

Protecting Against Complex Internet Threats

- Stop spyware, mobile malicious code, and Trojan horses
- Prevent phishing and pharming plays
- Immobilize network-bound infections

Abstract

The same activities that make your employees efficient and productive – doing research over the internet, sharing files, sending instant messages to customers and coworkers, and emailing status information while traveling – are making your IT infrastructures vulnerable to mobile malicious code, spyware, viruses, Trojan horses, and phishing and pharming. Gateway firewalls and antivirus software are no match for these new, virulent threats.

To ensure the needed protection, organizations need to incorporate content-level protection into their overall security strategies. The Websense® Web Security Suite™ provides an integrated web security solution that fills the time and technology gaps left open by traditional security solutions.

Contents

Introduction	1
Exposure to Threats.....	2
Internet access	2
File sharing.....	2
Instant messaging.....	2
Email	2
Phishing.....	3
Pharming.....	3
Other web dangers	3
Hacked websites	3
Spoofed websites	4
Responding To These Security Challenges	5
The Answer – Websense® Web Security Suite™	5
Websense® Security Labs™ Services.....	6
Security Alerts.....	6
SiteWatcher™.....	6
BrandWatcher™.....	6
Desktop Security	7
Conclusion	8
About Websense, Inc.....	8

Introduction

The internet has become a critical resource employees rely on to get their jobs done. Employees use the web to perform research and gather information. They use email and popular instant messaging tools to help them stay in touch with coworkers and customers. And uploading, downloading, and sharing document files and other work products are now everyday activities.

Unfortunately, when employees perform these daily tasks, they expose the companies for which they work to serious security risks. Employers must now be concerned with more than simply preventing employees from doing things on the job that they should *not* be doing – visiting restricted or inappropriate websites, for example. Now employees are being exposed to harmful, destructive threats while in the process of *simply doing their jobs*. Companies should examine their IT security measures and determine whether they are sufficient to protect against these web-borne threats.

New security threats such as web attacks, spyware, malicious mobile code, and phishing cost organizations worldwide an estimated \$16.7 billion by the close of the year 2004.

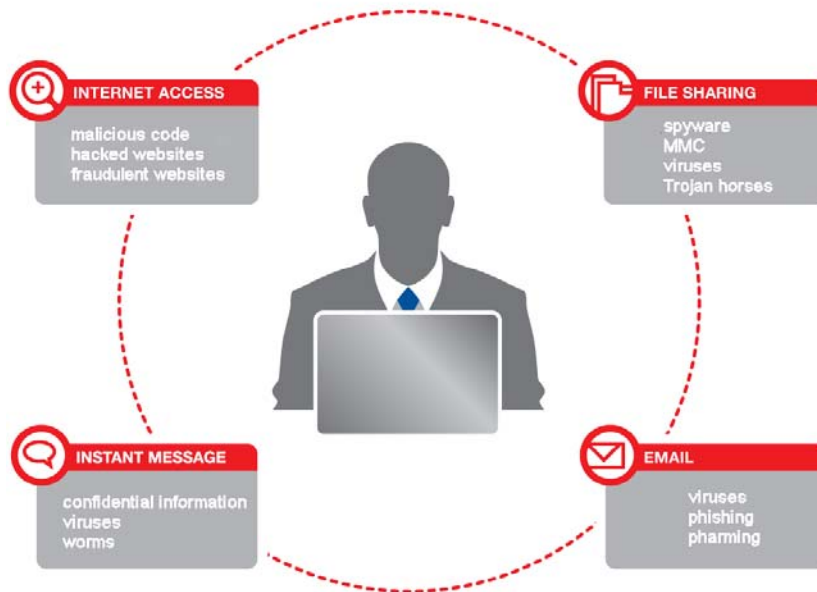
Computer Economics, 2004

Gateway firewalls and antivirus software alone cannot protect against the complex and varied malcode that threatens IT infrastructures. Firewalls can detect web traffic, but most have no means of monitoring the specific information being transferred. Antivirus solutions are reactive, not preventive; they are effective only against very specific threats, and they provide even this limited protection only after an attack has already occurred. Organizations need to supplement their existing security systems with a solution that complements these measures with content-level protection.

