Blue Coat

White Paper

The Alarming Shift in Cybercrime >

How Organized Attacks Now Target Your Wallet

Introduction

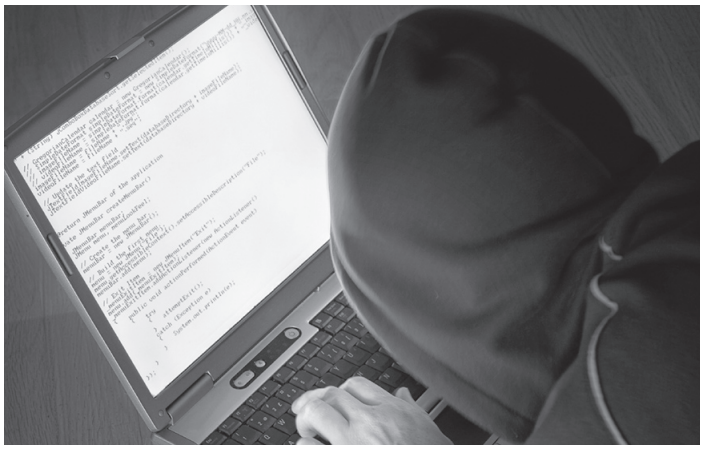
Despite over $7 billion a year being spent on anti-virus and other security software, the dangers of becoming a victim of cybercrime are increasing. What was once the hobby of amateur hackers has become the business of organized groups around the world. Cyberthieves want your identity and financial information, and they aren't just going through shady websites to get it.

It's now a popular marketing tactic to claim that "brand name" websites with well-known reputations are completely safe. However, it is exactly because of this perception that these sites are being targeted to become the unwitting hosts for invisible malware that can infect a computer just by the user checking the latest news or sports scores. Many websites of businesses, agencies, and medical and educational institutions that may not have been originally designed with tight security in mind are also being targeted for their databases which contain a wealth of personal information. For example, according to the the FBI, an average of over one million computers per year are currently being "hijacked" by botnets.

While the number of widespread, damage-causing incidents has dropped in recent years, the number of targeted, profit-driven attacks is on the rise. Fortunately, there are ways your company can protect itself and its employees. This paper will examine the shift in the nature of cybercrimes, how the thieves target their victims, and what can be done to prevent them.

The Evolution of Hacking

Hacking has been around for decades. The 1983 movie Wargames made the general public aware of the potential dangers of hackers, but it also glamorized them and inspired people to try to break into governmental or institutional computers. While some profit could be made stealing trade secrets and long distance phone codes, the main objective was prestige – how many systems could be affected and how much damage could be inflicted?



The years 1999-2001 were banner years for hackers. While there were countless cybercrimes during this period, there were three major, high-profile attacks of particular significance. First came the Melissa virus that caused $80 million in damage. Then the creation of a Filipino student, the "I Love You" virus, crippled millions of PCs worldwide. Last, and certainly not least, the Code Red worm infected hundreds of thousands of Windows NT/2000 servers, resulting in a staggering $2 billion in damages.

These incidents provided a major wake-up call to businesses and individuals who began arming themselves with billions of dollars of anti-virus and other anti-malware security suites. The number of virus attacks began to decline – dropping almost by half from 2001 to 2007. As a result, in recent years there's been a developing sense of complacency, a sense that if users delete all spam email, avoid downloading suspicious attachments, and stay away from websites of questionable morality, they will be safe.

Unfortunately, there has been an alarming shift in the nature of cybercrime. What was once the pastime of a computer geek on an ego trip has become an estimated $100 billion worldwide cash cow for professional criminals. The days of the widespread, highly visible incidents designed to cause damage and chaos, are being replaced by targeted, stealth attacks that are invisible to the victim.

