WHITE PAPER

Web Malware Explosion Requires New Protection Paradigm

March 2010

invincea™

EXECUTIVE SUMMARY

The proliferation of new malicious Web sites exploded by 225 percent in the second half of 2009, according to Websense Security Labs[1], and 25 million new malware strains were created last year—that's 10 million more than the previous 20 years combined, reports PandaLabs[2]. The volume and sophistication of today's constantly evolving threat landscape demand a visionary approach to protecting the enterprise.

Dynamic Web-borne malware attacks, 80 percent of which come through the browser and prey on unsuspecting victims, disrupt business operations, resulting in:

- Escalating remediation and recovery costs
- Employee downtime and diminished productivity
- Compromised critical data and intellectual property
- Brand and reputation damage
- Illicit bank wire transfers
- Regulatory noncompliance liability
- Ruined relationships with trusted customers and partners

The losses incurred as a result of stealth cyber attacks cost large enterprises an average $2.8 million each annually, according to Symantec's 2010 State of Enterprise Security Report[3].

Cybercriminals are launching strategic, aggressive and targeted malware attacks to steal valuable confidential company information, personal data, source code, intellectual property and money. They no longer just want to send a virus to the PC; they want to control it to secure ongoing access to proprietary data and to generate additional attacks. Today's preferred method of attack targets the increasingly vulnerable Web browser or plug-in, which installs malware when users click a link to a compromised Web page—often a familiar legitimate site included in a familiar email note. Some of these innovative exploits are "drive-by download attacks" that require minimal user participation to infect the desktop, while others prey on user desires to view interesting videos and multimedia content despite warnings from the operating system or security software. In either case, users often infect their desktops, and current solutions provide little protection against content pulled down by the user. Once the desktop is infected, Advanced Persistent Threats (APTs) evade detection, run silently, spread through the network, and communicate back to the attacker through highly dynamic botnet command and control networks.

> **"The Web is the primary source of malware infection."**
>
> —Gartner Magic Quadrant for Secure Web Gateway[4]

THE NEW FACE OF CYBERCRIME

Web 2.0 collaboration and communication tools have flipped the paradigm of content published by the site owner to user-generated and interactive content. This poses a new problem since 95 percent of user-generated comments to blogs, chat rooms and message boards are spam or malicious, according to Websense Security Labs[5]. Attackers create fake profiles on social media sites, like Facebook, Twitter and LinkedIn, brimming with personal data, to trick an individual's friends and colleagues into revealing personal information and corporate data, and/or they post infectious content or links on the sites. In addition, Websense found more than 200,000 copycat social networking sites in 2009[6]. Targeted email to users enables single-click infections based on a simple message to check out a social networking site update. Making matters worse, the code used to build the applications that users access to create their site profiles often is vulnerable, according to Symantec MessageLabs.

While social networking is a great tool, providing instantaneous connectivity to friends and colleagues everywhere, the nature of this open forum exposes the vulnerability the Internet presents to corporate networks. Online social interaction drastically multiplies one's connectivity touch points, enabling opportunities to unknowingly engage with a site harboring malware. Commonly, a user will get an email from someone he purportedly knows and is pointed to a site or application that results in infection. There's almost no way to know if a person is who he claims to be. It's an expanding playpen for those with malicious intent—as an example, Facebook alone surpassed the 300 million user mark in 2009.

Organized Crime and Money Changed the Game

No longer a hacker pastime, cybercrime has become a financially lucrative business, driving the growth of Web-borne malware attacks at an unprecedented pace. There's a lot of money to be made, both legally and illegally, depending on the country of origin. Some countries maintain few, if any, reporting requirements for nefarious Web activity. In fact, what may look like an illegal enterprise in the U.S. could be a culturally acceptable business proposition elsewhere. Attackers can install malware on a machine and essentially hold a user's data hostage via encryption, requiring a ransom payment to release the key. And, stealing login information for banking sites, state and national secrets, source code and software programs delivers big payoffs.

Malware Hosts

The majority of malware hosting locations are in the U.S. and Canada, which take credit for 50 percent of the global total, according to Cyveillance's 2010 Cyber Intelligence Report[7]. The U.S. continues to be the leading malware distributor, responsible for 69 percent of malware on the Internet. Distribution sites typically target specific types of Internet users. For instance, Germany is the leading host country for malware drop sites used to passively gather personal data, according to the Cyveillance report.