There is also the added complication that more employees are working remotely – that is, disconnected from the company's network – than ever before. While working remotely, employees are not protected or managed by the organization's perimeter security.

Exposure to Threats

The threats to which employees are exposed daily, vary depending on what employees are doing on the web. The illustration below summarizes some of these threats based on the task in which employees are engaged.



Internet access

While browsing on the web, employees may unknowingly visit malicious websites – websites that have either been hacked into or designed specifically to distribute malware. When a user visits one of these sites, hackers can exercise control over the user’s machine, download files, or install keyloggers or other malcode.

File sharing

When employees share files using peer-to-peer networks, they often download spyware and malicious

mobile code (MMC) along with the intended work product. Spyware gathers information about the user – often logging keystrokes, web surfing habits, passwords, and email addresses, and transfers that information back to the source site via port 80 back-channel communications. Malicious code can be delivered via web-borne viruses, Trojan horses, worms, or rogue internet code. The acquired MMC distributes itself using web pages or HTML code, including embedded ActiveX or Javascript code, and is embedded in the web pages.

Instant messaging

Using instant messaging (IM) applications, employees can “talk” and share files effortlessly. IM can help promote communication among team members and reduce the number of face-to-face meetings required. It can also be an invaluable ecommerce tool, with customer service reps supporting new customers by answering product questions, helping to finalize online transactions, and so on. Unfortunately, it can also be used to transmit proprietary company information in unencrypted format and transfer file attachments that completely bypass the existing security infrastructure. In addition, many IM downloads are infested with viruses, Trojan horses, and worms. In fact, several worms have targeted specific IM clients, sending users IM phishing emails and using IM buddy lists to spread.

IM in most companies is unregulated and bypasses security measures. In 2004, the most popular malicious use of IM was to send the user a link to a malicious website and/or a phishing or fraudulent site which then installed code, ran code, or duped the user into divulging confidential information.

Email

Even sending and replying to emails can be a risky business. Email gives hackers an easy way to distribute harmful content. Email messages can include file attachments infected with viruses, worms, Trojan horses, or other malware. Hackers send the infected files and hope that the recipient will open them.

Other malicious emails use browser vulnerabilities to spread. One example is the Nimda worm, which ran automatically on computers with a vulnerable (unpatched) version of Internet Explorer or Outlook Express.

Phishing

Phishing is another threat that capitalizes on the popularity of email as a communication tool. In many ploys, phishers send official-looking but phony emails to trick recipients into revealing confidential account or user information. Recipients are encouraged to click links in the emails, leading them to what appear to be customer service pages, complete with links, logos, and all the familiar layout and language of the authentic website. In fact, some fraudulent websites are so convincing that the users' address bar shows they are connected to a legitimate banking or ecommerce site.

Phishing is an especially lucrative threat. Brazilian police arrested the suspected leader of an internet crime gang in mid-March 2005. Police believe the gang of 18 stole \$37 million from its victims' online bank accounts by spreading a Trojan horse to thousands of computers via email. (theage.com.au, 3/18/05)

The incidence of phishing is on the rise. The Anti-Phishing Working Group identified 8,459 new phishing messages and 1,519 phishing websites in November 2004 alone (*The Washington Post*, 1/19/05). And a new Anti-Phishing Working Group report said that delivery of phishing email rose 42% in January 2005. (*New Straits Times*, 2/28/05).

