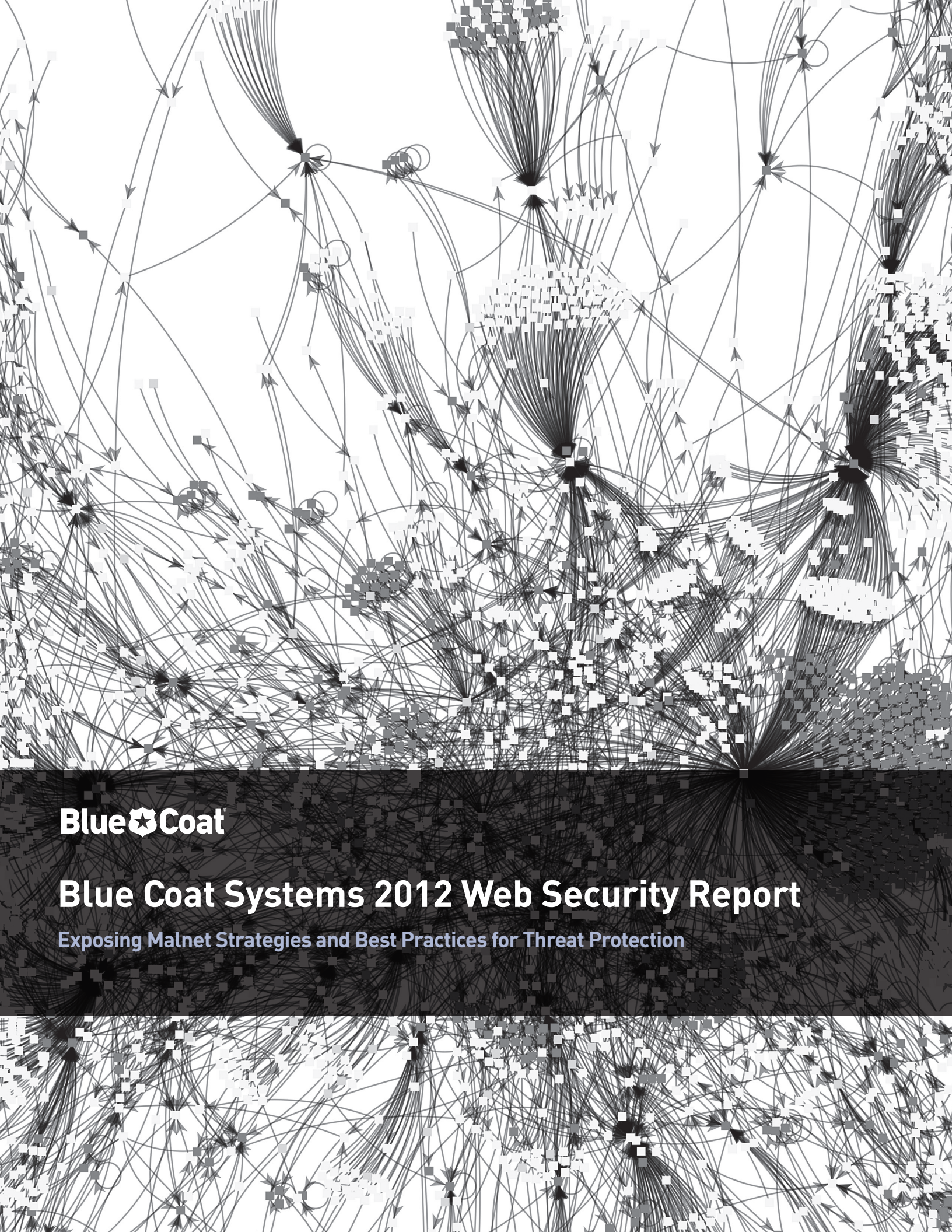


Blue Coat

Blue Coat Systems 2012 Web Security Report

Exposing Malnet Strategies and Best Practices for Threat Protection

Table of Contents

State of the Threat Landscape

In 2011, malnets (malware networks) emerged as the next evolution in the threat landscape. These infrastructures last beyond any one attack, allowing cybercriminals to quickly adapt to new vulnerabilities and repeatedly launch malware attacks. By exploiting popular places on the Internet, such as search engines, social networking and email, malnets have become very adept at infecting many users with little added investment.

Driven in part by malnet activity, malicious sites increased 240 percent in 2011. The increase can be attributed to a combination of factors. Chiefly, cybercriminals are more quickly rotating through domain names. As malicious software kits have become easier to buy, customize and deploy, there are also more people distributing malware.

The vast majority of attacks target users on their desktops and laptops. However, the explosion of mobile devices gives cybercriminals a new platform. While attacks on mobile devices are limited today, the growing usage will make them a high-value target moving forward. And cybercriminals are ready. Today's existing malnet infrastructures will be the same ones used to deliver tomorrow's attacks on mobile devices.

Malnet infrastructures enable cybercriminals to launch dynamic attacks that are often not detected by traditional anti-virus vendors for days or months. In one case in early February 2011, a malware payload changed locations more than 1,500 times in a single day. These types of attacks are far too dynamic even for defenses that inspect content in real time to keep pace. The rise of malnets demands a new type of security to protect against corporate data loss, financial or identity theft, and other costly consequences. Businesses need a proactive defense that can stop attacks before they launch by identifying and blocking the source. The key to this type of defense is to understand malnets, their structure, their targets and their strategy.

Malware Networks

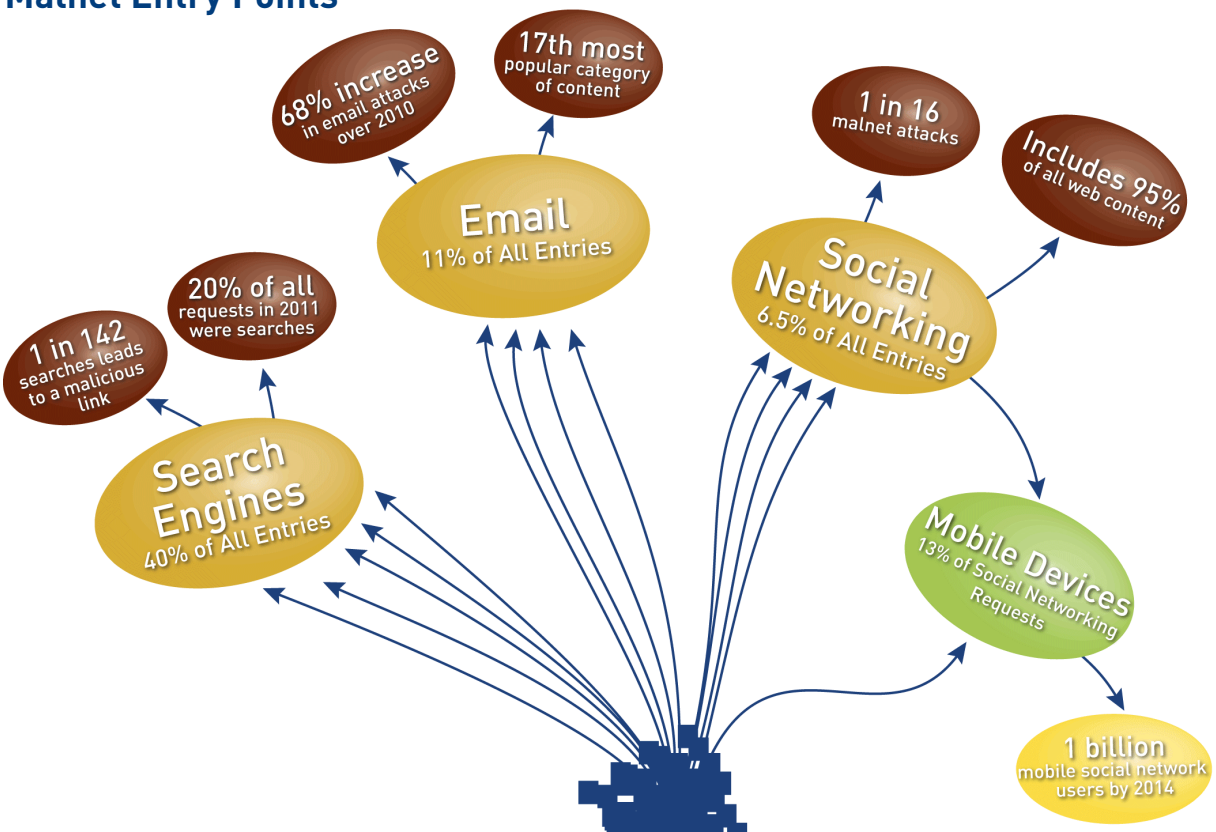
What You Need to Know to Protect Your Organization

A malware network (malnet) gathers users, typically when they are visiting trusted sites, and routes them to malware, via relay, exploit and payload servers that continually shift to new domains and locations.