> **71% of the Web sites harboring malicious code are legitimate sites that have been compromised.**
>
> —Websense Security Labs[9]

Spreading malware usually begins with clicking a recognizable and trusted link that takes the unsuspecting user to a compromised legitimate site where lurking malware awaits. A Web page hosting malicious content can exploit a vulnerability in a browser or plug-in and initiate a drive-by download, installing malware on the site visitor's computer. Other forms of malware can be placed on legitimate Web sites through third-party ad-serving networks. In one of many examples, in early 2010, cybercriminals legally purchased pay-per-click advertisements on *The New York Times* home page and used them to lead readers to malicious sites.

Threat Reaches Beyond National Security

The evolving threat is no longer exclusively a concern to those protecting our national security interests. It's been known and recognized in that arena for a while, but it's now surfacing more and more in commercial enterprises, as evidenced by the headline-grabbing attacks against

Most Common Domains in URL Spam, 2009 H2, IBM X-Force 2009 Trend and Risk Report[8]

The following table highlights the well-known domains falling in the top 10 list for 2009. In November and December, eight and even all 10 were well-known domains.

July 2009	August 2009	September 2009	October 2009	November 2009	December 2009
yahoo.com	yahoo.com	magshine.com	mediapix.ru	mediapix.ru	imageshack.us
webmd.com	blurblow.com	yahoo.com	yahoo.com	4freeimagehost.com	flickr.com
wallmotion.com	nyavekep.cn	google.com	cmeqopher.cn	imagechicken.com	yahoo.com
nyavekep.cn	blurpack.com	webmd.com	webmd.com	ipicture.ru	photolava.com
msn.com	bluenight.com	magcloude.com	google.com	topmiddle.com	pixfarm.net
pfizerhelpfulanswers.com	blurgreat.com	magroof.com	icontact.com	imageshack.us	mediapix.ru
akamaitech.net	by.ru	maghat.com	fuxehmg.com	inselpix.com	live.com
icontact.com	livefilestore.com	cmeqoher.cn	blingdisc.com	flickr.com	webmd.com
livefilestore.com	ally.com	nyavekep.cn	by.ru	commoncatch.com	picturebay.net
skyeclean.com	bankofamerica.com	ally.com	groundmons.com	yahoo.com	pixiurl.com

Google in December 2009. According to *Computerworld*, following a sophisticated attack in January 2010, Intel cited malware as a threat to its intellectual property in its February 2010 SEC 10-K filing, alerting investors to a risk that could potentially impact financial results. "We regularly face attempts by others to gain unauthorized access through the Internet to our information technology systems," stated the filing [10].

IT Fights Losing Battle

When it comes to defending against today's agile exploits, the burden typically falls on IT staffs with limited resources. Constantly required to do more with less, they're already overwhelmed managing a complex infrastructure of defense-in-depth layers and incomplete solutions. Then there are the constant internal client requests to set up new machines and deploy network devices. Increasing security demands driven by the surging frequency of attacks escalate IT operations costs and prevent staff from proactively protecting and improving the enterprise infrastructure. Since they can't keep up with the threat, enterprises typically invest limited IT and security resources in the post-infection phase, remediation and recovery.

THE BUSINESS IMPACT OF WEB-BORNE MALWARE ATTACKS

Using readily available black market automated software development toolkits, an average technologist, bored teenage hacker or developer can create increasingly capable, technically sophisticated malware programs. These attacks target individuals holding or with access to valuable information, including state and national secrets, bank passwords, financial and investment portfolio details, personal data, contacts and intellectual property. What used to be the domain of a few smart and sophisticated attackers has expanded to include anybody with malicious intent who chooses to manufacture custom targeted attacks guaranteed to evade anti-virus systems.

The Hard and Soft Costs

The most common losses are compromised confidential customer information, downtime, and theft of intellectual property, which lead to significant overlooked economic costs in terms of crippled productivity and lost revenue. An infected machine requires an IT staff investment for remediation, as well as the user's time to reinstall programs and restore the computer to its former state.

Soft costs often encompass personal as well as company brand, image and reputational damage, and loss of trusted relationships with customers and partners. Nobody wants to do business with a company that can't protect proprietary or confidential information. And, there's opportunity cost. The IT person rebuilding the machine could have been proactively improving enterprise security defenses rather than reactively responding to a malware infection that required remediation, and the knowledge worker whose machine was infected could have been performing normal job functions.