Phishing impacts businesses as well as consumers. Well-known, trusted banks and other online service providers are concerned that fears of identify theft and account-napping will stop consumers from making purchases and processing other financial transactions online. Visa International has joined the first worldwide aggregation service in an effort to combat phishing. As Kamran Siddizi, General Manager, Middle East, Visa International, said, "As a leader in the payments industry, Visa is focused not just on shutting down phishing sites, but preventing phishing emails from ever reaching consumers worldwide." Microsoft, eBay, and PayPal have also joined the fight – along with the Anti-Phishing Working Group. (*Middle East Company News*, 3/8/05)

Phishing can also target confidential company information. By targeting employees (sending an email to all employees at a specific company supposedly from the IT department, for example), phishers may successfully gain access to corporate usernames and passwords. Using this information, hackers may be able to infiltrate and access the corporate network and, in turn, confidential corporate, customer, or user information, which can present not only legal liability issues, but also regulatory compliance problems.

Pharming

Automated malware that lies in wait until a user connects to a target website (primarily banks and other online financial institutions and ecommerce sites) uses a new scheme called "pharming." Like phishing, this ploy aims to steal confidential account information. Unlike phishing, however, this method does not rely on phony emails to lure unsuspecting victims; in fact, it is nearly undetectable. Pharming uses Trojan horse viruses that change the behavior of web browsers. User attempts to access an online banking site or one of the other target sites actually trigger the browser to redirect to a fraudulent site. Once a machine is infected, a user can type the correct URL and still end up at the fraudulent site.

Other web dangers

Companies also run the risk of their corporate websites being hacked into or spoofed.

Hacked websites

Hackers can transform a company website into a malicious website. When websites are hacked into, the sites themselves become attack vectors and are used to distribute malicious code. When a company's web server is

compromised, customers (or potential customers) are unwittingly infected with malicious code when they simply visit the site; these infections occur without the customer having to run any programs or open any attachments.

Spoofed websites

Cyber criminals are capitalizing on consumer confidence in certain products and brands, and using this trust to trick users into divulging confidential account information. A typical scenario involves sending users a phishing email, asking them to click a link to update their account information. The HTML in the emails looks convincing and familiar. Many users readily comply with “their bank’s” request, providing sensitive account information at the linked-to websites – sites that appear valid, but are, in fact, fraudulent.

“The long-term damage phishing can do to brands is the real concern,” according to Fran Maier, executive director and president of TRUSTe.

TechWeb News, 3/15/05

Whether or not users fall victim to these ploys, they are becoming wary and suspicious of any communications from ecommerce or banking sites, and are now less likely to engage in online transactions. These fears – although justified – may be impacting global ecommerce.

Responding To These Security Challenges

Most organizations rely on a combination of gateway firewalls and antivirus software to protect against web-borne threats. However, today's new computing threats are designed to operate in a world full of firewalls and antivirus solutions. While firewall technology has not changed much in the last few years, today's computing threats employ sophisticated techniques to bypass perimeter security. For example, many of these applications are able to communicate dynamically over different ports, thereby "hopping" right past static firewalls that block specific ports.

Moreover, the network perimeter is rapidly disappearing – the computing activities of employees using laptops, home networks, hotspots, and wireless workstations are not being managed by traditional perimeter security.

Some 71 percent of (European) IT managers are concerned about security breaches when corporate laptop and mobile devices are reconnected to the company network. But only 21 percent of companies have policies or products in place to ensure laptops remain safe when used outside the office.