5000 Threats
Confront the average business every month

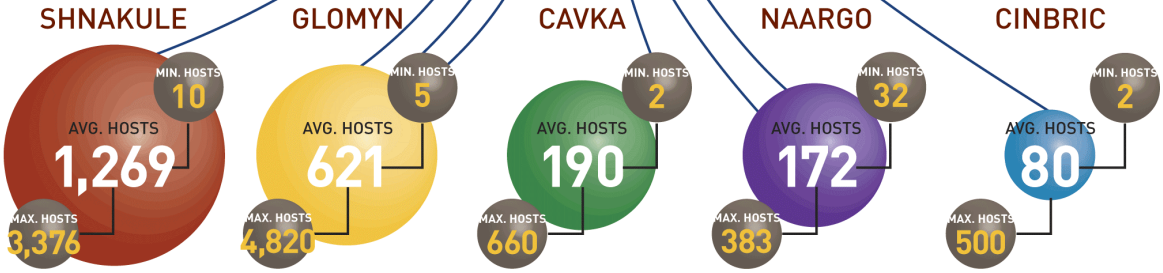
240%
Increase in malicious sites over 2010

Malnet Entry Points

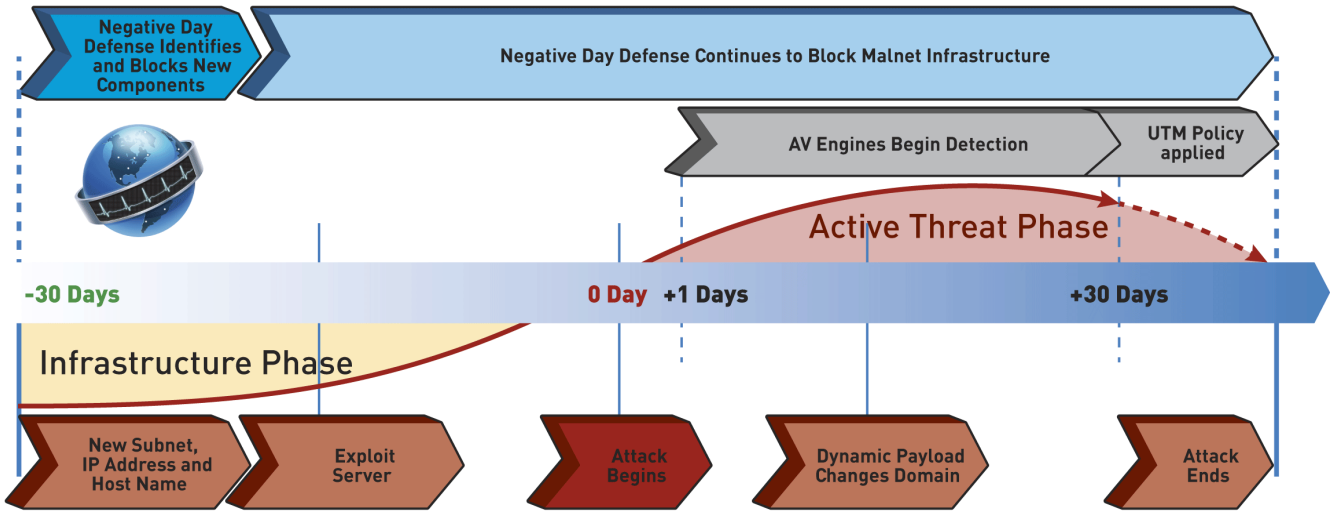


Top 5 Malware Networks

Blue Coat Labs is tracking over 500 malnets like these



A New Malnet Defense



Key Takeaways for Your Organization

- **Real-time analysis** of search results is required to identify malicious links
- **Granular application and operation controls** are essential to effectively manage and mitigate risks of social networking
- **Layered defenses** are critical to protect against malicious executables within webmail, which remains a valuable threat vector despite a decline in popularity of email
- **Negative day defenses** are required to stop future attacks by blocking them at their source

The insights reviewed in this report are derived from Blue Coat Security Labs' analysis of data from the WebPulse collaborative defense. Blue Coat WebPulse™ is a cloud-based, real-time analysis and ratings service that unites users in a common defense. Delivered via Blue Coat ProxySG appliances and the Blue Coat Cloud Service, WebPulse receives one billion web requests from 75 million globally diverse users. With comprehensive visibility into the web ecosystem, WebPulse can automatically identify abnormal traffic and correlate it to known malware networks (malnets) to block attacks before they are launched. Utilizing these techniques and other advanced analysis tools, WebPulse blocks 3.3 million threats per day.

Malnet Strategy: Build Once, Use Often

Malnets are distributed infrastructures within the Internet that are built, managed and maintained by cybercriminals for the purpose of launching a variety of attacks against unsuspecting users over extended periods of time.

They gather users, typically when they are visiting trusted sites, and route them to malware, via relay, exploit and payload servers that continually shift to new domains and locations.

Sequence of a Malnet Attack

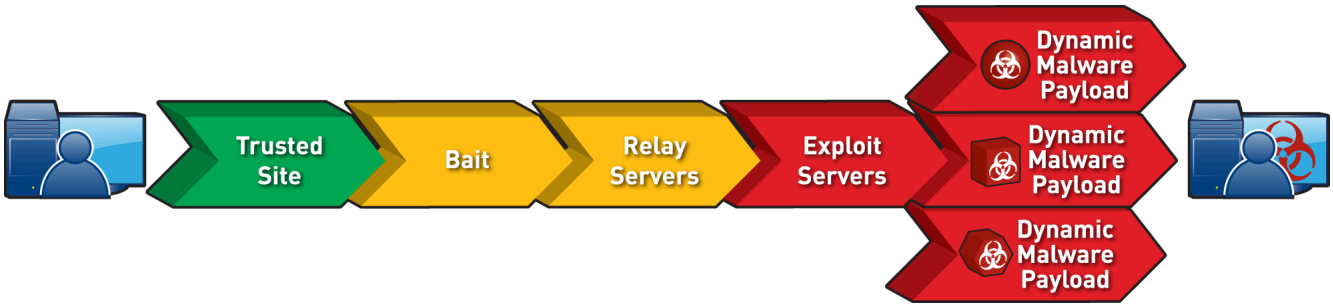


Diagram 1 - Caught Within a Malnet

Like any business, malnets leverage the pervasiveness of the Internet and the connectedness of the world to drive users to their sites through various means. Malnets are designed and operated to preserve anonymity by means of a constantly shifting landscape of links, servers and malware payloads. The goal of most malnets is to induce users to share personal or financial information or even money.

A malnet is comprised of several thousand unique domains, servers and websites that work together to funnel users to the malware payload. Diagram 1 is a linear representation of a typical attack launched by a malnet. Essentially, this is the path that a user would follow from point of entry to the dynamic payload.

A malnet uses this existing infrastructure of relay and exploit servers to quickly launch new attacks that deliver dynamic malware payloads. With an infrastructure in place, attacks can be tailored to exploit trending news- or celebrity-related lures that quickly attract potential victims before security technologies identify and block it.

Each attack will use different trusted sites and bait to lure users. Some attacks forego relay servers; instead, they send users that have taken the bait directly to exploit servers that can identify system or application vulnerabilities. Once a vulnerability has been identified, a malware payload will be served.

In some cases, as with iFrame injections, users will travel the malnet path unknowingly. The relay and exploit server action takes place in the background and secretly installs malware. In other cases, downloading malware requires the user to click on a link.

In 2011, fake anti-virus software and fake video codecs continued to be the most popular vehicles for distributing malware. The fake anti-virus attack typically utilizes a simulated hard drive scan that uncovers malware on a user's computer and offers to clean it with anti-virus software. The fake video codec is popular for social networking-related attacks in which users are asked to click a link to watch a video or see a picture. They are then told that to do so, they need to download a new codec by clicking on a link.

Negative Day Defense: Agnostic to Attack Type

In 2012, Blue Coat Security Labs expects that nearly two-thirds of all new attacks will come from known malnets. The best protection against these attacks is a negative day defense that can proactively block them before they launch.

The entrenched nature of these malnets and, in some cases, their geographic diversity, makes it nearly impossible to shut them down. As long as the infrastructure is in place, cybercriminals will continue to launch dynamic attacks that change far too quickly for traditional security defenses to keep pace.

