FROST & SULLIVAN

A MORE SECURE APPROACH TO DYNAMIC WEB THREATS

A Frost & Sullivan White Paper
Sponsored by Postini

Analyst and Author: Terrence Brewton, Research Analyst, Network Security

"Partnering with clients to create innovative growth strategies"

TABLE OF CONTENTS

INTRODUCTION

Organizations of all sizes are dependent on the Internet for business. Access to the web is not an option anymore. However, criminal hackers have cost United States (US) businesses an estimated $67.2 billion a year, according to the US Federal Bureau of Investigation (FBI).[1] Often enough the vector used to exploit an unsuspecting user's vulnerabilities are not the usual infectious websites such as pornography sites, but increasingly are seemingly benign websites such as MySpace and YouTube, as well as Web-based clients such as Instant Messaging (IM) and Web mail.

Alarmingly, and yet not surprisingly, hackers are supported by organized crime syndicates. These syndicates are using the skills of talented hackers to crack open corporate network vulnerabilities and to exploit the network's vital information to be sold and extorted for financial gain. The latest variants of malware are able to quickly adapt to past and present countermeasures thereby bypassing them and infecting an enterprise in a matter of seconds. Therefore, yesterday's strategy of protecting enterprises with firewalls and deploying the latest patches, Universal Resource Locator (URL) block list and anti-virus signatures are no longer effective in stopping Web-borne threats. A new approach, one that can respond to dynamic threats in real-time, is needed to secure this vital communication channel.

CHALLENGES TO PROTECTING THE ENTERPRISE

There are numerous challenges involved with protecting the enterprise today. While this is a high priority, there are still many outdated beliefs that are held in the enterprise. These beliefs are very dangerous as many of them can lead to a false sense of security.

Older Technologies Do Not Protect Against Today's Malware

Older filtering technologies such as proxy servers and URL filters are effective in enforcing acceptable use policies by preventing employees from visiting the usually offensive pornographic and hate sites that can result in costly workplace lawsuits. However, present day URL filters don't provide security because they are heavily dependent on old analysis rather then real-time analysis. They simply cannot protect against dynamic, malicious websites that can change content on the fly.

Present day hackers are more concerned about financial gain rather than public notoriety. Therefore, in order to avoid detection and to capitalize on financial gains, hackers and malware engineers are developing tools that can quickly capitalize on zero-day exploits and unknown vulnerabilities. Many of these vulnerabilities and exploit tools are not publicly shared, even within the hacker community, and by the time vendors have discovered and released patches and anti-virus signatures, the hackers have already exploited and pilfered vulnerable networks.

1. Joris Evers: "Computer Crime Cost $67 Billion, FBI Says"

Debunking the Porn and URL Myths

Myth: If I do not visit porn, gambling and hacker sites I am safe from malware.

Fact: Sites of leading corporations like Google, Tom's Hardware and AMD have been hacked in the past and other leading corporations will be hacked in the future.

Myth: My URL filter blocks all malicious web sites. Therefore any site that I am allowed to visit is safe from infections.

Fact: URL filters are not updated in real-time and zero-day exploits are released on the Web daily. Therefore all websites could be infected and you would not know it until it was too late.

Myth: If I have the latest software patches and ant-virus updates, my enterprise is protected.

Fact: While the latest software patches and anti-virus signatures do protect enterprises from known viruses they do not protect against zero-day exploits or unknown viruses. New exploits and viruses are hard to detect and when detected, it takes days or weeks for a patch or anti-virus signature to be developed and released.

Even though major virus outbreaks are rarely reported these days, highly regarded websites continue to be hacked. For example:

- The Dolphin's Stadium website was hacked before the 2007 Super Bowl. The website redirected thousands of visitors to phishing and malware sites.
- The Better Business Bureau links sponsored by Google infected users with key-loggers that recorded and stole banking information.
- Tom's Hardware - a popular technology Website - infected users over the course of several days earlier in 2007 with Trojans that stole personal information from their computer.

The Constantly Changing Threat Landscape

Insider Threats

There exists a common misconception that internal threats are always either disgruntled or terminated employees. This is a dangerous misconception as the greatest number of internal threats comes from valuable workers who unknowingly bypass safeguards to download family pictures, listen to their favorite webcast or click on a greeting card link. Bypassing controls and safeguards opens the network to bandwidth intensive applications that can cripple the network and to a withering array of malicious applications. Internal threats can be very costly to an organization, and it is estimated that a company of moderate size could pay over $14 million annually to respond to insider security breaches.[3]

Most computer security experts agree that security training augmented by real-time content filtering technologies is the best security practice to guard against both the internal and external threats that feed on an enterprise's vulnerabilities.

Attack Evasion

Another emerging threat is the use of evasive attack methodologies. This new tactic is used by hackers to bypass signature-based and URL database filtering technology. Criminal hackers are currently setting up Web servers that offer legitimate advertisements or content to the visitor. However, the advertisements and content contain malware that is injected only once into the user's computer and on subsequent visits the user is not infected because their IP address has been recorded. Additionally, this technology evades filtering technologies and reputation services by identifying the service's IP address and heuristics and presenting legitimate content. As a consequence, they avoid being black or gray listed, opening them up to more networks, like yours, to infect.