WHY CURRENT DEFENSES FALL SHORT

Due to the staggering number of new malware variations surfacing daily, current conventional defenses—even when combined—including anti-virus, firewall and Web gateway products, cannot adequately protect individuals and enterprises. At best, these reactive point solutions partially mitigate the problem after the infection incident, but they don't prevent it, and they can't detect new unknown threats. It's a game of chase. The solution providers can't keep up with the constantly growing and evolving threat because their fundamental approach relies on quickly profiling patterns and developing signatures, informing as many data points as possible, and then denying access when signatures of known malware surface. But, this means the threat is already resident on the machine, so while this may involve detecting, it's not protecting. Secondly, the solution must know what to look for—the method of attack—and there's no way to keep the tools up to date with the latest threats, given the pace of proliferation.

Anti-virus

Anti-virus (AV) software is inherently reactive, discovering infections after they occur, and unable to

The Cyveillance Cyber Intelligence Report (February 2010)[11] finds that traditional anti-virus products cannot adequately detect and protect against new and quickly changing malware threats on the Internet. A 2009 analysis measured the average daily detection rate of 14 of the most widely used AV products against real-time confirmed attacks for six months and found that they detected less than half of the malware threats. Additional testing found that the leading six AV products demonstrate only about a 50 percent chance of protection even a week after the release of new malware threats. Eric Olson, Cyveillance Vice President of Solutions Assurance, says that anti-virus and firewall systems, while necessary, are insufficient defenses because they are reactive to the threats. Malware writers own anti-virus software too and know how to counter it, explains Olson. The bad guys are no fools. They can test existing anti-virus and firewall technologies, run malware samples against them, and then make necessary adjustments to ensure a successful attack.

detect new malicious code variants. Using recently captured malware, from malwaredomainlist.com, for instance, look for the signature of the infecting process on virustotal.com. Typically, only a handful of the 40+ anti-virus products will know about the malware. Again, this is because today's threats are more sophisticated and constantly morphing to subvert detection. Some anti-virus offerings now feature heuristic patterning, in which threats are grouped and analyzed according to common characteristics. But, heuristics are guesses by the AV companies—not known threats—and thus are subject to false-positive alerting. Some AV vendors augment their resident data repositories with a real-time cloud-based service in order to reduce the time it takes to identify threats and provide updates to customers. However, the fundamental approach remains unchanged. These tools are still only identifying *known* threats, so they're missing the most sophisticated elements of the threat landscape.

Anti-virus maintains a role in a layered defense approach against malware. Ongoing vigilance in looking for known threats is a good attribute and one that makes sense. If somebody emails you a known infected file and you save it to your hard drive, your anti-virus software likely will catch it and prevent your machine from becoming infected. It's just not enough against today's threat.

Firewalls

One traditional way of protecting the enterprise is to build a wall around the castle—in other words, a network firewall, which is designed to stop inbound threats to services that should not be offered outside the organization. In the context of a Web browser, firewalls are ineffective since they block only inbound attacks, and browser malware is initiated by outbound Web page requests that pass through the firewall. The bad actor or content doesn't try to penetrate the network or desktop; it's invited in from the inside. Also, firewalls don't stop desktop exploits.

Firewalls maintain a role in a layered defense approach as they help to prevent inbound attacks against exposed ports and services. Also, if an attack occurs at the network layer, a firewall can block the connection and prevent it from compromising other machines within the enterprise. It's just not enough against today's threat.

Web Gateways

Web gateway solutions, like Bluecoat, Websense, and those offered by some of the major anti-virus providers, selectively block Web content from a known untrusted source, so when a user clicks a link, the gateway may prevent the browser from fully rendering the complete site. Similar to anti-virus and firewall programs, gateways only block traffic that they know to be bad; otherwise, they don't sound the alarm. Gateways deliver a broader solution than anti-virus because they can blacklist IP addresses and URLs, but malware can be broken up, distributed across multiple sites, and passed across the infrastructure, not surfacing as a threat until it reaches the endpoint—the desktop. This leaves gateways playing the chase game.

Savvy malware developers quickly and frequently move rogue code around to other URLs using fast-flux dynamic domains to evade blacklisting Web gateways. So a Web gateway adds value, but it cannot effectively defend against today's most prevalent and dangerous threats. It's just not enough.