However, it is the very existence of a sustained infrastructure that creates a new opportunity to stay ahead of cybercriminals. This negative day defense is a significant step forward in an industry that has always been forced to wait until an attack is launched to study and develop a defense against it.

At the heart of this negative day defense is a clear understanding of malnets. Blue Coat Security Labs maps the relationships between malnet components to identify and block new subnets, IP addresses and host names when they come online. Once the malnet infrastructure has been identified, it can be blocked at the source before attacks are launched.

The negative day defense is a unique and robust security strategy because it no longer matters whether the payload is a key logger, a worm, a Trojan or some other malware. The traditional tricks that cybercriminals use to obfuscate their attacks no longer matter. The attack type and content don't matter. Zero-day exploits can't impact the network. Payload encryption is pointless.

Diagram 2 shows the negative day defense in action. This attack, named the Urchin, was launched in October of 2011. The Blue Coat WebPulse collaborative defense identified and blocked components of the attack as early as June (Notes on the Urchin Site-injection Attack).

The Urchin Attack

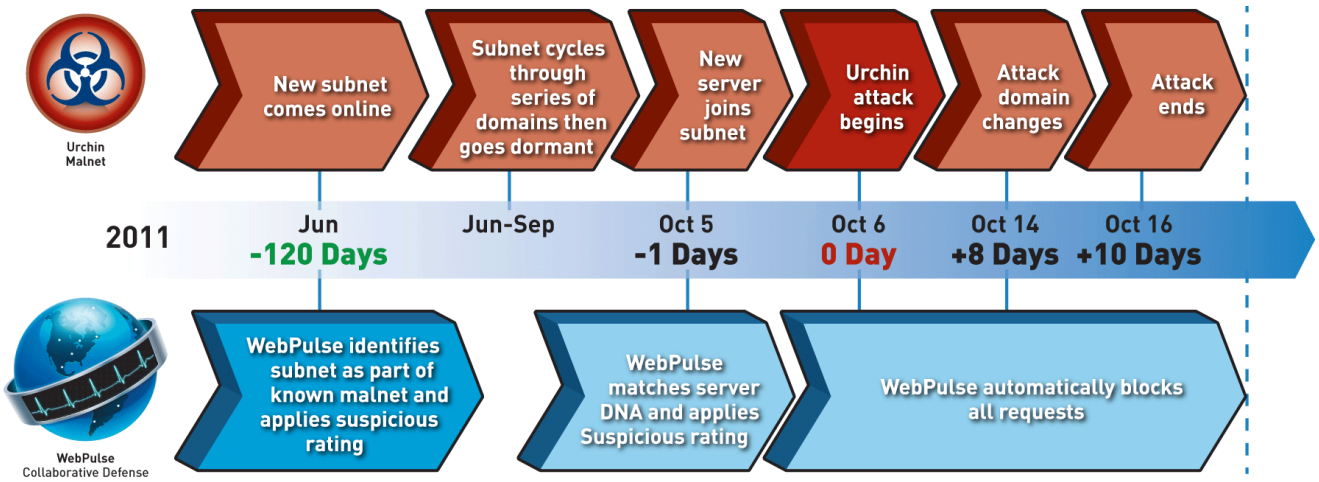


Diagram 2 - WebPulse Collaborative Defense Delivers Negative Day Protection

WebPulse began protecting users more than 4 months before the attack was launched

Know Your Enemy: The Five Largest Malnets

Blue Coat Security Labs is currently tracking more than 500 unique malnets and subnets. As malnets expand into new types of malicious activities and prepare new attacks, new subnets or domains come online and exploit servers are added. Not all 500 malnets will be active on any given day, and the actual size of the network may vary from day to day.

Top 5 Malnets

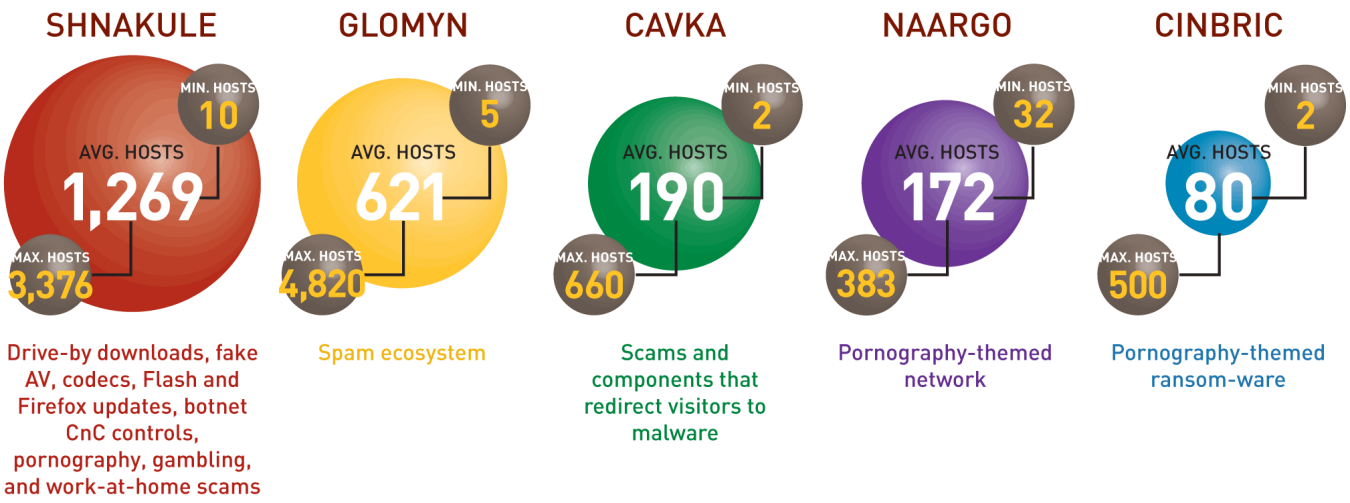


Diagram 3

Source: Blue Coat Security Labs

In Diagram 3, Blue Coat Security Labs ranks the five largest current malnets by size and describes the primary malicious activities of each.

Cinbric and Naargo consistently appeared on the list of the five largest malware networks in 2011. Both are smaller on average than malnets like Glomyn or Shnakule. However, they both have shown significant spikes over the last several months where the infrastructure grew to launch new attacks. In the case of Cinbric, the maximum size was more than six times as large as its average size, demonstrating the ease with which new components can be added to an existing malnet infrastructure.

Glomyn is a spam ecosystem and has been in continuous operation for 10 straight months. At times over the last several months of the year it was the largest malnet on the Internet. However, in early October, daily activity plummeted from as many as 4,800 host names to less than 100. This drop off suggests a transition to a new infrastructure.

Cavka launched in September and is largely focused on scams. Like Glomyn, it was very active shortly after it launched, reaching a peak of 660 host names in a single day. In November, activity dropped off significantly.

In 2011, the Shnakule malnet largely dominated malicious activity on the Internet. In fact, it is so large that during the course of the year it absorbed several smaller malnets. In late April, Blue Coat Security Labs began tracking the Ishabor malnet, which focused on the distribution of fake anti-virus scareware. Shortly thereafter, Security Labs experts determined that this new network was actually part of the larger Shnakule malnet. The cadence of Ishabor's activities and eventual absorption into Shnakule imply that the malnet was a new infrastructure created and tested by Shnakule's operators prior to being integrated into the parent network.

Not only is Shnakule the largest malnet, but it is also launching some of the most aggressive attacks and branching out into new attack vectors. In July, Shnakule expanded its traditional activities to include malvertising. In September, it launched an attack seeking to obtain the credentials of high-value users.

