Avoiding the Newest Security Threats From Web-Based Attacks

A multi-layered approach to supplement traditional security measures

Abstract

Organizations face a complex challenge in securing the computing environment they rely on to conduct business. The employee computing environment has changed dramatically over time, offering access to rich content and tempting new applications on the Internet. Because of this evolution, organizations must now deal with even more security risks than ever before. Recent web-based attacks illustrate clearly the inadequacies of most existing security measures. Gateway firewalls and antivirus software alone cannot protect against the complex malicious code that threatens the organization's IT infrastructure. These emerging threats pose new challenges that IT must address.

This paper examines some of these recent threats in detail and explains how Websense software can be used to combat them. Because Websense software filters at multiple points at the internet gateway, network, and desktop, it offers a comprehensive solution that can provide organizations with complete protection against the emerging security threats discussed in this paper.

Websense, Inc.
World Headquarters
10240 Sorrento Valley Road
San Diego, California 92121
USA
Tel: 800.723.1166 or 858.320.8000
Fax: 858.458.2950
www.websense.com

Contents

Executive Summary

Recent web-based attacks illustrate clearly the inadequacies of most existing network security measures. 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. 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 a solution that complements firewalls and antivirus solutions with content-level protection. As described in this paper, only Websense software can provide full protection against emerging blended threats.

Background

The Challenge

IT managers are under tremendous pressure to provide an open, collaborative networking environment. At the same time, they are responsible for protecting the organization from the financial losses and legal liabilities that may result from security breaches. Organizations have responded to this challenge by deploying a combination of security products and services from different vendors. These technologies, such as antivirus protection, firewalls, and intrusion detection systems, are generally excellent within their intended sphere, but they do not provide sufficient protection from advanced blended threats such as Code Red and Nimda, which cost businesses worldwide an estimated $3 billion, according to research firm Computer Economics.

The internet has become significantly more dangerous for users in recent months, with several attacks using the web to launch and spread into the mainstream. Some new exploits that specifically targeted web browser vulnerabilities — including the web attacks of June and July 2004 — illustrate the sophisticated techniques hackers have developed to spoof, or fake, websites and how easily malicious code can steal user names, passwords, and other vital information.

Blended Threats

Nimda and Code Red are two examples of "successful" blended threats - a malicious application that uses the same methods to spread as an ordinary virus or worm but blends the ability to spread through, or attack, security vulnerabilities commonly found in applications and operating systems. A virus needs to be a script or macro, or attach itself to an executable file. Worms often spread through memory and disk space. A blended threat may attempt to infect by having the properties of a mass email virus and also by attempting to find software that hasn't been updated to plug a security hole, to infect or attack that operating system or application.

Once a blended threat gets into a desktop or server, it can destroy or manipulate files. Or it can leave back doors, secret ways to get back into a system left by the programmer; Trojan horses, programs that appear to be benign but aren't; and zombies, small programs that can be awakened later to turn the infected system into one of many systems used to launch distributed denial-of-service attacks that overload a server with information requests. Blended threats create "virtual hackers" by automating the ways hackers break into systems.

InformationWeek, May 20, 2002

Hackers can use vulnerabilities in web browsers to inject phony content — such as their own credit card-stealing form — into a frame of an actual trusted website. Users visit what they believe to be a trusted site, such as an online bank or an e-commerce site, and while the image they see *looks* valid, it is, in fact, a sham, and they are now vulnerable to hackers working in the background.

Seemingly every day a new threat emerges, whether through web attacks, spyware, malicious mobile code, or phishing. These threats cost organizations an estimated $12.5 billion worldwide in 2003.[1] Organizations cannot predict

[1] Source: InformationWeek, July 5, 2004.

when the next threat will appear, where it will come from, or the exact form it will take. The key is to plan now to protect your organization from new, emerging, and increasingly dangerous security threats.

