

The WebPulse Collaborative Defense >
Proactively Defending Your Network Against Malware

Introduction

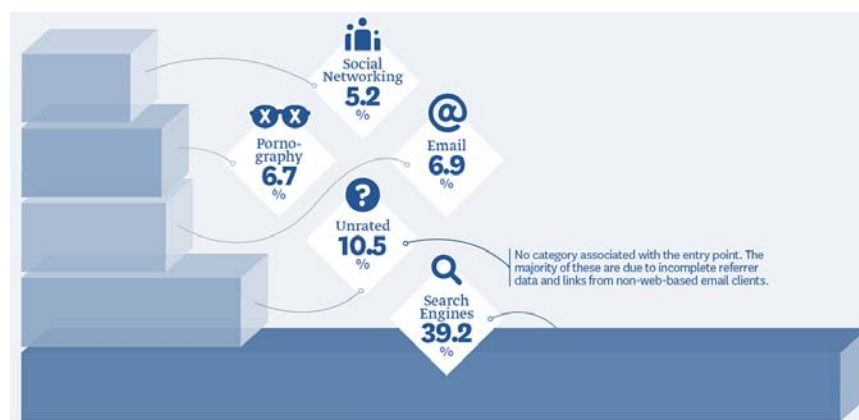
The ease with which we can access and share information in today's highly connected world is changing everything – the way we live our personal lives, interact with our governments, and run our businesses. It informs our interactions, helps us build relationships, refines our decision-making, and shapes our understanding of the world around us. But these daily exchanges are not only invaluable to us. They also become a treasure trove for a potential attacker. All of this information and all of these new ways of communicating and interacting represent a huge opportunity for financial gain for a highly organized, highly motivated cybercriminal community.

The New Threat Landscape

Spam, scams, spyware and malware are all about separating your users or your company from their property. The new threat landscape is defined by a sophisticated network of hackers working for professional organized cybercrime rings. In its 2011 Security Threat Report, Sophos reported a 60 percent year-on-year increase in malware – 150,000 new malware samples every day, or a unique file almost every half second, and 19,000 new malicious URLs each day. The volume of threats is matched only by their sophistication. To avoid being caught, cybercriminals are constantly changing the landscape. As any seasoned security expert can attest, when you think you know what to expect, the attacks quickly evolve into something new.

Attackers understand there will be some kind of blocking or restriction technology between them and their targets, and they work very hard to bypass those restrictions. However, they also understand how people currently use the web and they leverage this new user behavior to commit cybercrime.

Today, a typical web browsing session will start in a popular website we know and trust or with a search engine that is normally *allowed* by our company's security policy. In their 2011 Security Report, Sophos revealed that more than 80% of the malicious URLs they found were legitimate websites hacked by cybercriminals. In 2011 research by Blue Coat's own Security Labs, Search Engine Poisoning (SEP) ranks as the number one web threat delivery method.



In the latest research from Blue Coat Security Labs, we see by far the greatest risk coming from poisoned search engine results. Of the others, social networking now ranks as almost equal with familiar classic malware sources like pornography and email.

And of course, just like pickpockets in a busy city square, cybercriminals will go where most of the people go. Recent analysis by Blue Coat reveals the most popular web lures are being placed in social networking applications such as Facebook and Twitter feeds. Productivity issues apart, the social networking ecosystem is a prime target for scammers and cybercriminals.

In general, the effectiveness of these threats is based on lures or traps that originate from legitimate sites, popular search results or trusted friends that direct the unsuspecting user to a shifting, complex network of relays and dynamic links – a malware delivery network.

Why Conventional Security is Failing

To defend against the new threat environment, you need an approach that starts from a position of deep and current understanding of the new Internet and can identify the many potential attack vectors of a sophisticated attack. It must also be capable of keeping up with the dynamic and scalable changes in web threats.

Original, conventional security wisdom told us to build a hard shell around the network, protecting entry and exit points with firewalls. Since then we have added anti-virus and web filtering, but that oversimplifies web web-threat security on two principles: network protection as the primary defense, and preventing users from visiting the dangerous parts of the Internet. With this constrained defense model, organizations are often forced to apply static, reputation-based URL- or content-filtering policies that try to characterize the web as a series of safe or unsafe sites or content types and to use filtering to simply deny or allow access based on that characterization.