The Long Reach of Shnakule Malnet

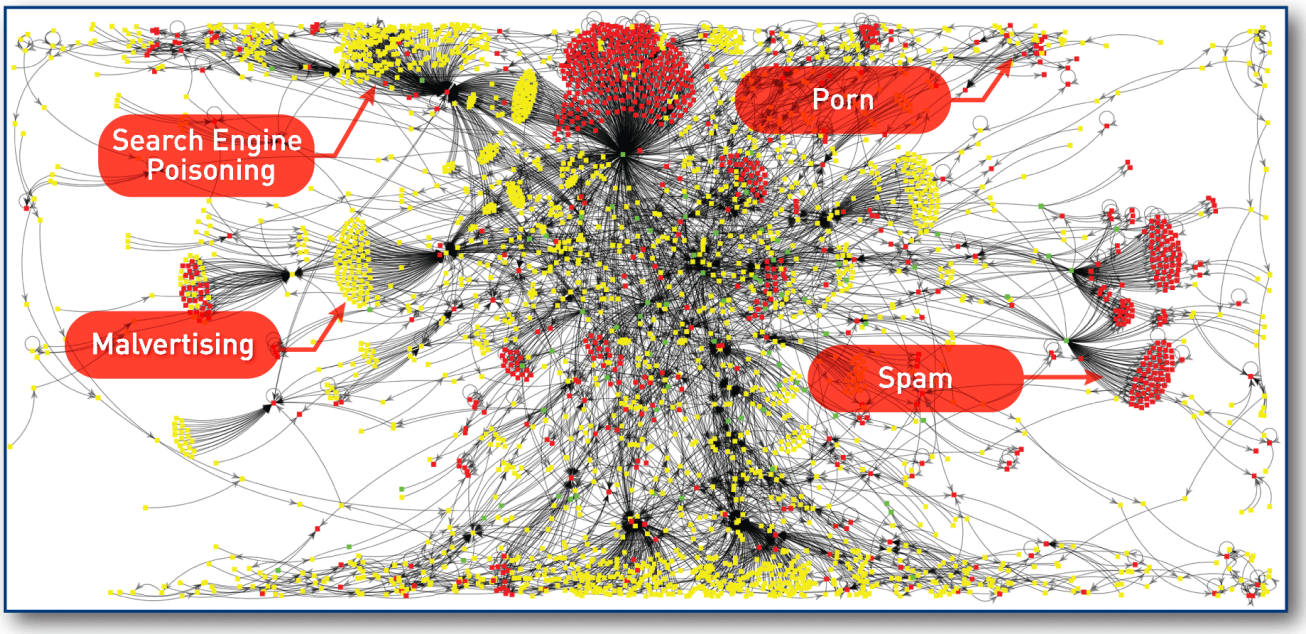


Diagram 4
Source: Blue Coat Security Labs

Diagram 4 maps out the network of components that comprise the Shnakule malnet. Identifying and mapping the components of an individual malnet, allows Blue Coat Security Labs to identify the types of attacks it is engaged in. In the diagram above, spam, porn, search engine poisoning and malvertising attacks are all represented.

It's important to note that the unique components of a malnet are not always malicious. In the graphic, the green dots represent legitimate sites. The red sites represent the malicious components of the malnet, such as the exploit servers or malware payloads. The yellow points represent sites that cannot easily be classified as good or bad, as in the case of a relay server that is not technically malicious or a hacked legitimate site that is unknowingly acting as a component in the attack chain.

Like legitimate businesses, malnets can exist on a multinational scale. The very nature of malnets is flexibility, which allows operators to move from one country to another or from one country to many. Diagram 5 shows the locations in which each of the five largest malnets had a point of presence at the end of 2011.

Shnakule is the most geographically dispersed of the five largest malnets with a presence in countries throughout Europe, the Middle East, Asia and the Americas. It is most concentrated in the United States and Germany. Naargo is based in Israel, the Netherlands and Russia.

Global Reach of Malnets

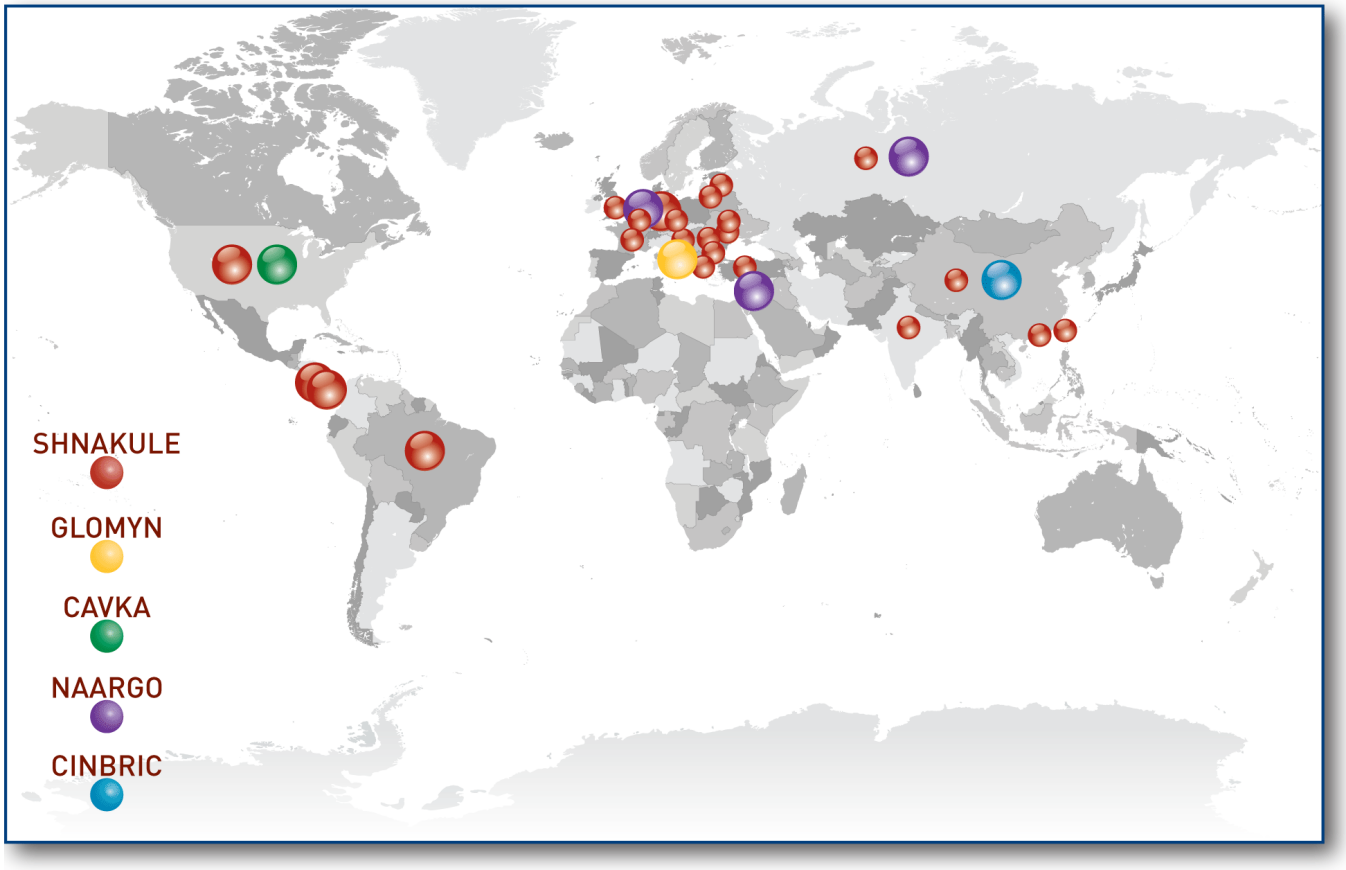


Diagram 5
Source: Blue Coat Security Labs

The geographic distribution of these malnets indicates collaboration across cybercrime organizations and demonstrates an expanded reach in which attacks can quickly be launched across a broad range of countries. Additionally, this distributed nature makes it more difficult for any one country to shut down the infrastructure.

Glomyn, Cavka and Cinbric are single-country malnets based in Italy, the United States and China, respectively. This nationalized model indicates that the operators are highly localized and profit from activities focused exclusively on their country of residence.

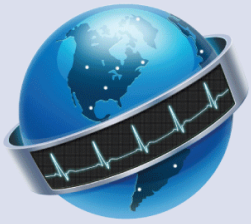
Finding the Internet Watering Holes

The success of malware attacks depends on finding many users in one place. A look at the most requested categories of content shows the changes in collective Internet behavior over time and suggests how that might be exploited by cybercriminals.

In 2011, Search Engines/Portals was once again the most requested category of content. In fact, requests for this category grew by more than two percentage points, demonstrating that users still access information on the Internet primarily through search engines.

Social Networking rose from the fourth most popular category of content in 2010, to third in 2011, representing roughly 10.5% of all requests. The rise of social networking as a requested category of content confirms its increasing acceptance in business environments. Some businesses are actively embracing the benefits of social media for extending their brands, recruiting employees or creating partner or customer environments. In other cases, businesses are allowing the use of social networks because they now have more tools to mitigate the risk of data loss or ensure employee productivity.