As reported in the Google report, "The Ghost in the Browser,"[2] there are four ways that users can get infected from websites:

1) Web Server Security – where vulnerability in a web site is exploited by an attacker.
2) User Contributed Content – user-edited blogs, profiles, comments, etc. often are not all that they seem to be.
3) Advertising – Links to advertising are really just Javascripts pointing to Javascripts pointing to Javascripts, which can be compromised anywhere along the chain.
4) 3rd-party Widgets – Widgets are external links to applications that webmasters use to add utility or value to their web site, like visitor counters, calculators, etc.

No matter the technique, the point is that as more content comes from more and more sources, the chain of trust for that content gets weaker and eventually breaks, resulting in viruses, keyloggers and Trojan Horses on your network even though your users never violated your Appropriate Use Policy.

2. Google Report Ghost in the Browser 2007
3. 2006 Annual Study: Cost of Data Breach, Ponemon Institute

Blended Threats

Multi-channel or blended threats are a network attack methodology that combines the different characteristics of computer worms and viruses. The blended methodology exploits known or undocumented vulnerabilities in computer systems and networks. Before deploying their attack methodologies, hackers download the latest virus signatures and simulate their methodologies to ascertain how fast or the method by which their attack will be detected. The simulation will give them the needed foresight to fine tune their attacks for effective strike. A documented example of such attacks is the Storm worm and its many variants that hit the Internet in late 2006 and has kept mutating into September of 2007.

Web 2.0

The growth and power of social networking sites, wikis and blogs is directly attributable to rich content provided by users, known as Web 2.0. However, this technology presents new vulnerabilities that can expose the workplace to Internet-based attacks. Web 2.0 is heavily dependent on lightweight programming models such as Extensible Markup Language (XML), which are vulnerable to session hijacking. Asynchronous JavaScript and XML (Ajax) frameworks, another popular Web 2.0 technology, have serious coding flaws that would enable a knowledgeable hacker to exploit the flaw via evasive attack methodologies. In December 2006, MySpace shut down hundreds of user profiles that were infected by a worm that took advantage of an Ajax vulnerability in order to redirect users to phishing sites where they were asked to confirm usernames and passwords.

SOLVING THE CONTENT FILTERING CHALLENGE WITH ON-DEMAND SERVICES

As the threat landscape is being transformed by brazen hackers who are developing new zero-hour attacks to expose an enterprise's vulnerabilities, IT managers cannot depend on present technologies such as URL filtering and appliance-based solutions. Most importantly, the majority of network defense mechanisms such as firewalls, UTM and other network-based filtering technologies lack the ability to respond to and prevent attacks due to a lack of the most current signatures, patches and URL block lists. The cost of ownership is staggering in terms of subscription costs, additional hardware and manpower required to maintain hardware-based technologies. Therefore, a host-based or on-demand alternative can be an effective means of stopping Web-borne threats and keeping cost of ownership low.

On-demand services have proven to be one of the best approaches for corporations seeking an agile solution when defending against ever-changing malware threats, throttling

the misuse of bandwidth and preventing data leakage. IT managers and CIOs should take notice of the following when considering integrating their network with a managed service:

- The service should easily integrate with the existing enterprise and have little to no downtime.
- The service should reduce the overall cost of ownership for hardware and manpower.
- The service should provide scalable protection against known and unknown threats, including zero-day exploits.
- Management tools should be securely available on a 24x7 basis from anywhere in the world.

Comparing Web Filtering Technology Functionality

	URL Solutions	UTM Solutions	Appliance-Based Solutions	On-Demand Solutions
Effectiveness against known and zero-day exploits	Low	Moderate	Moderate	High
Provides real-time threat updates	No	No	No	Yes
Automates surfing restrictions	Yes	Yes	Yes	Yes
Cost of ownership	Moderate	High	High	Low
Degree of initial implementation, continued maintenance and manpower cost	Moderate	High	Moderate	Low
Scalability	Moderate	Low	Low	High

