use. Blue Coat, ProxySG, PacketShaper, CacheFlow, IntelligenceCenter and BlueTouch are registered trademarks of Blue Coat Systems, Inc. in the U.S. and worldwide. All other trademarks mentioned in this document are the property of their respective owners.

v.WP-2011 MID-YEAR SECURITY REPORT-V1-0611