> *"Preparing for [that] emergency requires a security architecture capable of automatically detecting and blocking threats, both known and unknown. The dominant [antivirus] technologies today are those that filter out infections based upon signatures. This approach works only with known vulnerabilities and exploit code. Given the shortening time between vulnerability disclosures and exploit availabilities, that simply isn't enough. The goal should be to have enough defense layers so that a breach of one layer won't compromise your ability to do business."*
>
> *Eric Litt, Chief Information Security Officer, General Motors Corp., in Computerworld, July 12, 2004*

Recent Threat Examples

The malware attack of June / July 2004 known as *JS/Scob-A* (also called *Download.Ject* or *Toofer*) ushered in a new kind of threat, using the web itself as the method for transporting the malicious code. Websites were hacked into, and unsuspecting users who simply visited one of the infected sites were attacked. The attack capitalized on vulnerabilities in both Microsoft Internet Explorer and specific web servers.

When users visited infected web sites, their clients were redirected to a Russian website, where a backdoor and a keystroke logger were secretly installed. The insidious program sat quietly in the background, waiting. When it detected that users visited certain target URLs (primarily bank web sites), the program started logging keystrokes. Sensitive information such as user names, passwords, and account numbers were then posted directly to the hackers' host computer in Russia. Unlike other recent attacks, in which malware was installed when a user responded positively to a lure in an email or clicked on a web site (often called "phishing"), *all this occurred with no user action at all.*

Internet service providers and law enforcement agencies, working together with Microsoft, identified the web server in Russia and shut it down on June 24, 2004. Although the foreign website that was spreading *JS/Scob-A* is now shut down, IT administrators should anticipate copycat versions of this attack, as has been common in previous outbreaks.

> *"The security landscape changes daily as hackers continue to advance their techniques of writing malicious code to infiltrate organizations, which bypass traditional security measures such as firewalls and antivirus software," "Most recently, we are seeing spyware, IM and P2P as very alluring avenues for malicious attacks. As these threats multiply, it's important to not only alert the public of these dangers, but also notify them of what types of security remedies are available to mitigate these threats."*
>
> *Lawrence Orans, Principal Analyst, Gartner Research*

Websense customers using Websense Enterprise® Security PG™ software received enhanced protection against the recent internet attack from *JS/Scob-A* (aka *Download.Ject* or *Toofer*). Websense technology prevented its customers from being infected in the critical time before antivirus vendors had signatures available to combat it.

Chronology

Websense became aware of the *JS/Scob-A* threat on the morning of June 24, 2004. The Internet Storm Center (SANS) released a report that a new Trojan horse was on the internet. At the same time, a Websense customer requested help in identifying some mysterious web traffic going to a website in Russia. That same day, Websense Security Labs researched the security threat and added the Russian website into Security PG.

By June 25th, Websense had updated its mining processes to search for sites infected with this new malicious code. Websense determined that approximately 130 sites were infected and that all pages on these sites were infected – a total of more than 10,000 URLs. Websense updated its products through the nightly database download to include these sites and web pages.

On June 28th, Websense released statistics on client and server infections to the security community. This information included the fact that Websense had identified \more than 130 unique domains that were still infected. These sites were running IIS 5.0 and SSL and were infected on both HTTP and HTTPS URLs. The IP addresses of these sites were in the United States, Australia, New Zealand, Canada, Japan, Spain, the United Kingdom, and Norway.

On June 29th, analysis and research identified yet another new exploit (now called *IMBIG.Trojan*), which also uses websites to infect users. This new exploit uses a different IE vulnerability and a BHO (Browser Help Object) that records keystrokes and sends them to a remote website. Websense identified a site that was infected and captured a sample of the malicious code to reverse engineer it. It was discovered that the first part of code went to another website to get another piece of the malcode. This new version tied two applications together. Websense updated its products through the nightly database download and blocked the newly identified infected websites and then reported the findings to the security community.