Top 5 Most Requested Categories of Web Content



WebPulse
Collaborative Defense

2011		2010	
Search Engines/Portals	20.8%	Search Engines/Portals	18.1%
Computers/Internet	11.8%	Web Advertisements	10.5%
Social Networking	10.5%	Computers/Internet	9.4%
Web Advertisements	7.9%	Social Networking	9.1%
Content Servers	7.8%	Content Servers	6.2%

Source: Blue Coat Security Labs

Social Networks: An Internet within the Internet

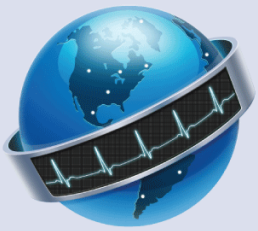
It's a worthwhile exercise to take a deeper look at Social Networking as a growing category of content. This is truly a different beast among web content types. In 2011, businesses continued to turn to social networks. This transition from a business inconvenience to a business imperative requires organizations to provide access to their users while safeguarding their assets.

The move to social networking is really the extension of a trend that first began on the consumer side. Since 2009, social networking has increasingly eclipsed web-based email as a method of communication. For the last two years, Email was the 17th most requested category of content, representing nearly 1.5 percent of all requests in 2010 and just over 1 percent in 2011. In 2009, Email was the ninth most requested category of content.

Now, social networking is moving into a new phase in which an individual site is a self-contained web environment for many users – effectively an Internet within an Internet.

As they develop into self-contained web environments, these sites include a variety of content that should not simply be categorized as Social Networking. By looking at the types of content within social networking sites we can discern different user behaviors. In 2011, the Blue Coat WebPulse collaborative defense categorized content on social networking sites into 80 further subcategories. The result is that 95% of all content types on the Internet are also found within social networking sites. The following table examines the most requested subcategories for the year.

Top 5 Most Requested Content Within Social Networking

	Most Requested Subcategories 2011		Most Requested Subcategories 2010	
 WebPulse Collaborative Defense	Games	37.94%	Education	18.21%
	Society/Daily Living	23.81%	Adult/Mature Content	9.89%
	Personal Pages/Blogs	6.38%	Travel	9.78%
	Pornography	4.94%	Online Games	8.11%
	Entertainment	4.23%	Entertainment	7.25%

Source: Blue Coat Security Labs

Two things stand out in this data. First, user behavior within social networks is very different from behavior on the Internet. None of the five most requested categories within social networks match the most requested categories for the Internet as a whole.

In fact, social networking activity is dominated by Games and Society/Daily Living. These two categories were responsible for more than 60 percent of all requests, a significant growth over 2010, where they represented just over 14 percent. Looking at it from another perspective, almost one in every four new Social Networking requests fell into the Society/Daily Living category compared to one in every 16 in 2010.

Among the other top five categories are Personal Pages/Blogs, Pornography and Entertainment. The sheer diversity of this content makes it utterly impossible to simply categorize it all as Social Networking. Within the top five categories alone there is a mix of content that might be acceptable within a workplace, content that would invite the scrutiny of Human Resources and content that could consume large amounts of bandwidth and employee productivity.

It's essential to understand that social networks are portals that effectively host a variety of content. Bringing some granularity of visibility to social networking is important for businesses that are trying to put policies in place to protect against the risk of data loss, lower employee productivity and web-based threats.

Business Impact: Businesses can no longer simply block social networking, but require more granularity and control to mitigate the risks associated with it. To fully leverage the benefit of web applications and content, businesses must have detailed analysis and control, not just of social networking sites, but also of the individual web applications and content within those sites. Additionally, they need to be able to filter out any malicious links from within the allowable content.

Luring Users: Follow the Path of Least Resistance

Most malnets are driven by financial profit, which is ultimately determined by the success of the attacks they launch. To increase the success of any one attack, cybercriminals tend to target vectors that are easily exploitable or are utilized by large, diverse populations of users.

Most Common Malnet Entry Points

2011	
Search Engines/Portals	40.17%
Email	11.62%
Unrated	8.64%
Social Networking	6.48%
Pornography	4.4%

Diagram 6 - Following the Path of Least Resistance
Malnets exploit search engine, email, social networks to lure users
Source: Blue Coat Security Labs

By looking at the entry points into malnets, we can begin to understand how cybercriminals target users as well as behaviors and activities that may expose users to greater risk.

Diagram 6 shows the leading entry points into malnets for 2011.

It's clear from this data that cybercriminals are increasingly using the path of least resistance to create entry points into malnets. The two most popular entry points are Search Engines/Portals and Email. To exploit them, cybercriminals need only use these entry points as they are intended to be used by anyone.

For example, email simply requires cybercriminals to send an email with a malicious link. In fact, the barrier to entry for email use is so low that cybercriminals are increasingly returning to it. So, while it ranked 17th among most requested content for all of 2011, Email jumped nearly five percentage points as an entry point in the last six months of the year.

What is known as search engine optimization by businesses is called search engine poisoning when used the same way by cybercriminals. To exploit search engines, cybercriminals need only provide relevant content to ensure that their sites rank high in the search results page. They can exploit the very algorithms that search engines rely on to deliver meaningful results to ensure that their malicious results are delivered as well.

Over 2011, Blue Coat Security Labs saw Social Networking rise from the fifth most popular point of entry into malnets to the fourth. This shift parallels the rise of Social Networking as a requested category of content. These sites continue to expand their consumer user bases, and with businesses now investing in social networking, the prospect of greater financial return from attacks is much higher.

Malnet operators follow a low investment/high impact strategy. Targeting search engines and social networking offers them the greatest number of potential victims; search engines and email provide easily exploitable attack vectors.

While Social Networking rose as an entry point, pornography fell more than two percentage points and now represents only 4.4 percent of all entries into malnets. Pornography has traditionally been popular for malware, but its popularity in terms of requested content is declining. In 2011, it ranked 20th among the most requested content versus 5th in 2009. Web usage is evolving as more users access a varied range of content. This shift diminishes the value of pornography as a malware entry point.

Malnet Bait: Catching a Wave

With a proven infrastructure armed and ready to launch an attack, malnet operators exercise patience, waiting for an event they can exploit to drive unsuspecting users to malware. These events include things like scheduled regional or global activities such as sporting tournaments, elections and holidays, breaking news, or celebrity-related gossip, any of which can stimulate users to view videos or pictures or click on links. By maintaining a malnet infrastructure beyond any one attack, cybercriminals can easily launch new, topical attacks that can lure curious web users to malware.

Interestingly, attacks that use search engines as the primary entry point typically do no target these big news events. Rather, they target a variety of search terms to cast a wide net. Potential victims searching for news about a big event are often shielded from malicious results by the sheer volume of legitimate sites with actual content.

However, these newsworthy events may be used to drive attacks through email or social networking. In these environments, the news-related content actually helps the attack stand out in an inbox full of emails or a wall of posts.

In 2011, the following stories served as topical bait for attacks:

13 March	8.9 earthquake and tsunami in Japan
29 April	Royal wedding of Prince William and Catherine Middleton
2 May	Death of Osama bin Laden
23 July	Death of Amy Winehouse
5 October	Death of Steve Jobs

The tried-and-true tactic of targeting death, disaster and drama will continue to serve as potential bait for attacks in 2012. In addition to unexpected natural disasters, world leadership changes and celebrity-driven gossip, the following activities are likely to be exploited:

Elections	Presidential elections in Bolivia, France, Greece, India, Mexico, the United States and Venezuela
Sporting Events	Wimbledon, the French Open, the NCAA Tournament, and regional sporting events such as Copa Libertadores
Technology Releases	iPad3, iPhone5, Windows 8 and the Wii U
2-5 June	Diamond Jubilee of Queen Elizabeth II
27 July-12 August	Summer Olympics in London
17 December	First anniversary of the death of Kim Jong-il
21 December	End of the 5,125-year cycle in the Mayan calendar

Malware Payloads: Hiding in Plain "Site"

The final component of malnet infrastructure is the payload. Malnet operators prefer to host malware and other malnet components on hacked sites to make detection more difficult.

The table below shows the top categories in which malicious content was located.

As we saw with the entry points into malnets, cybercriminals are again following the path of least resistance. In the case of Online Storage and Software Downloads, these sites typically host files as part of their business model, so a malware payload would simply represent another file. In the case of Software Downloads, there is an added advantage in that users are actively looking to install software.

Most Dangerous Categories of Content

Category	Percent of malicious ratings in 2011
Online Storage	74%
Open/Mixed Content	39%
Dynamic DNS Host	15%
Software Downloads	10%
Content Servers	5%
Web Hosting	5%
Gambling	3%
Web Advertisements	3%
Hacking	3%
Search Engines/Portals	3%

For four of the five most dangerous places on the Internet (Online Storage, Open/Mixed Content, Software Downloads and Content Servers), businesses typically don't apply security policies based on the perceived 'safe' or generic nature of the content. This creates an easy entry path for malware targeting these categories.