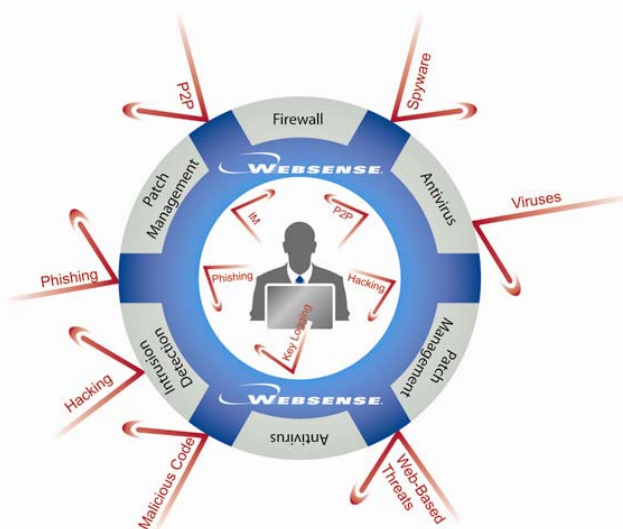
Computing, 3/17/05

Even in traditional implementations, gateway firewalls and antivirus software alone cannot protect against the complex malicious code that threatens the IT infrastructure. Firewalls can detect web traffic, but most have no means of monitoring the specific information being transferred. Spyware is penetrating firewalls; other threats like P2P or IM can do the same. Since antivirus solutions are reactive, not preventive, they are only effective against very specific threats, and they provide even this limited protection only after an attack has already occurred. Organizations need a solution that complements firewalls and antivirus solutions with content-level protection.

The Websense solution complements traditional security solutions; it addresses the gaps that these traditional solutions leave, while creating a robust security solution spanning the gateway, network, and desktop.

The Answer – Websense® Web Security Suite™

Websense Web Security Suite provides an integrated web security solution that blocks spyware, MMC, and other web-based threats, as well as spyware and keylogging transmissions back to their host sites. It also protects employees from phishing and controls the sending and receiving of IM attachments. The Websense Web Security Suite provides real-time security updates for immediate protection from new security threats and includes award winning web filtering technology, and robust reporting and analysis tools that provide organizations with complete information on user access to fraudulent sites or vulnerability to malicious code. Websense Web Security Suite also includes subscriptions to Websense Security Labs™ security alerts, as well as SiteWatcher™ and BrandWatcher™ services.



Websense® Security Labs™ Services

Websense Security Labs focuses on areas such as malicious web sites, phishing-based attacks, and other emerging threats associated with keylogging, spyware, IM attachments, and corporate use of P2P applications. Websense Security Labs mines and analyzes over 50 million sites daily for MMC. The team manages a honeynet of unprotected computers to discover new MMC, Trojan horses, keyloggers, and blended threats. The findings are used to study techniques, actions, and behavior on an enterprise network system. Information gained from the network of honeypots provides valuable information that enables Websense Security Labs to discover attacks quickly and deliver a remedy to Websense customers before antivirus signatures are available, thus closing a critical window of exposure. With this early detection system in place, Websense is able to provide a high degree of protection against rogue applications and new viruses to its customers, while providing the security community with a much-needed resource.

Security Alerts

Websense Security Labs Alerts are email notifications sent to the security community and Websense customers, informing them of emerging threats and attacks such as malicious websites, phishing attacks, keyloggers, and other web-based threats. The emails contain links to more comprehensive information about the threat, as well as remediation recommendations.

SiteWatcher™

Hackers can transform a company website into a malicious website. When websites are hacked into, the sites themselves become attack vectors and are used to distribute malicious code. Websense Security Labs sees more than 5,000 sites every day that have been hacked into and are still online; IIS, Apache, PHP, and other technologies have several vulnerabilities which are being exploited.

To help protect customers from the threat of malicious code, Websense developed a service called SiteWatcher. This valuable service notifies customers immediately if their organization's website becomes infected with MMC. This early notification allows the organization to take immediate measures to prevent the spread of MMC to customers, prospects, and partners visiting the website.

As part of its daily mining activities, Websense Security Labs mines registered companies' main websites. Engineers match the heuristics and signatures of code for MMC, and then notify registered users immediately via email if MMC is detected.

BrandWatcher™

A company's brand and reputation are one of its most valuable assets. Cyber criminals are capitalizing on consumer confidence in certain products and brands, using this trust to trick users into divulging confidential account information. New brands are being targeted daily, and the engineers at Websense Security Labs have noted more than 1,500 reports of phishing attacks every day. As keylogging malicious code becomes more and more popular, ecommerce sites and small regional banks have started to be targeted, along with the larger, more well-known banks and ecommerce sites.