Table 1. Summary of Events

Date	Event
6/24	SANS releases report of new Trojan. Websense customer requests help identifying anomalous web traffic. Websense Security Lab adds Russian website into Security PG.
6/25	Websense mining process searches for infected sites and identifies 130 sites. Security PG updated to include all sites and pages (10,000 URLs).
6/28	Websense releases stats to security community: 130 unique domains still infected.
6/29	Websense research identifies another new exploit (IMBIG.Trojan), captures code, and reverse engineers it. Websense updates products to block infected sites. Websense reports findings to security community.
7/5 7/6	AV signatures for JS/Scob-A and IMBIG.Trojan available and released.

> *"I believe that this particular type of malware represents a huge threat to the online financial industry. As the proliferation of ad/spyware shows, installing executable software on users' machines is far too easy. The approach of using the BHO makes this method of stealing identity information all the more insidious."*
>
> *Tom Liston, Researcher for SANS who analyzed the attack, in eWeek.com, June 29, 2004*

It took several days for many antivirus companies to have signatures for this malcode available and released. During this period of time, Websense customers were protected, even though antivirus virus signatures were not yet available.

The three points of policy enforcement provided by Websense software — at the internet gateway, on the network, and on the desktop — comprise a multilayered security approach to protect against this new type of threat. Security PG blocks employee access to websites known to have mobile malicious code (MMC), such as those spreading the Trojan horse. Security PG also prevents the transmission of sensitive information to unauthorized servers (the web server in Russia, for instance). Security PG also features SiteWatcher™, a value-added service that alerts IT administrators if the organization's external website becomes infected with MMC.

> *"The new attacks on the IT environment are becoming more malicious and sophisticated, circumventing traditional antivirus solutions. The nature of the uncertainty and potential harm to the network are certainly top-of-mind for security professionals. With Websense Enterprise Security PG and Client Policy Manager, Websense customers can block employees from unknowingly visiting sites with malicious code, as well as effectively protect their computers and the network from infection."*
>
> *Dan Hubbard, director, Security and Technology Research, Websense, Inc.*

For added protection at the desktop level, Websense® Client Policy Manager™ (CPM) ensures that employee computers are safeguarded from MMC while in "application lockdown" and "network lockdown" modes. Application lockdown allows only applications on an organization's approved list to run on employee computers. This feature provides robust protection against rogue Trojan horses and other internet threats such as spyware. Network lockdown ensures that infections on employee computers are not able communicate and propagate themselves across the network, thereby protecting the network from further spread of malicious code once it has hit.

> *Despite sitting behind firewalls and anti-virus gateways, local desktops are still sources of virus and worm infections, especially from traveling users who catch a bug on the road and then unleash it onto the LAN when they return. Local desktops also expose the network through Trojans, spyware, and rogue applications downloaded from the Internet, as well as through unpatched OSs.*
>
> *Network Magazine July 1, 2004*

How Websense Protects Against Web-Based Attacks

Websense's three points of policy enforcement — at the internet gateway, on the network, and on the desktop — comprise a multilayered security approach to protect against web-based attacks.

The heart of Websense Enterprise® is its Master Database, the largest and most accurate collection and categorization of sites, protocols, and applications in the industry. The Websense Master Database includes the most frequently accessed sites, protocols, and PC applications on the web. The database contains more than 8 million sites, in over 90 categories and more than 50 languages.

Sites are identified through proprietary software techniques, including WebCatcher™, and then classified into categories using a combination of unique processes and technologies and human web analysts. The database is refreshed every seven hours for accuracy and is updated daily with additions, changes, and deletions.

WebCatcher allows Websense Enterprise customers to send uncategorized URLs — websites that do not fall into any of the company's more than 90 categories of content — to Websense for analysis. Websense's unique WebCatcher technology identifies uncategorized sites based on access logs from hundreds of Websense customers worldwide.

Sites are evaluated, categorized, and then quickly added to the Websense Master Database. This happens on a daily basis, allowing for continuous refinement in the accuracy and coverage of the database.