Ease of use is part of the reason Online Storage has been the leading category for hosting malware for the last three years. In 2011, 74 percent of all new ratings were determined to be malicious. Although this is down from 90 percent in 2010, it is still a top category for malicious content.

The second largest host of malicious content, Open/Mixed Content, is the most dangerous because of its popularity as the seventh most requested category of content. It's both a popular location for malware and a widely visited category, which helps enable a high success rate for malware. This should encourage businesses to set policies around executable files for this category to protect users from the elevated risk it poses.

Dynamic DNS Hosts, the third most dangerous category, have been used as 'phone home' data exfiltration sites in many high-profile targeted attacks. If businesses are not blocking this category of content, they should review their logs regularly to determine if there are above-average levels of traffic to these sites. This would indicate potential botnet and advanced persistent threat infections.

Content Servers are in fifth place, both as a requested category of content and as a dangerous category of content. It has become popular to host content closer to users with the goal of improving the user experience, and many legitimate sites are now utilizing content servers. This category represents reputable, well-known companies that host content such as images and videos. Though the expectation is that they will self-police for obvious malware, Blue Coat Security Labs has seen cases of malware distribution from these sites.

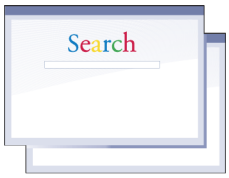
In the last half of 2011, Blue Coat Security Labs saw a significant increase in malvertising, where major ad networks were duped into serving malicious ads from affiliate networks. In 2011, malicious content within Web Advertisements increased 50 percent over 2010. While Web Advertisements ranks ninth on the list of most dangerous web content, it is the fourth most requested category of content and is served on nearly every site. About half the malvertising attacks utilize a fake AV scanner page; the other half use silent drive-by downloads with a variety of exploits.

While Search Engines/Portals and Social Networking ranked high in terms of most requested content, the actual malware payloads aren't often hosted in these categories. Rather, these sites serve as a conduit into malnets via trust-based lures. Search Engines/Portals ranks 11th on the list of most dangerous content where roughly 3 percent of all new ratings are determined to be malicious. Similarly, Social Networking was third on the list of most requested content but doesn't even rank in the top 15 most dangerous categories.

Confirming earlier findings about the demise of Pornography as a tool for cybercriminals, it is now 33rd on the list of most dangerous content.

Business Impact: Block all content from dangerous categories such as Pornography, Gambling and Spam. Block executable content from unrated domains and categories that typically host malware, such as Dynamic DNS Hosts, Software Downloads, Online Storage and Open/Mixed Content. Refer to the appendix for more detailed recommendations.

Top Attack Vectors: Malnet Tactics



Search Engine Poisoning - Polluting the Well

In 2011, search engine poisoning asserted its dominance as the leading attack vector for web-based threats. With Search Engines/Portals representing the most requested category of content, it is not surprising that this category is also the leading entry point into malnets.

With a well-built infrastructure in place, malnet operators conduct search engine poisoning attacks on a 24/7 basis. Millions of people search for data every day. To be successful, an attack needs to divert only a small percentage of that traffic.

In search engine poisoning attacks, malnet operators make constant adjustments to the bait content they feed to search engines but don't necessarily focus on big news events. Rather, they target every sort of search imaginable to cast (and maintain) the widest possible net. Potential victims searching for news about the current big event are often shielded from search engine poisoning links by the sheer volume of legitimate sites with actual content.

Cyber Monday, the largest online retail shopping day in the United States, provides a recent example of how cybercriminals utilize search engine poisoning. During that one day, users searching for terms such as "cyber monday," "cyber monday deals" and "best cyber monday deals 2011" were being funneled into malnets (Search Engine Clutter).

As we saw earlier in the report, the use of Search Engines/Portals is growing year over year. This dominant use, coupled with the inherent trust users place in search engine results, makes this a significant ongoing risk for businesses.

Business Impact: Training users to conduct 'Who Is' searches and to look for suspicious URLs can help determine whether a website has been recently registered. But while user education can help mitigate the impact of search engine poisoning as an attack vector, it is not a scalable solution. Businesses need to supplement education with a web security solution that can analyze links in real time to determine whether they're funneling users into a malnet.

Social Networking - A Parallel Universe

As we noted earlier, social networking is one of the most requested categories of content on the Internet, and, not surprisingly, one of the leading entry points into malnets. Users implicitly trust social networking sites where they build their circles of friends. That makes the pages, postings and links on social networks ideal places to plant bait.

Whereas search engine poisoning does not typically rely on news-driven events to attract users, social networking does. Fake foto attacks on Facebook typify attacks that leverage people's interest in the latest social news (Another Facebook Fake Foto Attack, on Hacked Russian Site). Attacks like these are prolific on social networking sites. They exploit not only interest in the latest news topics but also the voyeurism that is endemic to the Internet. Invitations to view someone behaving badly have a high success rate because they tap into a common behavior very effectively.

Additionally, the growing use of social networks for all things Internet has resulted in a blend of virtual and real economy (purchasing virtual cash or goods with real funds) that provides cybercriminals with a high return on stolen credentials. This is particularly true for games.

While many enterprises discourage the use of social networking games in the work place for productivity reasons, it's a good practice to educate users on the potential risks as well. It won't be long before cybercriminals introduce malicious games or

compromise existing popular games to attack a social networking account and create a conduit into the enterprise network. Educating users is a pre-emptive step towards protecting the organization.

Business Impact: IT organizations should have the ability to filter social networking content as well as to enforce granular acceptable use policies around social networking operations. By using these types of controls, businesses can allow their employees to access social networking while mitigating its potential risks.

Malvertising - One Stop Shopping for Cybercrime

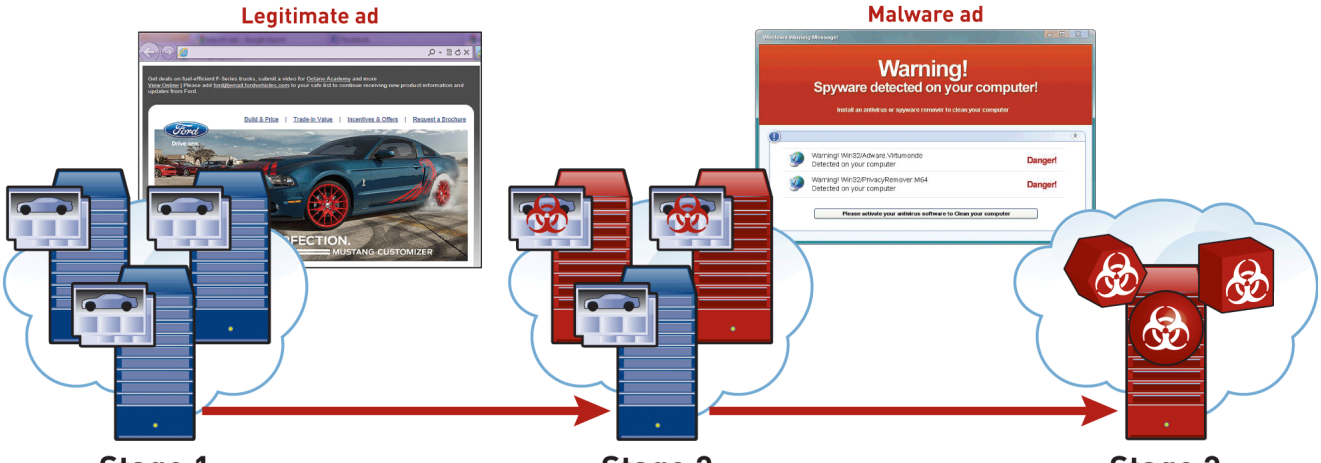
Web Advertisements is becoming a key vector for cybercriminals. As we saw earlier, Web Advertisements represent 8 percent of requests. Of all new Web Advertisement ratings, 3 percent were malicious. When we look at the high volume and pervasiveness of web advertisements, we can see that malvertising is quickly becoming one of the more insidious attack vectors.

Malvertising exploits the hierarchical nature of web advertisement models to insert malicious ads into legitimate ad networks. Before they attack, malnets will operate legitimately for several months to gain the trust of the large ad delivery networks. iFrame injections into the malicious ads trigger drive-by downloads that install malicious software on a users' computers without their knowledge.

An attack from June 2011 (Busting a Big Malvertising / Fake-AV Attack), illustrates the common tactics malnet operators use in malvertising attacks. In the first stage of the attack, new ad servers were set up with different registrars as independent entities. For more than a month, they served legitimate ads to gain a good reputation.