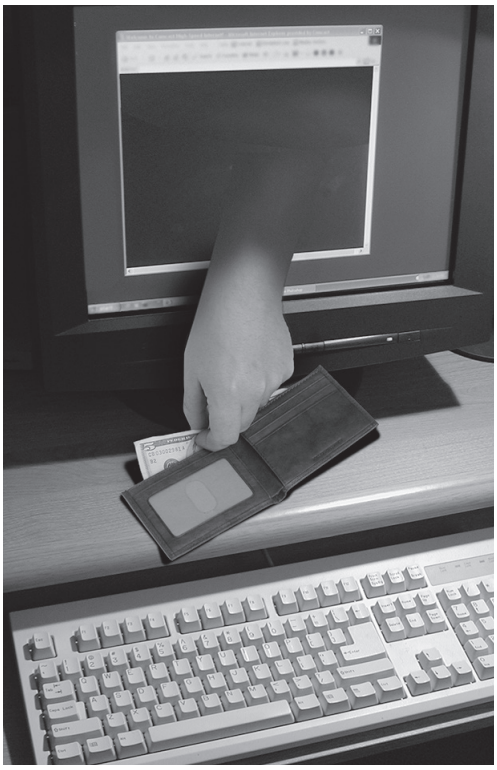
An eye-opening example involved the chairman of the highly-regarded, international Barclay's Bank. In January of 2008, someone managed to obtain enough personal information to get a bank card in the chairman's name. The thief then used the card to withdraw $19,574 from the chairman's account, and he had no idea what was happening until after the money was long gone. If the chairman of the world's 18th largest company can be so easily victimized, what hope is there for the average business and individual?

One Click Away

Analyst firms estimate that as many as 90% of Internet access points of corporate networks are inadequately protected. As a result, they are exposing themselves and their employees to Web-based attacks. However, unlike the Barclay's Bank example, a well-planned organized crime attack need not target a few high profile victims for thousands of dollars. Since personal identities have become the "currency" of the criminal side of the Internet, the

smart play is to fly quietly under the radar and steal a small amount from many people without raising any red flags. Here's an example of how cybercriminals can make an "easy million":

A criminal organization sends out one million emails that contain a link/URL to malicious software, trying of course, to cleverly disguise them as something harmless. If only 10% of recipients open the email and click on the link, the criminals will have successfully infected 100,000 computers. If they can use that spyware to get personal identity information – in the form of passwords, social security numbers, credit card and bank account numbers, etc. – from just 10% of those computers, that's 10,000 victims lined up like sitting ducks.



No sense getting greedy at this point and making your scheme obvious, as the longer a crime goes undetected, the longer the perpetrators can profit from it. If the criminals have obtained passwords, removing $100 from someone's account might go completely unnoticed. If that is done for each of the 10,000 victims, that's a cool $1 million for the criminals without them barely having to raise a finger off their mouses.

Such types of theft don't just happen "to the other guy," and no one should get a false sense of security. Consider the statistics: ID theft is one of the fastest growing crimes, and 10 million Americans become victims every year. In just a single theft from retailer T.J. Maxx, there were 45.7 million debit and credit card numbers stolen, and such threats will only escalate as cybercriminals continue to go after the easy money.

The Myth of Reputation

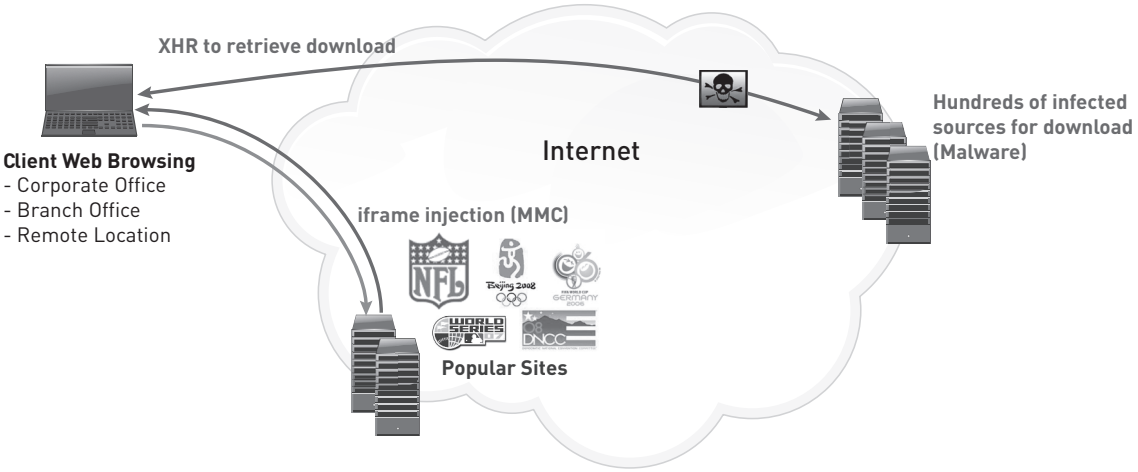
A conscientious employee may never use the company computer to visit porn, gambling, or other websites of an illicit nature. However, after a long day on the road, he may connect to the hotel WiFi to use his laptop to check his teams' scores and catch up on the latest world news. Perhaps to reward himself for landing a big account, he also purchases some new gadget he has been