Core Menaces

Current defenses (anti-virus, firewalls, Web gateways), which have become increasingly complex, expensive, and difficult to manage, don't protect against three hard-hitting and growing classes of attack. Perpetrators can simultaneously leverage these components of the threat landscape, making them even more dangerous:

Advanced Persistent Threats (APTs): The attacker seeks highly sensitive information and intellectual property. A small amount of sophisticated code is installed on a machine and lays dormant but persistent, leaping into action whenever it detects an advantageous opportunity—a user logging on to a banking site, for example. Rootkits are used to hide the processes from the operating system and system defenses. Running under the radar of existing defenses, these threats embed themselves into the system and continuously but unobtrusively search both the hard drive for desirable documents and the network for other computers to infect, while not alerting the user. Some APT variants have become extremely difficult to eradicate even when their presence is detected.

Zero-Day Attacks: These threats exploit previously unknown vulnerabilities in software; the attacks against Google in December 2009 exploited a previously unknown vulnerability in Internet Explorer. Since the vulnerabilities these attacks exploit are not known or published, no signatures of these attacks exist on Day Zero. They're brand new and indefensible by standard desktop and network defenses.

Custom Targeted Attacks: A variant of Zero-Day attacks, these threats are intentionally crafted to infiltrate the computer systems of specific individuals or organizations. Since these are custom tailored attacks, no signatures exist in virus definition files. These attacks are relatively easy to develop using today's emerging malware toolkits, such as MetaSploit. The perpetrator creates a custom targeted attack against known brands and high-value targets that flies under the radar of existing defenses.

Man in the Browser Attacks: Recent sophisticated attacks have defeated authenticated hardware tokens with one-time passwords required for banking transactions, as well as even two-man authentication rules. The so-called "man in the browser" attacks ride the coattails of the authentication. In this attack, the browser already suffers from a prior infection. When the user authenticates (via hardware token, RSA keys, two-man rule, etc.) and authorizes a wire transfer, the malware running in the browser replaces the user-directed transfer with its own wire transfer, then rewrites the balance showing on the browser Web page to conceal the subterfuge that occurred.

> **"You can search on LinkedIn and find 375 nuclear physicists who have worked at Lawrence Livermore National Lab. Social networking allows attackers to single out specific groups of individuals and disseminate a targeted attack."**
>
> —Greg Hoglund, CEO and Founder of HBGary[12]

Passive network defenses are inadequate because complex malware and varied attacks are outmaneuvering firewalls and intrusion detection systems. "The pace of software and hacker toolkit development has become highly automated. It's almost a production line approach," says Keith Rhodes, Senior Vice President and CTO for the Mission Solutions Group of QinetiQ North America. Today's threat landscape requires a paradigm shift from reactive signature-based detection of resident threats to proactive behavior-based enterprise *protection*.

INVINCEA™ BROWSER PROTECTION: A NEW BREED OF SECURITY SOLUTION

Invincea™ Browser Protection is the first and only fully virtualized secure browser that protects users from all types of Web-borne threats by running the browser in its own virtual environment, separate from the desktop operating system, to provide the best endpoint protection available. Stopping all manner of Web-borne attacks, this revolutionary solution delivers behavior-based detection, strong protection, and a safe and secure browsing environment without placing additional burdens on users. This strong prophylactic layer of defense integrates seamlessly with and fortifies the existing security infrastructure.

Detecting *and* Protecting

In addition to automatically detecting today's complex and evolving malware threats in real time, Invincea Browser Protection, more importantly, protects the desktop and the enterprise network from infection. The browser runs in a safe isolated environment, creating a protective virtualization layer that separates the desktop from untrusted content on the Web to eliminate business interruptions, Web 2.0 security risks, and desktop recovery costs. The browser always starts in a clean environment, which eliminates APTs and Man in the Browser attacks. The PC remains uncompromised, secure and operational since Web-based attacks never reach the desktop operating system.

Invincea's finely tuned sensors observe behavior in the virtual environment, and when the sensors detect any aberrant activity, the user is informed, the tainted environment is disposed, and a pristine environment is rapidly restored.