But in today's threat environment, these traditional defenses fall short because they:

- > **Rely too much on reputation:** An acceptable web site may have been infected with a trap that automatically transfers the visitor, via a silent background relay, to a malware downloader, without any action on the part of the user. Search results could be returned that have been compromised by a cybercriminal; the attacker uses bait that could link the user to a payload that has been obfuscated, encrypted, or doesn't match any known attack pattern ("signature"), so it's allowed to run.
- > **Fail to keep up:** They're too focused on the seemingly hopeless attempt to characterize websites and content as safe or unsafe based on past reputation and known risks. These characterizations tend to be static, changing only infrequently through some kind of database download or update cycle on a weekly, daily or even hourly basis. With things moving so fast, anything less than real-time awareness will likely be too late.

These limitations are challenged by today's reality and our concept of the network, and by threats that are no longer resolved by a conventional security model. Instead, as described in this white paper, today's reality needs a system that understands the new threat environment, and can work in real-time to defend against it.

The Need: New Controls for New web Behaviors

Search-engine poisoning is the number one web threat delivery method. To be more specific, image searches have surpassed text searches and are now the top vector for malware delivery. This makes users searching for pirated media a prime concern and a prime target for cybercrime.

Most employees expect to be able to use social networking at work – in fact; some roles and job functions actually require it. So today's assumption by IT is that it's no longer appropriate just to block Facebook. However, IT departments struggle with tradeoffs between security versus the need to communicate and share information. Cybercriminals know this and exploit it. Inside a social network, cybercrime can betray the trusted environment when our guard is down because we're among friends.

Traditional web control policies and filtering defenses will struggle to protect against the risks associated with this new web behavior because they don't:

- > **Understand where clicking on Search result leads:** When Blue Coat Security Labs researchers looked at categories that host malware, they found that four of the top five categories are typically considered acceptable usage and are allowed by most corporate IT policies. Remember, cybercrime has actively poisoned search results and will use them as entry points, via a series of constantly changing dynamic links and relays, to malware hosts.
- > **See inside of social networks:** A social networking message from your friend may actually be an invitation from a cybercrime ring that stole the account holder's credentials and is trying to compromise your accounts and perpetuate the infection to *your* friends.

Entry points into malware delivery networks and behavior that has been shown to be risky are often within allowed acceptable usage in categories that users are allowed to visit. So our new defenses must see beyond the entry points all the way through the shifting, short-lived links and nodes of the malware delivery network. We also need to understand what's inside the social networking web communication ecosystem, and enable policy controls that understand specific activities and applications within specific social networking domains.

Blue Coat's WebPulse Collaborative Defense

Blue Coat WebPulse™ is a cloud-based, community-driven analysis and ratings service that delivers real time ratings to users via their Blue Coat web security products. Launched in 2004, WebPulse is one of the most mature security services of its kind in the world. It leverages a global community of 75 million users that contributes all unrecognized sites and pages into WebPulse as input to its analysis and ratings service. The WebPulse community is both global and diverse, ranging from consumer users to enterprise users. This serves to deliver a robust range of inputs that uncovers both many different forms of threats, and different entry mechanisms to malware delivery networks.

WebPulse Cloud Architecture

WebPulse is based on very sound analysis-system design principles:

- > **Input:** Clearly, in an analysis system the larger the sample size the more accurate the analysis. This massive, diverse, global input is a major strength of the WebPulse system, which handles over 500 million web requests per day.
- > **Processing:** Like any analysis system, accuracy is important. Independent tests have shown that WebPulse has an advantage of about 45% in malware-detecting accuracy over the next most accurate vendor. In addition, given that this system is about eliminating risk, speed is equally important. WebPulse therefore includes a series of automated systems, mostly working in real-time, as well as deep background ratings analysis.

-> **Output:** Having found and analyzed the input (especially if it's about threat and danger) we want the alarm to be sent out as fast as possible. WebPulse outputs over 1.2 billion dynamic ratings per week on average.



With WebPulse we have a powerful mechanism for sharing intelligence contributed anonymously into the cloud, and rapidly delivering more accurate ratings and protection back to the Blue Coat web security products and their associated community of users

Inside the WebPulse Cloud

Blue Coat's own technology features a variety of tools, scanners, and background checkers, along with real-time notification mechanisms, designed to automatically analyze input from the user community and identify potentially malicious behavior. In terms of threat detection: 16 analysis techniques including antimalware, antivirus, script analyzers, web correlation, sandboxing techniques, and web-token machine analysis work together in real time. Perhaps the strongest feature of this threat detection is *dynamic link analysis*. It looks not only at the entry point – which may be an infected website, a poisoned search result or a compromised social networking link – but traces requests all the way through the shifting links and relays that make up the malware delivery network.