wanting by using his debit card at a respected online retailer. He then goes to sleep secure in his knowledge that he has nothing to worry about.

In reality as he sleeps peacefully, a cybercriminal could be using the employee's debit card, accessing his bank account, and selling both his personal information, as well as the other employee information obtained by accessing the corporate database. How is this possible if the conscientious employee only visited websites that are household names with excellent reputations?

According to a 2007 Google report, 70% of web-based infections are in legitimate websites. These websites are specifically targeted by criminals because they are rated as acceptable web content by URL filters and pass reputation ratings with flying colors. If there is one message to be gained from this paper it is that web reputations alone can't protect you!

Attack Surface Area Profile



The Herd Mentality

Cybercriminals are opportunistic in many ways, particularly when it involves the chance to target large numbers of victims in a very short period of time. Ideal circumstances for these opportunities arise on websites that will garner increased traffic during national and international events, such as the Olympics, the presidential campaigns, the Super Bowl, and news coverage for natural and manmade disasters around the world.

Whereas legitimate businesses view "herd mentality" as opportunities for ad revenue, cyberthieves see the chance to deal in the currency of the criminal side of the Internet – identities. If they can steal the personal and financial information of everyone who visits a reputable news website to read the details of the latest terrorist attack or election results, they could victimize millions within hours.

The Invisible Enemy

It could be argued that the perfect crime is one that is never discovered, and the perfect weapon is one that looks harmless. In the world of cybercrime, that can translate into turning a legitimate website with an excellent reputation into a weapon to steal corporate, personal, and financial information without the user ever having a clue.

This is most often accomplished with Mobile Malicious Code, or MMC. MMC software is obtained from remote systems, transferred across a network, and then downloaded and executed on a local system without explicit installation or execution by the recipient, who is totally unaware of what is transpiring. This enables the low risk, low visibility, highly profitable attacks that criminal organizations seek. Below are some specific examples of techniques employed in cybercrime:

iframe Injections: An iframe makes it possible to embed an HTML document within another document, and therefore it is an ideal way to inject malicious code into websites that are perceived as being safe. This piece of HTML code then redirects Web browsers to a server that tries to infect the victim's computer using some type of malware tool. These tools are capable of attacking a PC in a number of ways, such as installing a keylogger or Trojan, which effectively allows the criminal to gain control over the infected computers.

An infamous example of an iframe injection occurred in June of 2007 and is known as the "Italian Job," as 80% of the infected sites were in Italy. Over 10,000 legitimate sites were quickly infected, including sites for hotels and tourism, and even government sites. According to the FBI, this swift, sudden, and successful attack was clearly the work of highly organized criminals.

SQL Injections: SQL injections target specific security vulnerabilities, such as the automated attacks that compromised more than 70,000 websites in January of 2008. The hacked websites included many trusted .edu and .gov sites, which had Javascript tags added to every piece of text in their SQL databases. These tags then prompted browsers to execute the malicious code. This attack was made possible by exploiting an obscure flaw in Microsoft Data Access Components (MDAC).

XHR: XHR, or XMLHttpRequest, is a web development technique that can be exploited for iframe or SQL injections, and can result in cross-site request forgeries, denial of service attacks, and cross-site scripting. Some of the many popular web applications that use this technique are Google Maps, Facebook, and MapQuest.

Fast flux DNS: Another stealth technique involves fast flux DNS, utilized by botnets to change DNS records every few minutes, and disguise delivery sites with thousands of sub-domains that have already been compromised, making host IDs useless for protection. This is a popular method for launching phishing attacks. One of the most notorious attacks of this type was the Storm Worm which was launched in January of 2007 and affected thousands of computers which used Microsoft operating systems.