Invincea Browser Protection effectively protects enterprises and end users against the most aggressive and damaging exploits in today's threat landscape: APTs, Zero-Days, targeted attacks, and Man in the Browser attacks. Typically, when an APT hits, for example, it lodges in the operating system, usually in the kernel, beneath the radar of existing defenses. With Invincea Browser Protection, the threat impacts the isolated layer, but the virtual environment is disposable, so once the infection occurs, the environment is thrown out along with the malware. With Invincea, Advanced Persistent Threats don't live up to their name; they're not persistent in the protected environment.

Behavior- Vs. Signature-Based Detection

The Invincea solution protects against today's most prevalent and debilitating threats because, unlike existing reactive defenses, it doesn't rely on malware pattern signatures to detect a known attack vector already resident on the machine. Invincea Browser Protection inherently protects against targeted and Zero-Day attacks because its signature-free detection method proactively eliminates the threats before they ever reach the desktop.

Secure Freedom: Empowering Vs. Constraining

Web 2.0 technologies and tools are critical to the economy and workforce innovation, a company's core business value, but many organizations implement restrictive policies and controls that prevent employees from accessing sites like Facebook and MySpace. Most security solutions constrain users, prohibiting them from going where they need to go and from collaborating online to effectively perform their jobs. They can't visit certain sites, can't have full access to browser functionality, can't enable JavaScript, can't send or view PDFs, or can't view detail. The Invincea approach removes the handcuffs and empowers knowledge workers to securely go where they need to go online and browse safely to be as effective and productive as possible, without jeopardizing the enterprise's critical physical and intellectual assets. Web-borne threats are detected and stopped; PCs and data are immune to Web-borne attacks; the user and the organization are protected.

Transparent, Seamless User Experience

Invincea Browser Protection is unobtrusive to users; they are unaware, and need not be aware, that they're working in a protected, isolated environment. It has the same look and feel as their familiar native browser, so users don't have to learn anything new to browse freely and safely. The only time they will notice a difference is if the browser environment gets infected. Invincea Browser Protection will notify the user regarding the corrupted environment, which will be disposed, restoring the pristine state.

When the browser icon on the desktop is clicked, Invincea Browser Protection launches, but it looks and acts exactly like Internet Explorer, Firefox, Safari, Chrome, or the browser of choice. Enterprises can distinguish the native browser from Invincea Browser Protection by personalizing or skinning the browser with a custom look. There's no need for users to use multiple browsers unless the enterprise prefers the native browser for an internal collaboration site, for example.

Invincea Browser Protection features silent installation that can be easily deployed to many employees using the current centralized desktop management infrastructure, and it's easy to maintain and update.

Superior Detection and Reporting Capabilities: The Benefits of Shared Actionable Intelligence

Within Invincea's virtualized browser environment, malicious activity is detected, and detailed cyber threat forensic intelligence is captured and reported in real time… the site that caused the infection and the code's actions, system changes, communications and spawns—all of its behavior. Event details about all programs, executables and malware that are downloaded during a session are tracked, and all system behavior is observed. This quantifiable data includes additions, deletions or changes to system registry keys, modifications to the file system, and network requests to other servers by malware. Unlike today, an enterprise will know how, where and when its systems are infected. Using Invincea Browser Protection, an enterprise flips the collection process—now the adversary, rather than sensitive data, is collected.

At the same time the environment is being restored to its pristine state, all the data Invincea has collected during the corrupt session is shipped to a database locally or in the cloud, which will gather valuable trend information regarding which Web sites are infecting users, the nature of the infections, and whether they are known to existing anti-virus and firewall products. As Invincea deployments grow and scale, protecting more users and collecting more malware data, this intelligence gains greater value and can be used to power complementary security devices. Automated reports, including infected URLs and executables collected by Invincea, can be used to feed anti-virus definition updates and URL blacklists on Web gateways, and fortify other existing defenses.

The analytics component of this automated forensic reporting capability will apply to the individual desktop, enterprise and aggregate domains. For a particular enterprise, Invincea will be able to identify the Web sites that are infecting the company most often, the hosts that get infected most frequently, and the most common infectious vectors or programs. And, using the enterprise's cost metrics or industry trend data, Invincea will be able to compute the financial value of prevented attacks, such as the direct cost savings of not performing remediation and recovery. Since Invincea can detect, observe and eliminate malicious behavior in real time, it can compute the amount of money an enterprise saves by calculating the hard costs of averted infections.