Blue Coat has developed over 300 language-category real-time rating libraries, the largest collection of automated web rating technology in the industry. Ratings are provided for over 80 categories with up to four ratings per web request (for example: IM/Chat *within* social networking). This is important as this granularity drives Blue Coat's defense systems and enables the controls inherent in the web filtering technology at customer sites. Ratings are provided in 55 languages, 19 of them in real time. Finally, and critically, Blue Coat's automated systems are backed up and trained by the expertise of professionals in Blue Coat Security Labs around the world. They provide in-depth analysis of suspicious behavior on the web and deep insight into the workings of malware delivery networks – not just the malware payloads they deliver.

Why WebPulse Works

The fundamental design principles, the volume and immediacy of input, and the speed and accuracy of the analysis in the context of a cloud service map offer clear advantages for people using Blue Coat web security products backed by the WebPulse service:

- > **Awareness in the cloud.** A massive number of people in a cloud-connected community, visiting many web pages and clicking many links, will provide a better-detailed view of the Internet and uncover vastly greater numbers of compromised results than any other method.
- > **Intelligence of a 16-tier defense.** Once this scale of awareness is possible, the Industry's best analysis and threat-detection technologies, featuring 16 advanced threat-analysis layers and dynamic link analysis of malware delivery networks, provide immediate and continuous protection against known and unknown web-based threats.
- > **Delivery that's on-demand.** Because WebPulse continually keeps its master cloud database constant up-to-date with intelligence and awareness, it's important to make the results immediately available to the community. A cloud service comes up trumps here by delivering without requiring downloads or other update cycles.

Clearly, WebPulse is positioned to provide more accurate threat analysis and ratings – and more quickly – than competing approaches. Evidence backs this up, as shown by these independent test results:

% of Blue Coat	Malware	Phishing
Cisco/Iron Port	41%	39%
McAfee WG	30%	26%
Websense	44%	17%
Barracuda	7%	.08%
Fortinet	5%	8%
Palo Alto Networks	22%	3%

In a benchmark test for real-time cloud defenses, **Broadband-Testing¹**, analyzed over 12 billion web requests and compared the 12,000 that were identified as malware sources or phishing attacks by WebPulse against leading vendor solutions in the Secure Web Gateway and UTM/Firewall categories.

Putting WebPulse to work

Blue Coat defenses – deployed as appliance-based, cloud-based or combined hybrid systems – leverage WebPulse to stop malware before it reaches a customer's network. New defenses or adjustments to current defenses in WebPulse can be made in the WebPulse cloud immediately, with no requirement for patches, downloads or updates at web gateways or web security SaaS users. WebPulse scales to keep pace with cybercrime and is managed by Blue Coat Security Labs.

WebPulse serves as the first layer of a multi-layered defense strategy by offering a community-driven, cloud-based malware defense that analyzes dynamic links and the content delivered from them.

Organizations use Blue Coat Webfilter, backed by WebPulse, to protect against threats, control browsing, and enable compliance.

¹ "Blue Coat Security Report," Broadband-Testing, October, 2010

A complete hybrid defense solution from Blue Coat includes additional layers, deployed in appliances, as a cloud service, or as a hybrid combination of both:

Threat Detection

Working on ratings from WebPulse, proactive threat-detection engines inside Blue Coat web gateway appliances or our web security Cloud Service can analyze all inbound web objects (and optionally outbound as well) for malware, spyware and mobile malicious code. Content filters look at file types, leveraging True File Type checks and container mismatch detection to remove any suspicious attachments or file types. As noted earlier, EXE downloads from unrated or suspicious web sites should be blocked as a best practice. Optionally, active script/content filters can be applied for web content as the Blue Coat ProxySG provides visibility to web request headers and responses. WebPulse has extensive real-time and background-active script analysis tools that are maintained by security lab experts to avoid the false positive issue. Inline threat detection provides further protection against malware and threats contained in web mail attachments and software downloads, or encrypted inside SSL traffic. Web gateways or a web security cloud service with inline threat detection provide additional defense before web content arrives on the desktop.

Defined Policies

Blue Coat Secure Web Gateway appliances and the Web Security Module of the Blue Coat Cloud Service both provide full protocol termination of all types of web traffic, to provide total visibility and context – and therefore control – over all web transactions mapped to users or groups. You can apply granular policy for applications, protocols, content and users by integrating with all of the top 11 authentication methods.

Web Content and Web App Control

Blue Coat web filtering, running on an appliance or as a cloud service, provides up to four category ratings per web request. These categories are used to apply granular control, as well as protection, in policies defined and linked to people or groups by authentication methodology. For social networking, we provide over 45 secondary ratings within the 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.