On the day of the attack, the same ad servers began serving malicious ads that relayed users to the malware payload, which changed frequently in an attempt to avoid detection from anti-virus software. As an example of the level of sophistication in play with this particular attack, none of the rogue ad servers appears by name in the pages that host its ads, indicating that the victimized legitimate sites were not directly using these ad servers but were being served the malicious ads through an ad network.

Three Stages of Malvertising



During this attack, which continued to operate for several weeks, the Blue Coat WebPulse collaborative defense blocked requests for the malware payload from more than 15,000 users. On the initial day of the attack, only two of 43 anti-virus engines identified the payload as malicious or suspicious.

This demonstrates that web-based malware is changing far too quickly for traditional single-layer defenses to keep pace. The most successful defense against this kind of attack is a solution like WebPulse, which can identify correlations between known malicious networks and new servers in real time and block user requests to those sites.

Business Impact: A single anti-virus solution at the desktop will leave the organization extremely vulnerable to new types of malware. Layer anti-virus solutions at the desktop and the gateway to provide more thorough protection against malicious executable files. Utilizing different anti-virus vendors at each location will increase the likelihood that an attack missed by one will be blocked by another.

Spam - A Resurgent Attack Vector

In 2011, Blue Coat Security Labs saw a resurgence of spam as an attack vector. Spam utilizes email as a delivery mechanism, and this resurgence correlates with the rise of Email as an entry point into malnets.

The Glomyn malnet, which often rivaled Shnakule as the largest malnet on the Internet, focused exclusively on spam. This large infrastructure peaked at 4,800 host names after it initially launched.

The classic spam attack utilizes an email that directs the recipient to click on a link to update an account, receive a message or verify information. For example, depending on the set-up, there may be an attachment that is intended to appear as an invoice.

In October, Blue Coat Security Labs tracked an attack that utilized the U.S. Postal Service as bait (A Package-scam Malware Attack). Emails referenced a USPS delivery and included links that appeared to offer delivery confirmation and an invoice:

www.usps.com.ww051.com/shipping/trackandconfirm.php?navigation=usps&respLang=Eng&resp=10242011

www.usps.com.ww051.com/shipping/invoice.php

Note that the URLs are constructed a bit like classic phishing URLs. The subdomain and path strings look legitimate at a casual glance. While the majority of users are more educated than ever about the dangers of clicking on unknown links, it is still quite common. In this attack, more than 100 users clicked on the link and attempted to download the malware.

The EXE payload for this attack was well-cloaked and detected as malicious by only four of 43 anti-virus engines.

Business Impact: Businesses should always utilize additional layers of defense in conjunction with an anti-virus engine. In contrast to the low detection rate by anti-virus engines, the Blue Coat WebPulse collaborative defense dynamically flagged and blocked all the EXEs as Suspicious. WebPulse looks at a variety of different characteristics to determine whether something is malicious. It offers an additional layer of protection, catching threats that slip by anti-virus engines.

Botnets: The Danger within Your Network

The most active botnets in 2011 have all been in existence for more than a year. While some have been taken down over the last two years, the infected systems still exist and attempt to communicate with command and control servers. In many cases, end users appear to be infected with multiple botnet-producing Trojans, with each exploit making various phone home requests with respect to their own functionality. This symbiotic sharing of botnet space enables easier monetization of malware.

The WebPulse collaborative defense identifies and blocks communications between infected end user systems and command and control servers. This allows Blue Coat Security Labs to track a botnet's success in infecting computers rather than its size.

In 2011, Zeus was far and away the largest botnet. Zeus and SpyEye are virtually the same banking Trojan, in which the same traffic is generated, the same components are used in updates, the same command and control communication is in place, and, in some cases the same domains are used. The size of this botnet has created a cottage industry of sorts with exploits created solely for the purpose of delivering the Zeus/SpyEye payload. Murofet, which was first reported in 2010, is an example of this type of exploit.

An http p2p botnet was the second most active in 2011. This botnet operates by creating a network of http p2p communications that is used to deliver payloads. The most famous example of this type of botnet was Waledac. Though the Waledac botnet was taken down by Microsoft in March 2010, Blue Coat Security Labs continues to see traffic from infected systems.

The TDSS botnet was the third most active. Discovered in 2008, it was distinguished by its rootkit capabilities, which install malware before Windows OS starts. By installing itself deep in the system, this malware makes itself difficult to detect and remove. An example of one of the installed components is a file that allows malnet operators to anonymously web surf on infected computers – a service for which cybercriminals can charge a monthly fee on the black market.

It is clear from the data that though botnets may be taken down, infected computers remain. Conficker provides a prime example. Two years after the initial attack in April 2009, there is evidence that it continues to generate thousands of site names every day, waiting for its controller to register one of the domains and tell the infected machine what to do.

Business Impact: Businesses should deploy real-time reporting to ensure the IT organization has visibility into any botnet activity on the network. Understanding normal traffic patterns will enable the ability to identify anything out of the ordinary and isolate infected systems as soon as they're detected.

Advanced Persistent Threats: Danger Knocking at the Door

Following high profile attacks like Aurora that utilized advanced persistent threats (APTs), business awareness of their threat and potential danger drove changes in user behavior and security policies.

In contrast to mass market malware, APTs are highly targeted attacks looking to steal specific high value assets. While APTs have historically targeted government agencies, contractors and suppliers, they have rapidly entered the private sector as demonstrated by the attack on RSA that targeted the company's SecureID authentication products.

The distinguishing characteristic of APTs is motivation. Conventional attacks will utilize fake AV attacks to install exploit kits that can mine bank accounts or other personal information. APTs, on the other hand, typically tailor their approach for each target, using spear-phishing and social engineering to acquire the credentials of key corporate employees (Notes from RSA: Advanced Persistent Threats). These are well researched, well funded and often exploit unknown vulnerabilities.

APTs can lurk within a network. Eventually, though, they will need to communicate with command and control servers. Monitoring for any communication is a crucial defense against these threats.

Business Impact: In addition to other APT security measures, it is imperative that IT organizations understand their various network and web traffic logs, so they can identify anomalous behavior. At Blue Coat, that means using Reporter to monitor traffic in categories such as Dynamic DNS Hosts, which correlate highly to APT infections. It also means understanding Reporter well enough to create customized reports that can act as APT detection tools.

The Mobile Dilemma: New Threat Frontier

Mobile device adoption has been accelerating for the last few years, and that growth has now turned into an explosion. Companies are adopting "bring your own device" (BYOD) initiatives as a way to reduce costs and enable employees to select devices that work best for their needs. At the same time, they're rolling out their own mobility initiatives, distributing iPads to sales reps for product demonstrations, to pilots for flight safety checks and to doctors for accessing and updating health charts.

However, the introduction of new initiatives presents new risks. There are three primary security concerns related to mobile devices. First, is data loss in the form of contacts, emails or other sensitive corporate information that can be easily stored and shared from mobile devices. Second, is a new entry vector for malware through web-enabled mobile applications and more traditional vectors such as social networking. Third, is the increasing use of mobile devices for online banking and other financial transactions that makes users high-value targets for cybercriminals.

Businesses are now faced with finding a way to extend security to networks and devices over which they have little or no control. Employees, however, are reluctant to cede control of their personal devices to IT. As corporate and personal lines continue to blur, this contention between users and their IT organizations creates an opportunity for malware to enter.

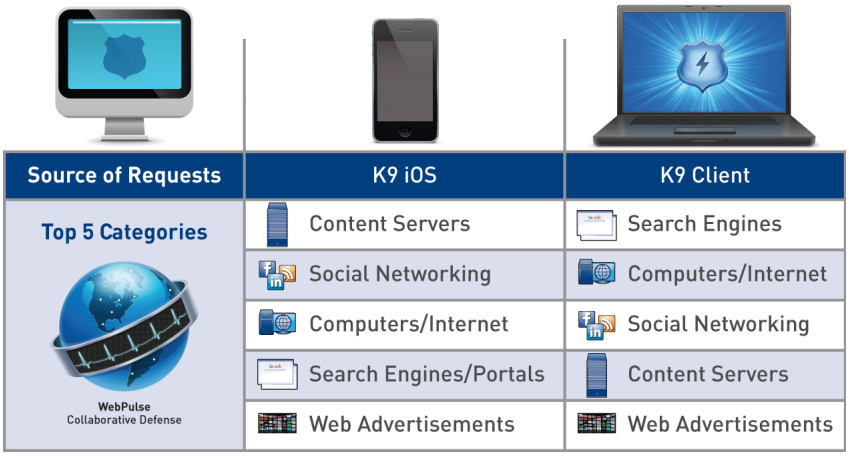
Mobile security is in its early stages and is broadly defined to include everything from remote lock and wipe to threat protection for mobile devices. Today, according to Nemertes Research, the top mobile security measures deployed by companies are wipe and lock functionality (77.4% of companies surveyed) and encryption (63% of companies).