When people opened an email with the subject heading "230 dead as storm batters Europe," a backdoor Trojan was injected. Within months the worm spread to an estimated two million computers worldwide, creating a zombie grid that gave the attackers enormous power, comparable to the largest supercomputers. In just one example of the Storm Worm's effect, vital computer systems of the country of Estonia were crippled and had to be shut down, including those of the government, banking institutions, law enforcement, and the media.

Right now, even more sinister malware is slowly coming to light. The MayDay and Mega-D botnets are highly sophisticated and capable of circumventing most companies' security systems without any visible exposure. What anti-malware can't see, it can't begin to defend against, so these new botnets represent an ominous trend that could signal the next cybercrime wave.

The threats posed by these invisible enemies will continue to grow and become more dangerous, fed by complacency, ignorance, and lack of precautions.

There are ways to protect the corporate networks and databases, as well as individual users, but the approach must be comprehensive and employ the latest and best hardware, software, and security policies.

The Invisible Shield

There's a saying in medicine, "First, do no harm." It is a similar situation when it comes to security measures – don't harm an employee's ability to do his work by enacting overly restrictive policies. In other words, don't block the good when trying to prevent the bad.

For example, the U.S. Computer Emergency Readiness Team made a recommendation in January of 2008 to disable features such as JavaScript, Java, and ActiveX controls, plug-ins, cookies, and pop-up windows. This presents more of a bunker mentality that equally eliminates the benefits of some of these features, and is not a realistic approach for the average user.

There is a more rational approach. At their most basic levels, the best approaches to thwart cybercriminals can be stated in three steps:

1 When it comes to outgoing and incoming web traffic, enterprises must scan everything, and if possible, do it without latency.

2 For anyone with a laptop, it is imperative to employ two-factor passwords, identity based controls, and encryption.

3 For web developers, they must design sites with security as a primary concern, and run regular penetration tests.

Specifically for an enterprise, they must create a secure web gateway that balances security and performance, without one compromising the other. Such a secure gateway would involve the following:

-> Deploy a proxy appliance with an intelligent cache to filter and scan all web traffic, never caching infected content and rescanning cached objects for gateway updates.

-> Utilize URL Filtering to reduce employee exposure to objectionable and unproductive content, plus a real-time rating service as 75+% of the Internet is unrated.

-> Deploy best-of-breed inline anti-malware software with heuristic and behavioral engines that analyze web content before it has a chance to execute anywhere on the network.

-> Leverage active script control features while having an allow list of approved "drive-by" updates.

-> Utilize SSL hardware acceleration to increase performance when analyzing encrypted web traffic for threats, never caching confidential information.

-> Implement an open gateway architecture for third party integration, such as data loss prevention solutions.

-> Test your secure web gateway for scale and performance at full load with your desired policy, plus plan for internet traffic bursts and fail over scenarios.

-> Provide LAN-quality performance and security regardless of location or policy choices.

-> Provide all the benefits of Web 2.0 while averting the dangers.

IT organizations are faced with a myriad of hardware and software products from many different vendors, but piecing together a solution may create its own problems in terms of management, and leave gaps where products don't securely overlap. Fortunately, Blue Coat offers comprehensive solutions that address all critical aspects in the fight against cybercrime.