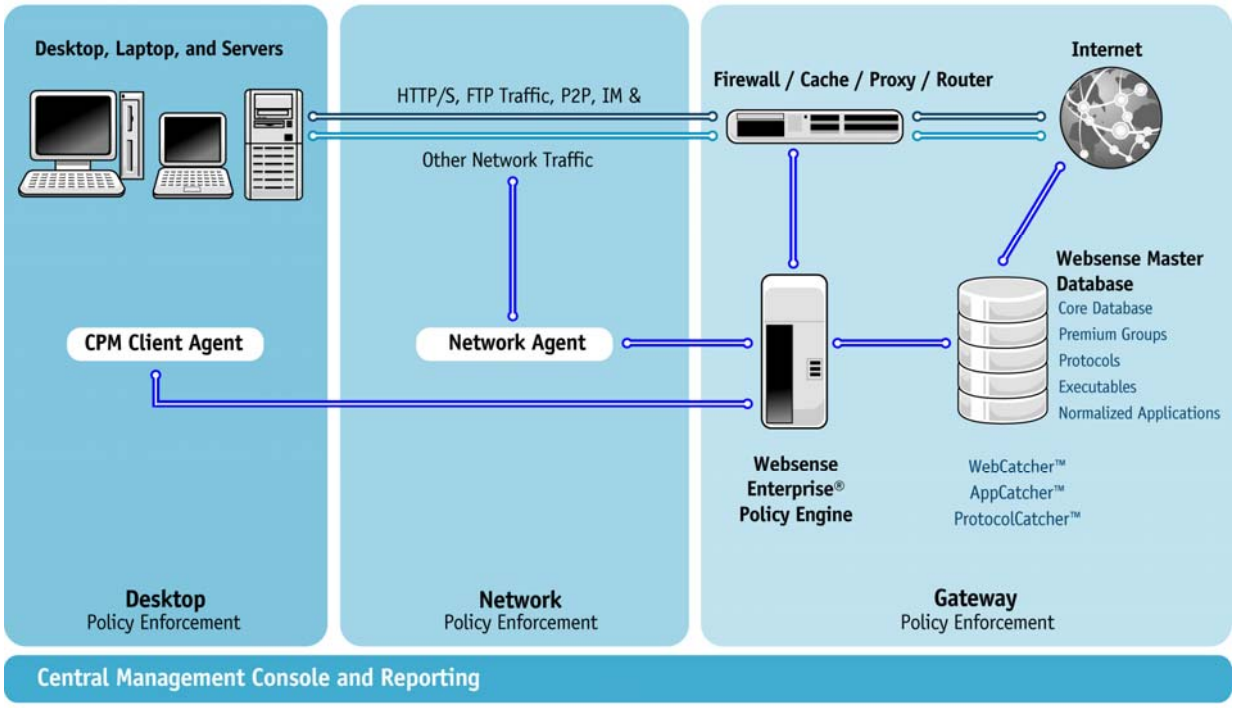

Figure 1. WebCatcher identifies uncategorized sites, which are then evaluated, categorized, and added to the Websense Master Database.

Database enhancements triggered by WebCatcher submissions are made available to all Websense customers through the daily database download process. Thus, each Websense customer receives the benefit of the aggregated surfing patterns of the entire Websense customer community. Capturing all uncategorized URLs from customers is the best possible method to ensure coverage in filtering employee use of the internet. Websense's WebCatcher feature combines state-of-the-art classification technology and human review to enable optimal precision. The result is a control list that maximizes both breadth of coverage and accuracy.

AppCatcher™, a feature of CPM, ensures that new or not-yet-classified applications and executables launched by employees are categorized and added to the Websense Master Database. AppCatcher does for customer applications what WebCatcher does for URLs. AppCatcher virtually ensures that Websense will be able to stay abreast of the newest executables and applications to ensure they are categorized and normalized. When AppCatcher is enabled, information about each unknown executable is automatically and privately sent to Websense, where application analysts research it, assign it to a category, and perform normalization[2] as well. When the CPM server next downloads the updated Websense application list, information about previously unknown applications and executables is added, thus allowing them to be automatically categorized and normalized.