Attack patterns within an industry segment tend to be similar. Web-borne exploits unleashed on the Department of Defense track closely with those launched against leading defense companies, for example. It's the same people after the same secrets. Although not a prevalent practice today, knowledge sharing plays a critical role in preparing to proactively respond to infectious activity.

This reporting capability is of particular interest to agencies and organizations that protect national security interests, as well as healthcare providers and financial services companies that have legal obligations to report any attack or penetration involving the personal information records they retain. Invincea data will improve their ability to ensure compliance with information protection requirements, and the reports can

System Requirements

Operating System	CPU	Memory	Disk Space
Windows XP, all service packs (32-bit only), or Windows Vista, all editions (32-bit only)	32-bit Intel or AMD x86 CPU 1.5GHz or faster	XP: 1.5 GB minimum on-board memory Vista: 2 GB minimum on-board memory	2 GB of free space

provide the accountability required for an audit, documenting all attempted attacks and how Invincea Browser Protection prevented them and disabled any compromise of personal information records.

COMPETITIVE SOLUTIONS

Sandboxes, which claim to provide a secure Internet experience, are fundamentally different from Invincea Browser Protection in that they allow the browser to run natively on the host operating system. They examine browser activity, and if there's improper writing to a system registry, for example, the sandbox will deny it, rewrite it to a safe system registry, or, most often, ask the user if he wants to allow it.

> "Our philosophy is to make security inherent and not ask users to make security choices because, odds are, they will make the wrong decisions."
>
> —Anup Ghosh
> Founder and CEO, Invincea

Invincea allows the behavior, whatever it is, but since Invincea Browser Protection runs non-natively in its own environment, all of these malicious activities occur in an isolated environment where they can be detected, monitored and eliminated before they've had an opportunity to infect the system. Sandboxes either don't detect the actions, allow them, or let the user decide, and by then, the system is infected.

Other competitive products offer a "safe" desktop for the browser, invoked manually by end users, so that any malicious code running on the system cannot access information like username and password when the user goes to a banking site, for example. But, the problem with these solutions is that users have to remember to click the safe desktop icon before going to a banking site, and these solutions do not prevent infections; they just attempt to block them from monitoring online behavior. Also, if the user goes to a trusted site like CNN.com and unknowingly gets infected, and then goes to a banking site without clicking the safe desktop icon, he will not benefit from any additional protection.

Once again, these products require users to take actions to be secure—to make the correct decision every time. With Invincea Browser Protection, the user doesn't have to remember to launch an application before going online; it's a secure browsing environment that inherently protects the machine and the network. In addition, Invincea Browser Protection employs the same browser the user is currently accessing—no special browser is needed for particular transactions. There's no need for users to remember which browser to run when visiting a banking site. The same browser can be used for all of the user's online needs. And, with Invincea's robust detection approach, the browser is restored automatically when the session becomes corrupted.

Enterprises and government organizations count on Invincea Browser Protection to eliminate business interruptions, Web 2.0 security risks, and desktop recovery costs.

INVINCEA CUSTOMERS: NATIONAL SECURITY PROBLEM SPREADS INTO SIGNIFICANT COMMERCIAL THREAT

In terms of markets served, there's a clear dividing line between federal agencies, defense contractors and system integrators tasked with protecting national security interests and most commercial entities, which are more concerned about the financial impact of Web-borne malware. However, all face escalating risks and need to take aggressive actions to protect their vital assets.

The national security and defense industrial space has highly developed cyber defense forensic capabilities and skills, and they regard any and all threat incidents very seriously. They want to identify the victim, his location, the origin of the infection, all details regarding the threat, and any appropriate offensive action.

In the commercial arena, the intensity of the threat typically dictates the reaction. When an email is used to turn a home machine into a spam relay, that's one type of attack, but it's quite a different matter when somebody gains access to a company's source code repository or customer data. Now you're messing with the secret sauce and brand reputation, and that involves economic impact. Invincea's value proposition to inherently protect against Web-borne malware threats truly resonates in environments where critical and valuable IP is at risk. Companies like Google spend billions of dollars on R&D; they can't afford to have it stolen.