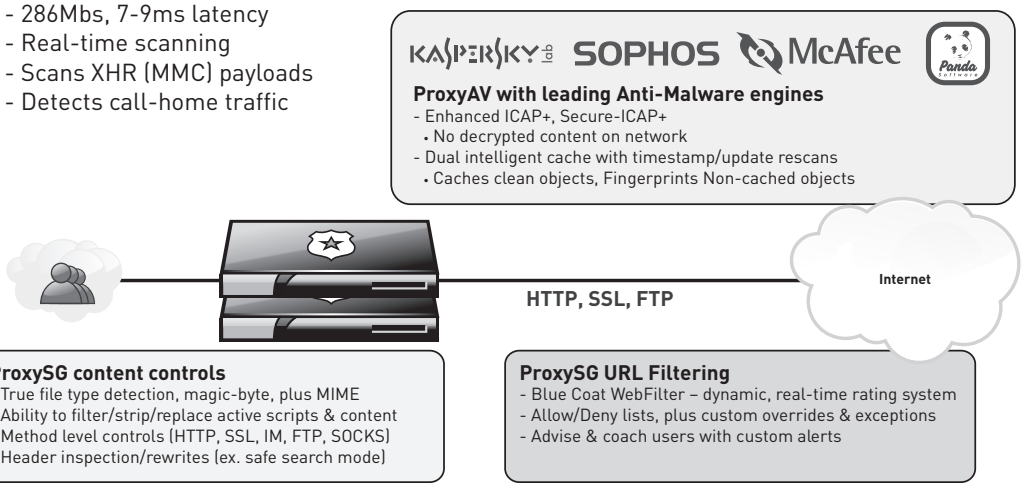
Blue Coat Solutions

Making assumptions about the safety of web communications can be a dangerous game. It is far better to adopt the mindset of "Trust Nothing, Scan Everything."

Blue Coat is the acknowledged leader in providing solutions for protection against Web-based threats. Blue Coat products not only ensure all content is scanned and secure, but also improve web performance. At the heart of Blue Coat's solution are the ProxySG and ProxyAV appliances. The following highlight some of their features.

Layer Defenses at Web Gateway

Enterprise Performance/Scale:
- 286Mbs, 7-9ms latency
- Real-time scanning
- Scans XHR (MMC) payloads
- Detects call-home traffic



As proxy appliances are positioned between users on a network and the Internet, they serve as excellent platforms for content security and control policies. Blue Coat ProxySG is the world's leading proxy appliance that delivers both security and uncompromising performance in a single appliance.

ProxySG Features

-> Performance – Patented MACH5 acceleration technology optimizes application performance regardless of where the application resides.

-> Security – ProxySG's security architecture addresses a wide range of requirements, including filtering Web content, preventing malware and other malicious mobile code, scanning for viruses, inspecting encrypted SSL traffic, and controlling IM, P2P, and streaming traffic.

-> Control – IT can custom design policies to include user, application, content, and other criteria. ProxyClient software ensures control for mobile and remote users, as well.

ProxyAV

Blue Coat's ProxyAV appliances detect malware and mobile malicious code (MMC) at the Web gateway, while delivering enterprise performance and manageability. ProxyAV allows IT the ability to choose among the best anti-malware and virus scanning engines, including Kaspersky, Sophos, Panda, and McAfee.

When integrated with ProxySG, features include:

-> Accelerated gateway performance with up to 286 Mbps throughput with less than 9 milliseconds latency.

-> Detection of malware, MMC and viruses in HTTP, HTTPS, and FTP.

-> Utilizes four modes of detection – scan, trickle first, trickle last, and defer scan (long-load web objects).

-> Ability to scan active scripts and payloads, plus detect malware calling home to report infection points.

-> Caches clean objects with timestamps, and fingerprints non-cacheable objects to optimize performance. Also rescans cached objects after anti-malware engine updates on future user requests.

-> Multi-layered defense – Anti-malware proactive detection engine, Web content analysis and checks, plus method level controls, URL filtering with real-time rating service for new or unrated content, policy and user/group authentication, and Data Loss Prevention (DLP) integration.

Combined together with the best anti-malware engines, Blue Coat's ProxySG and ProxyAV offer unsurpassed anti-malware protection by scanning all content of enterprise Web communications to stop zero-hour attacks and prevent malware from reaching desktops.

Conclusion

Blue Coat's customers include 93 of the Fortune Global 100, with over 6,000 customers across more than 150 countries. With over 40,000 appliances shipped, Blue Coat solutions are the trusted choice around the world.

Organized cybercriminals will continue to search for vulnerable targets, and any given day could bring a new wave of malware that threatens both your company's security and your wallet. This is a war that uses stealth weapons to steal identities and information, and the best defense is to protect your computer systems with the best comprehensive hardware and software solutions offered by Blue Coat.

Next Steps/Actions

To learn more about Blue Coat's distributed enterprise solutions, visit the Blue Coat web site at www.BlueCoat.com, email sales@BlueCoat.com or call 1-866-302-2628 or +1-408-220-2200.

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