These features, which are traditionally part of a mobile device management solution, are directed at device and data loss. They typically lack web security functionality for protecting devices and users from rogue web-enabled applications or mass market malware that targets mobile device platforms.

Mobile Behavior

It's useful to examine how people utilize the Internet from mobile devices to understand where they might be the most vulnerable. Blue Coat Security Labs compared web requests from the Blue Coat K9 iOS application with web requests from K9 desktop users to identify differences in behavior.

Most Requested Categories of Web Content for K9 Mobile and Home Users



Mobile User Behavior Drives Different Threat Priorities

Mobile users access the Internet in different ways indicating key potential threat vectors for mobile devices

While the five most requested categories are consistent for both sets of users, there are interesting differences in the ways people use mobile devices and desktops. Search Engines/Portals is the leading category for desktop users but only fourth in popularity among mobile device users. This reflects a common reality in which mobile device users access the Internet through applications rather than search engines. This suggests search engines may be less popular entry point for targeted mobile malware.

Content Servers are the most requested category of content for users on mobile devices. Earlier, we saw that this category is also one of the most popular for hosting malware. As new mobile device vulnerabilities are discovered and exploited, this category of content could become a bigger threat to mobile users as a malware delivery point.

Social Networking is the second most requested category of content for mobile device users, jumping from third place for K9 desktop users. This is interesting because mobile devices offer the opportunity to communicate via social networks in the present, anywhere. Additionally, many applications have built-in sharing functions that provide updates to Facebook or Twitter from within the application.

As social networking becomes more integrated into mobile applications, this category of content will be a prime target for cybercriminals looking to exploit users. These tactics are further assisted by the small screens of mobile devices, which make it even easier for unsuspecting users to click on potentially dangerous links that are not fully displayed.

Rise of Mobile Malware

Though malware that specifically targets mobile devices is still relatively low, there is evidence of growing interest from cybercriminals. In late 2011, Blue Coat Security Labs identified a website that was hosting malicious Android downloads as part of an ongoing Android malware operation.

One of the attacks hosted on this site sought to exploit the Android operating system, utilizing a fake browser update attack. The domain registration of the site showed that it was only a couple of weeks old and included no details about the registrant, a dead giveaway that the update was not legitimate. It's important to state again that it's often more difficult to identify suspicious links on a mobile device screen than it is on the larger screen of a laptop because the complete link may not be viewable.

Blue Coat Security Labs has also seen targeted mobile malware that offers a new version of the Angry Birds game. Convincing users to download a pirated version of software has always been a successful tactic for cybercriminals. Mobile devices provide a new platform to which these attacks can be extended (Hunting for Android Malware).

Although free anti-malware software programs for Android are available, none of them compare to commercial anti-virus offerings for desktops and laptops. With the proliferation of exploit kits, it's easier than ever for cybercriminals to include exploits that target mobile vulnerabilities as part of a broader attack.

Recommendation: Traditional defenses, such as anti-virus and anti-spam endpoint solutions, simply do not translate to mobile devices. To extend control beyond the corporate network and protect devices and users, businesses will need to rely, in part, on a solution that can deliver security from the cloud.

The Bottom Line

This overview of web security developments leads to a few clear conclusions. One is that cybercriminals are ingenious, well prepared and quick to adapt to trends and technologies. They have standing network infrastructures in the form of malnets that can deliver malicious payloads at the most opportune hour. Their presence continues to grow in terms of mass market malware and targeted APTs.

Another obvious conclusion is that traditional security defenses can't protect businesses against sudden attacks from established malnet infrastructures. Instead of solutions that react to attacks as they occur – when damage has already been done – businesses need a defense that identifies and nullifies the sources of potential threats before they arrive.

Blue Coat identifies and neutralizes malnet infrastructures so that all future attacks, regardless of type or content, are blocked. The proactive negative day defense is uniquely capable of securing your users against attacks before they occur.

Appendix: Best Threat Protection Practices

Blue Coat Security Labs recommends the following actions for complete malware protection.

Recommendation 1: *Know your logs and check them frequently*

Use your reporting tools to regularly review the traffic on your network, so you can identify anomalous behavior. If, for example, you see a lot of unrated traffic coming from a computer on the network, it may be an infected machine trying to phone home to a brand-new malware command-and-control domain.

Reporting is a valuable tool for identifying botnet activity and potential APT infections. Use it to monitor a category like Dynamic DNS Hosts, which is highly correlated to APT infections.

Recommendation 2: *Block all executable content from unrated domains*

Any content that cannot be rated and is trying to download an executable has a high probability of being malicious and should be blocked as a matter of course.

Recommendation 3: *Set policies around dangerous and potentially dangerous categories*

Category	Reason
Block Category	
Phishing	Malicious sites that are designed to appear as a legitimate bank or retailer with the intent to fraudulently capture sensitive data
Malware Sources	Sites that host or distribute malware or whose purpose for existence is as part of the malware ecosystem
Malicious Outbound Data/ Botnets	Sites to which botnets or other malware send data or from which they receive command-and-control instructions
Pornography	According to a study about two thirds of attempts to download malware masquerading as other content were people looking for pornography
Extreme	Sites that are extreme in nature and are not suitable for general consumption
Hacking	Sites that distribute, promote, or provide hacking tools and/or information that may help gain unauthorized access to computer systems and/or computerized communication systems
Gambling	A high number of online casino sites attempt to persuade users to load a malware client
Suspicious	Many, if not most, of these are part of malware or spam networks
Placeholder	Generally 'dead' domains that have become 'search engine zombies' or 'ad bait' domains whose only purpose is to capture search engine traffic
Potentially Unwanted Software	Sites include adware-related and other "borderline" malware
Scam/Questionable/ Illegal	Many scammers with sites in this category are also involved in malware-related activities
Spam	Blue Coat Security Labs research has shown that users who click on spam offer are prime candidates to become infection vectors
Proxy Avoidance	Not blocking this category negates other blocked categories, allowing users to circumvent any policies. Blue Coat Security Labs research has documented that this is a regular search topic for victims of search engine poisoning malware

Block Category If Practical; If Not, Block Executable Files	
Adult	Many malware vectors begin with search engines, and many searches for Adult-themed material return links to malware
Software Downloads	This is a high-risk category because victims are actively looking for software to install, making it great vector for a malware author to target
Block Executable Files	
Open/Mixed Content	Many malware sites use open/mixed content servers to host parts of their site and occasionally their payloads. Legitimate business sites generally don't use these hosts
Online Storage	Many malware sites use online storage servers to host parts of their site, which frequently includes payloads
Web Advertisements	There has been a major increase in malvertising in the last half of 2011, where major ad networks have been duped into serving malicious ads from affiliate networks
Non-viewable	Sites in this category tend to be Tracker/Analytics services that intend to track users' visits to sites and can be seen as borderline spyware. They serve such non-viewable content as 1x1 pixel GIF 'Web beacons' or small chunks of Javascript. Since there is an implicit privacy risk inherent in these services, there is also a somewhat elevated malware risk
Dynamic DNS Hosts	Sites that do Dynamic DNS hosting or aliasing are abused on a daily basis and have been used as phone home data exfiltration sites in many high-profile targeted attacks

Note: These categories are specific to Blue Coat WebFilter. Other filtering solutions will categorize content differently.

Recommendation 4: *Block all non-SSL traffic that attempts to use port 443*

To avoid detection, many botnets use a custom encryption over port 443 for their phone home communications to command and control (C&C) servers. Using a proxy device to provide visibility into SSL traffic over port 443 and block all non-SSL traffic that attempts to use the port is a crucial defense layer.

Recommendation 5: *Layer anti-virus solutions at the desktop and gateway*

Deploying multiple anti-virus engines throughout your network will increase the likelihood that a malicious executable file missed by one engine will be blocked by another.

Recommendation 6: *Use granular application and operation controls in addition to web filtering technology to mitigate the risks of social networking*

As social networks expand to become an Internet within an Internet, businesses must have detailed analysis and control, not just of social networking sites, but also of the individual web applications and content within those sites. Granular controls allow businesses to give employees access to social networking while mitigating the potential risks of those activities. These controls should complement technology that can filter out any malicious links from within the allowable content and operations.

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

v.BC-2012-WEB-SECURITY-REPORT-V1-0212