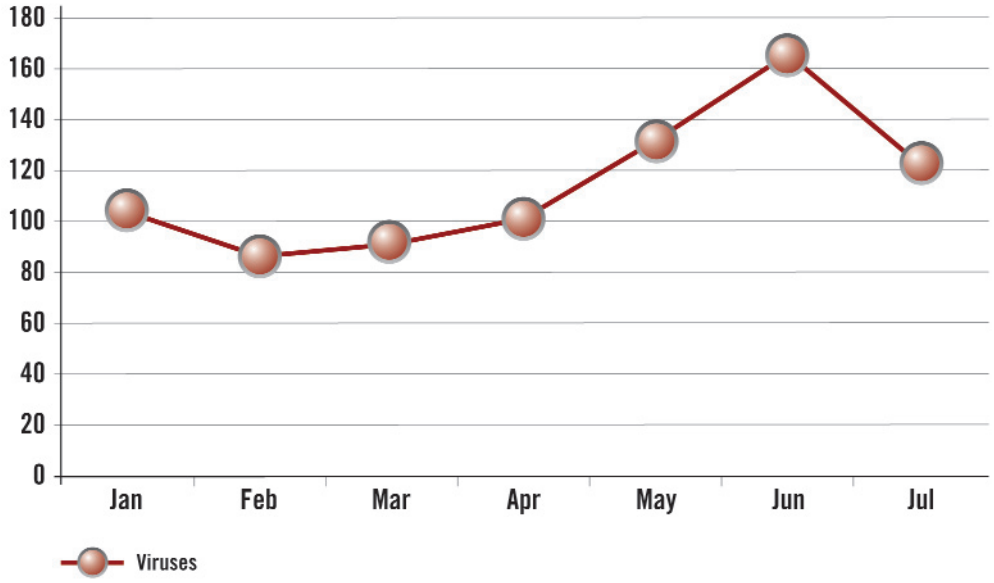
THE POSTINI WEB SECURITY SERVICE

Postini's global Web Security service provides an on-demand, secure gateway to corporations seeking to harden their enterprise against Web-based attacks. By using Postini's on-demand solutions, an enterprise can leverage:

- **Zero-hour Protection**
  The Postini Web Security service provides 24x7 dynamic and real-time protection by scanning traffic for malware and sensitive information before it

enters or leaves the network. Postini's threat detection solution goes beyond the deployment of patches and signatures updates. The service uses computer controlled heuristic scanning to analyze suspicious zero-day activity and deploy countermeasures in a matter of minutes or hours rather than days, as compared to traditional signature-based technologies that require the outbreak to appear before countermeasures can be developed.

New, Unique Viruses Detected and Blocked in 2007



Source: Postini

- **Best in Class URL Filtering**
  Postini Web Security service allows access to business-related Web content by tailoring an acceptable URL list to business requirements and blocks access to non work-related URLs. In doing so, the service reduces the risk of offensive and bandwidth-intensive content entering the network. By diminishing risk, the service helps reduce the probability of lawsuits and the cost of additional bandwidth.

- **High Performance**
  The Postini Platform is designed specifically for Web traffic, using highly parallelized processing for optimal throughput. Highly redundant provisioning ensures all customers are provisioned with a minimum of 100% head room on every server. All data is locally load balanced between two distributed data centers to minimize latency and maximize uptime.

Are you really protected with a desktop or gateway antivirus?

The chart to the left shows the number of new, unique viruses the Postini Web Security service detected and stopped BEFORE antivirus engines had signatures for these new malware attacks. Companies relying on desktop or gateway antivirus technology for protection would have experienced multiple infections - and remediation issues - before their signature databases could be updated.

- **Effortless Scalability**

  The Postini Web Security service is infinitely scalable so users can be added instantly at a fixed cost. Additional capacity planning is not required for corporate expansion or reduction, enabling you to roll-out the services across multiple international locations or branch offices with no lead time or additional capital expenditure, configuration or administration cost. Like all Postini services, Postini Web Security service has redundancy, availability and disaster recovery built-in, saving the resource and costs of planned or unplanned downtime.

- **A Low Total Cost of Ownership**

  The Postini Web Security service is an answer to IT managers' problem of providing high-quality solutions with a shrinking IT budget. Postini's on-demand solutions are designed to transparently integrate with existing network architecture, thus reducing implementation requirements. In doing so, the overall cost of ownership shrinks by not requiring additional software, hardware or manpower to deploy and maintain the solution.

- **A Key Component to Broader Communications Security**

  With Postini Communications Security and Compliance solutions, you can secure all electronic communications - email, instant messaging and the web – and manage communication policies from one central location.

CONTACT US

Silicon Valley
2400 Geng Road, Suite 201
Palo Alto, CA 94303
Tel 650.475.4500
Fax 650.475.1570

San Antonio
7550 West Interstate 10, Suite 400,
San Antonio, Texas 78229-5616
Tel 210.348.1000
Fax 210.348.1003

London
4, Grosvenor Gardens,
London SWIW ODH,UK
Tel 44(0)20 7730 3438
Fax 44(0)20 7730 3343

877.GoFrost
myfrost@frost.com
http://www.frost.com

Palo Alto

New York

San Antonio

Toronto

Buenos Aires

Sao Paulo

London

Oxford

Frankfurt

Paris

Israel

Beijing

Chennai

Kuala Lumpur

Mumbai

Shanghai

Singapore

Sydney

Tokyo

ABOUT FROST & SULLIVAN

Based in Palo Alto, California, Frost & Sullivan is a global leader in strategic growth consulting. This white paper is part of Frost & Sullivan's ongoing strategic research into the Information Technology industries. Frost & Sullivan regularly publishes strategic analyses of the major markets for products that encompass storage, management, and security of data. Frost & Sullivan also provides custom growth consulting to a variety of national and international companies.

The information presented in this publication is based on research and interviews conducted solely by Frost & Sullivan and therefore is subject to fluctuation. Frost & Sullivan takes no responsibility for any incorrect information supplied to us by manufacturers or end users.

For information regarding permission, write:
Frost & Sullivan
2400 Geng Rd., Suite 201
Palo Alto, CA 94303-3331, USA

WP37-0709