Below are brief sample deployments featuring the types of agencies and organizations successfully using Invincea Browser Protection to proactively protect their critical assets:

Federal (Military or Civilian)

National security agencies are tasked with trying to balance maximum protection with the benefits of Web 2.0 collaboration. These entities are targeted for attack because they have secrets foreign states want. Espionage adversaries seek a persistent presence on Department of Defense (DoD) networks, for example, so they can leak sensitive data whenever the opportunity arises. Security professionals in these organizations typically design their defenses to block hackers from breaking into the network, but employees now are inadvertently infecting the environment, which requires a complete shift in the protection paradigm to defend against Web-borne threats. In a different role, some of these organizations monitor the depths of the "Dark Web," which results in constant infections on their machines. Invincea Browser Protection can eliminate this cycle of data loss and endless remediation.

Defense Industrial/Commercial

This segment is under increasing pressure from the DoD to improve security. Defense contractors are transitioning from a wartime mindset to demonstrating cyber security expertise to defend against the digital domain threat. Confidential information, including DoD secrets, proprietary designs and proposals, resides on workplace desktops and must be protected. Networks and machines are heavily burdened with perimeters of defense, so there's a sense of high security, but the security perimeter is highly porous, and these organizations run a particularly high risk of threats entering a sensitive environment through the browser. Also, users take their laptops home and use them on the road, where they connect to untrusted networks outside of the corporate firewall and often get infected. When the user reconnects the machine to the trusted network, either physically or via a VPN, he introduces the infection onto the trusted network. Finally, many of these organizations struggle with the balance to attract and retain knowledge workers while prohibiting access to Web 2.0 sites.

Legal

Attorneys and law firm associates typically track their work to billable hours by client. Essentially, every minute of the work day is accounted for. If an attorney can't use his PC due to infection, there will be little or no productivity, no billable hours, and no revenue. Only billable lawyers are valuable lawyers. Maximum uptime and protection are critical in this environment. Law firms also are responsible for protecting confidential client data. A nationwide law firm with an in-house IT department and managed users currently deploying Invincea Browser Protection points to ease of use as the solution's best attribute.

Financial Services

Financial fraud is a major malware target and, unfortunately, it's relatively easy to commit identity theft. This segment is where the money is, so it lures attackers. The traditional security model involves examining server-based transactions to determine if somebody is using a stolen identity, but most identity theft is the result of Web-borne malware infecting the desktop. Typically, a rootkit with a hidden keystroke logger downloads to the desktop and disables the anti-virus program before recording username and password info when the user logs on to a banking site. This sophisticated malware records picture tokens and redirects the DNS table to the attacker's Web server, which looks identical to the banking site. Another important consideration for this segment is that financial services companies must adhere to a stringent set of regulations pertaining to personal information protection or face significant penalties due to noncompliance.

The Web malware explosion shows no signs of slowing down. Only companies and agencies that recognize the limitations of existing defenses and commit to taking an aggressive stance against evolving threats will effectively protect their critical assets and the bottom line. Unlike reactive signature-based tools, Invincea Browser Protection upends the traditional protection paradigm by proactively observing browser behavior and delivering inherently effective protection to the enterprise.

REFERENCES

1. Websense Security Labs State of Internet Security, Q3-Q4 2009

2. PandaLabs Annual Report 2009

3. Symantec 2010 State of Enterprise Security Report

4. Gartner Magic Quadrant for Secure Web Gateway, January 8, 2010

5. Websense Security Labs State of Internet Security, Q3-Q4 2009

6. Websense Security Labs State of Internet Security, Q1-Q2 2009

7. Cyveillance Cyber Intelligence Report, February 2010

8. IBM Security Solutions X-Force® 2009 Trend and Risk Report: Annual Review of 2009

9. Websense Security Labs State of Internet Security, Q2-Q4 2009

10. Intel 10-K Filing, February 2010

11. Cyveillance Cyber Intelligence Report, February 2010

12. Help Net Security Q&A: Malware Analysis

ABOUT INVINCEA

Invincea, formerly Secure Command, was founded by Anup Ghosh, Ph.D. to build next-generation security software products. The company is currently commercializing technology built under DARPA funding to address the rapidly increasing security threat from Web-based malware. The core concepts underlying this patent-pending technology were proven effective via multiple years of advanced research with an expert team in the Center for Secure Information Systems at George Mason University.

CONTACT INFO

Invincea, Inc.
3975 University Drive, Suite 460
Fairfax, VA 22030
info@invincea.com
invincea.com