Integrated Data Loss Prevention

Blue Coat intelligence and control over content and users can be applied outbound to prevent leaking of confidential data. The Blue Coat Data Loss Prevention appliance enables organizations to begin detecting and blocking potential data leaks quickly and accurately, achieve industry and regulatory compliance, and quickly mitigate risk.

Remote Users

Individual remote users and mobile workers can be given the same level of protection as their colleagues at headquarters via the proxy appliances with ProxyClient or via the Web Security Module SaaS. Both Blue Coat ProxyClient and the web security SaaS leverage the WebPulse cloud service to provide an enhanced layer of protection over existing laptop defenses.

WebPulse In Action

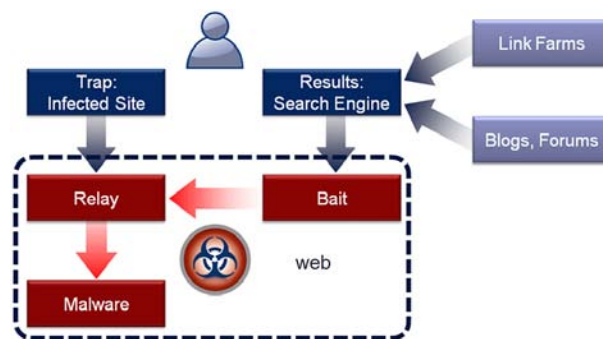
Let's briefly look at some of the techniques and mechanisms used by the new breed of dynamic web threats and how WebPulse enables you to protect your network from them.

Trap- and bait-oriented attacks

Trap-oriented attacks happen when a legitimate web site has been infected with a dynamic link, or an innocent user's social network account asks visitors to send a recommendation that includes a dynamic link. Traps will infect anyone who visits the page or follows the link; silently redirecting unaware visitors into the malware delivery network to a malware hosts many hops away.

Bait-oriented attacks normally appear as high-ranking results from a valid search on a popular search engine or a recommendation from a social network friend. Cybercrime seeds high-ranking search results for popular topics, offers free fake software to check for viruses (ironically), or enables viewing of a new picture or video recommended by a friend in a social network.

Both types of attacks try to lead the user into a malware delivery network to inject malware into their computer or collect information.



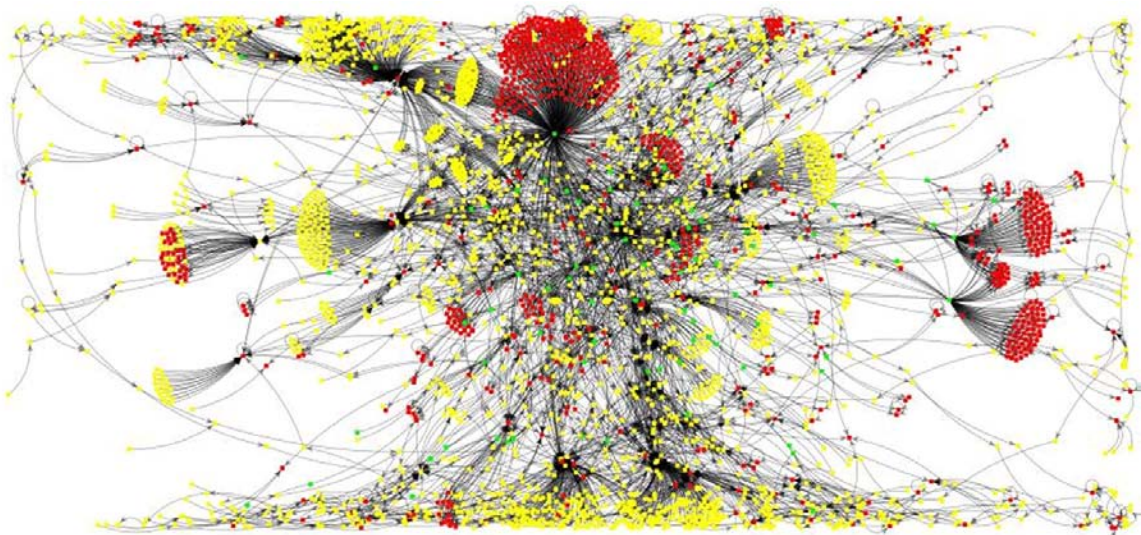
Traditional defenses that attempt to implement protection policies based on the reputation of sites won't work. But with the massive real-time awareness provided by a 75-million-strong community, WebPulse provides defense systems with awareness not only of the traps or the bait, but also of the relay and malware hosts, plus intelligence about the malware delivery networks themselves.