[2] Normalization involves classifying multiple executables into a single application name. For example, even though Microsoft Outlook is composed of multiple application components, CPM's inventory assessments will identify and report a single application called "Microsoft Outlook."

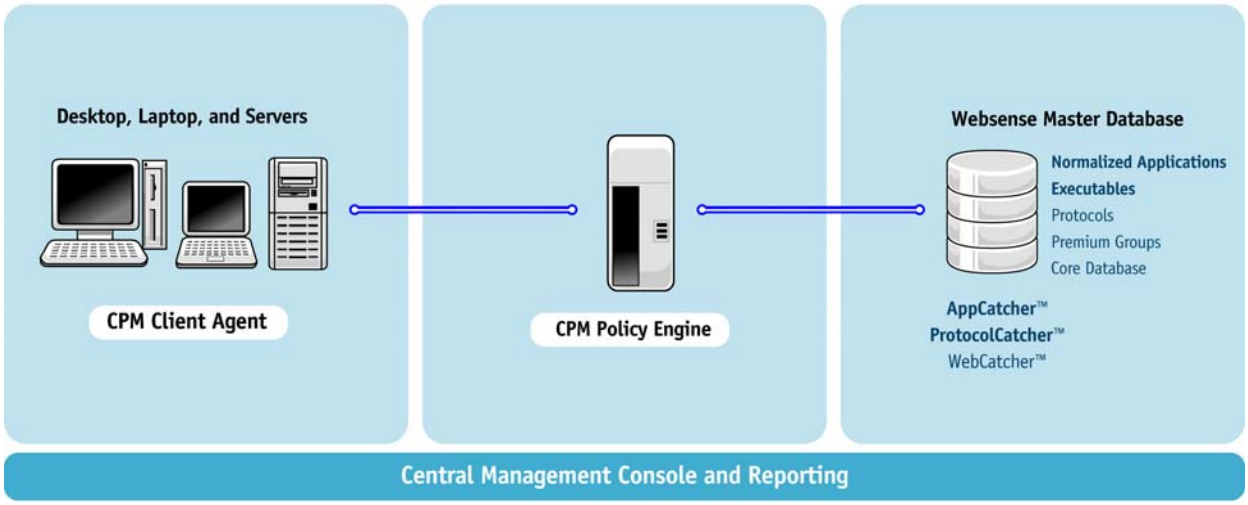

Figure 2. The CPM AppCatcher collects, categorizes, and normalizes unknown applications and executables.

WebCatcher and AppCatcher both leverage Websense's world-class mining, categorization, and distribution technologies and expertise and are part of what makes Websense Enterprise unique.

Conclusion

Seemingly every day a new security threat emerges, whether one like the recent web attacks described here, or through spyware, MMC, or phishing. Recent web-based attacks illustrate clearly the inadequacies of most existing network security measures. Gateway firewalls and antivirus software alone cannot protect against the new, complex malicious code that threatens the IT infrastructure. Organizations cannot predict where the next threat will come from or the form it will take. The key is to plan ahead and protect against new and emerging security threats.

Traditional security measures cannot adequately address these emerging threats. Companies need to augment their existing security defenses with a solution that offers true content management. Websense's three points of policy enforcement — at the Internet gateway, on the network, and on the desktop — comprise the needed multilayered, content-level protection for the employee computing environment.

For more information and to download a free, fully functional 30-day trial, visit **www.websense.com/downloads**.

About Websense, Inc.

Websense, Inc. (NASDAQ: WBSN), the world's leading provider of employee internet management solutions, enables organizations to optimize employee use of computing resources and mitigate new threats related to internet use, including instant messaging, peer-to-peer, and spyware. By providing usage policy enforcement at the internet gateway, on the network and at the desktop, Websense products enhance productivity and security, optimize the use of IT resources, and mitigate legal liability for our customers. Websense protects more than 23,600 customers worldwide, representing 18.5 million seats. For more information, visit www.websense.com.