The Websense BrandWatcher service lets customers know if their organization's website or brand has been targeted in a phishing or malicious keylogging code attack. This service provides the organization with security intelligence, including the attack details and other security-related information.

If the company's *website* has been spoofed, the reported information will include where the site is hosted (IP address, URL, domain, etc.), the location of the site, the registered owner of the domain name and the address space, and the status of the site (whether it is still up and running, for instance).

If the company's *brand* has been used in distribution of malcode, the attack information will include the source of the code, what the code does, and how widespread the distribution is.

"With the internet security landscape constantly changing, it is essential to employ multiple security layers to stay ahead of the threat. The Websense Web Security Suite will enhance our existing security layers and our overall enterprise security program. In addition, the new BrandWatcher service will give us more visibility into potential misuse of our company name and image."

Preston Wood, chief information security officer for Zions Bancorporation

Desktop Security

Another version of the Websense Web Security Suite is the Websense Web Security Suite- Lockdown Edition, which includes all the features of the Web Security Suite and also includes advanced lockdown features that protect desktops and the corporate network from threats associated with remote desktop use. This product prevents unauthorized applications – such as spyware, peer-to-peer file sharing, and hacking tools – from running on the desktop *whether or not the computer is attached to the corporate network*. Another advanced lockdown feature also ensures that unauthorized applications cannot launch and access the corporate network.

Web Security Suite - Lockdown Edition provides unparalleled desktop protection from web-based threats including keyloggers, spyware, Trojan horses, BOTS, scripts, and Active X controls. With the most comprehensive and effective database of web-based malicious applications, Web Security Suite – Lockdown Edition offers the highest available level of protection by detecting and blocking more web-based threats than any other solution.

Question:

Your employee has taken a laptop home or on the road and unknowingly downloads malware. How do you keep the infection from spreading into your organization's network when the employee returns to the office and reconnects to the network?

Answer:

With Web Security Suite – Lockdown Edition, you can be confident that all your computer assets are being protected, including laptops. Advanced lockdown features prevent unauthorized applications, such as spyware, keyloggers, and hacking tools, from launching on desktop or laptop computers.

Even if these malicious programs are acquired, they are prohibited from launching and prevented from transmitting information back to their sources. With Web Security Suite – Lockdown Edition, these malevolent programs are rendered powerless. Web Security Suite – Lockdown Edition also prevents these attacks from propagating over the corporate network. Network Lockdown blocks network access to specific ports and protocols by application category and stops the would-be infection in its tracks.

Conclusion

As web-borne threats become more complex and virulent, companies must face the need to supplement their existing, traditional security measures. The Websense Web Security Suite provides an integrated web security solution that blocks spyware, MMC, and other web-based threats, and prevents spyware and keylogging transmissions back to host sites. It also protects employees from phishing and controls the sending and receiving of IM attachments. The Websense Web Security Suite provides real-time security updates for immediate protection from new security threats. Robust reporting features and analysis tools ensure that organizations have complete information on user access to fraudulent sites or vulnerability to malicious code. And the Websense SiteWatcher and BrandWatcher services ensure that organizations are immediately informed of any attempts to hijack their websites or use their brand or company image in a fraudulent manner. The Websense Web Security Suite gives organizations the confidence that they are protected against and informed about emerging, complex security threats.

For more information and to download a free, fully functional 30-day trial, visit

<http://www.websense.com/Downloads/>

About Websense, Inc.

Websense[®], Inc., is the global leader in web filtering, and a premier provider of web security software. Websense products increase employee internet productivity and secure organizations from emerging internet threats by providing a proactive web security component that complements traditional security solutions. Only Websense delivers flexible, integrated policy enforcement at the internet gateway, on the network, and at the desktop. Websense provides solutions trusted by more than 24,000 customers and 19.8 million employees worldwide.

© 2005, Websense, Inc. All rights reserved. Websense and Websense Enterprise are registered trademarks of Websense, Inc. in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.