Malware Delivery Networks

Malware delivery networks are designed by cybercrime to route unsuspecting users to malware via relay, exploit and payload servers that continually shift to new domains and locations.

In 2011, there were on average 50 active malware delivery networks. The average number of unique host names per day for the top ten malware delivery networks was around 4,000, and Blue Coat Security Labs saw over 40,000 user requests per day destined for entry into these networks. The malware payload changed frequently during any given day in an attempt to fool anti-virus systems.

Because it is being supplied with awareness from a large, cloud-connected community, only an intelligent real-time system like WebPulse can keep up with the shifting nature and high volume of new domains inherent in malware delivery networks. Because it contains the industry's best threat-protection technology, working in real-time, the WebPulse cloud is aware of how malware delivery networks work and which domains, relay servers and malware servers they are made up for at any given time. In fact, Blue Coat security experts can now visualize them, and track subtle changes in the interconnections and routes that are gearing up for an attack.



In a visualization of Shnakule, the largest malware delivery network, we can clearly see how multiple dynamic links are intended to draw users to the malware payload server in the center.

Here is an example that illustrates the WebPulse difference and value. A bait-oriented attack, offering users a fake AV service, started June 29th 2011, leading users into the largest malware delivery network, Shnakule. The attack led to multiple dynamic links, but the threat came from malware and exploit servers that had already been identified by WebPulse as part of the Shnakule malware delivery network.

At the time of the attack, VirusTotal, a website that provides file checking using 43 different antivirus products, reported that only 2 out of 43 engines caught the attack. But with deep awareness of the Shnakule network, WebPulse was already blocking the malware payload *before* the attack was launched, protecting all 75 million members of the WebPulse community.

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 large multi-layer ad network infrastructures. And it is effective not only for legitimate advertisers, but also for cybercriminals. Indeed, in 2011, Blue Coat Security Labs identified *malvertising* (as in Malware Advertising) as number three in cybercrime's top ten methods for web attack.

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 intent is that the payload then infects the user’s computer, steals logins and passwords, or steals money or data from their employer. But as soon as a rewire event happens, someone in the WebPulse community will likely be first to identify it, and will report that to WebPulse. WebPulse will immediately recognize the relay and malware hosts in the new dynamic link configuration, and warn the rest of the community straightaway.

Fake Scanner Attacks

In a Fake Scanner attack, cybercrime will have built a fake AV scanner to look like a browser block page. These attacks are getting more sophisticated. Many now don’t even leverage search engine poisoning, social networking, malvertising, or spam to propagate. Instead, they use a more direct approach to draw a large number of prospective victims from a network of compromised sites, often pornography or illegal movie sites that have been either compromised directly or via a shared content server.



While some of the English may be awkward, it is not hard to see how someone quickly reading the pop-up could be fooled. Once the dialog box is clicked or even closed, the attack injects malware into the user’s computer.

As usual for professional malware attacks, the attack payload (a setup.exe program) is very well encrypted. Again, though, by understanding the relays and payload server elements of the malware delivery network, WebPulse users stand a better chance of being protected from attacks like these.

Conclusion

In the new threat landscape, the volume of threats is matched only by the sophistication of attacks and the constantly changing landscape. Infected reputable web properties, poisoned search results and a leverage of trusted social networking environments and new user behavior conspire to challenge traditional web security approaches. Instead, today's reality needs a system that understands the new threat environment, and can work in real-time to defend against it.

Our new defenses must see all the way through the shifting, short-lived links and nodes of the malware delivery network, and our web control policies must confront allowed acceptable usage. We also need to understand what's inside the social network ecosystem, and enable policy controls that understand specific activities and applications within specific social networking domains.

With WebPulse we have the mechanism to share intelligence contributed anonymously into the cloud, and deliver more accurate ratings and protection, more rapidly, back to the community that uses Blue Coat web security products powered by WebPulse.

The fundamental design principles, the volume and immediacy of input and the speed and accuracy of the analysis in the context of a real time cloud service provide clear advantages for people who use the products powered by WebPulse:

-> **Awareness in the Cloud**

-> **Intelligence of a 16-tier Defense**

-> **Delivery that's on-demand**

With its unique architecture, insight and granularity, WebPulse works together with Blue Coat web defenses to provide more accurate threat analysis and ratings more quickly than competitive approaches. Using Blue Coat web security solutions powered by WebPulse will give you web security and control that is more effective than traditional web security approaches.



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-WEBPULSE-V1-0911