

Protecting Your Network Against the Growing Danger of Web Attacks

An Osterman Research White Paper

SPONSORED BY



MessageLabs[®]
Now part of Symantec



Osterman Research, Inc. • P.O. Box 1058 • Black Diamond, Washington 98010-1058
Phone: +1 253 630 5839 • Fax: +1 866 842 3274 • info@ostermanresearch.com • www.ostermanresearch.com

Why You Should Read This White Paper

After email, the World Wide Web is among the most important tools available to people who use a computer as they perform their job. It offers a ready source of current information, an infrastructure for developing various types of content, and a platform for communications and collaboration.

However, the Web is also fraught with risks, such as malware that can be downloaded to a network or an individual's computer by doing nothing more than simply visiting a Web site. Further, even Web sites that are legitimate for use in a business context can serve as a source of these threats – there are thousands of examples of otherwise valid Web pages and entire sites that have become a source of malware ranging from simple keystroke loggers to much more malicious content.

The problem of Web-borne threats is not theoretical: millions of users have been impacted and the threat is getting worse.

The problem of Web-borne threats is not theoretical: millions of users have been impacted and the threat is getting worse. Today, Web threats are more numerous and more virulent than those that are delivered in email, and it is easier to be infected by them. Further, blended threats in which links to malicious Web sites are delivered in email, instant messages or through social networking communications are becoming more popular, making the simple act of Web surfing a potentially devastating threat to corporate networks and security.

The problem is going to get worse for two reasons:

- Most Web pages and sites are not adequately protected from infection, such as SQL injection attacks or cross-site scripting, leaving them vulnerable to exploitation by malware authors.
- Defenses against Web-borne threats are not as extensive as those protecting organizations from threats delivered through email.
- When presented with a threat delivered through email or instant messaging, users generally have to do something, such as click on a link in a message – with Web-based threats, nothing more than visiting a Web page is required to become infected.

WHAT SHOULD YOU DO?

Clearly, every organization must do something to protect itself against these threats. Among the many things that can be done is to implement any of the growing number of Web security capabilities that are available. While on-premise solutions are available that will provide robust protection against Web threats, hosted solutions offer some unique advantages, including lower costs, more proactive threat protection, lower impacts on bandwidth and storage, and the ability to free IT staff for activities that might provide more value to an organization.

This white paper, sponsored by MessageLabs, now part of Symantec, discusses the nature of Web-borne threats, the options that are available to organizations to deal with them, and information on hosted Web security services.

The Need to Protect Against Web-Based Threats

THE WEB REPRESENTS A GROWING THREAT VECTOR

For the past several years, email has represented the most serious threat vector for organizations of all sizes – viruses, worms and other forms of malware have all been delivered via email for many years. However, Web-borne malware is now more common than malware that enters an organization through email as demonstrated by the following statistics from MessageLabs Intelligence Reports:

- Email-borne malware dropped from 0.85% of all email in 2007 to 0.70% in 2008.
- The number of Web sites that carry malware increased from 1,068 new sites discovered per day in January 2008 to 5,424 per day in October 2008, an increase of more than 400% in just nine months.
- In July 2008, 83.4% of all the Web-based malware intercepted was newly discovered as a result of an increased number of SQL injection attacks.

One of the fundamental problems with Web-based attacks is that literally hundreds of thousands of Web sites can serve as infection points – even legitimate Web sites can infect a network. For example, the Web sites of *Business Week*¹, the Miami Dolphins², Audi Taiwan³ and the United Nations⁴ have all been infected during the past few years, infecting visitors who do nothing more than view the content on these sites.

Further, new Web sites are created every day and search engines can make virtually countless numbers of Web sites available in real time that will not be pre-screened by many conventional Web-filtering solutions. For example, during the 24 hour-period ended March 9, 2009, more than 125,000 new domains came online⁵, representing the potential for well over one million new Web pages, any of which can be harboring an infection that can impact corporate networks and individual computers.

THERE ARE A VARIETY OF NEGATIVE IMPACTS

What can happen as a result of an infection that originates from simply visiting an infected Web page? The quite serious consequences include:

- Malware can be downloaded automatically that can intercept keystrokes or other sensitive content. The result can be loss of login credential and consequent use by hackers, loss of financial information or trade secrets, and otherwise compromised network security.
- Bandwidth and network performance can become strained as malware, bots and other malicious content uses bandwidth in the corporate network. The result can be poor network performance, slow email delivery, and slow Web access.
- Storage costs increase because of spyware downloads and other malicious content occupying taking space on the corporate network.

Further, mobile and remote users are making the problem worse because many of the endpoints, such as mobile devices or home computers that access corporate networks, are not adequately protected against Web-borne threats and so represent an ingress point for all sorts of malicious content.

What Can You Do About the Problem?

There are a variety of things that organizations can do to address the growing problem of Web-based threats, although some of the practices and procedures that organizations can implement will be more effective than others.

ESTABLISH POLICIES FOR EMPLOYEE USE OF THE WEB

One of the first and most important things that organizations should do to address the Web threat problem is establish formal and detailed policies for their employee's use of the Web. Many organizations do not have adequate Web-use policies, if they have them at all. Any employee-focused policy on use of the Web should address the types of Web sites that employees are allowed to visit and those that are not permissible. Obviously, gambling and pornographic sites will be banned in most organizations, although some organizations may also want to ban non-business sites, as well. Various studies over the years have found that employees spend inordinate amounts of time visiting non-business Web sites, particularly around the time of significant events like the Super Bowl, World Cup and the like.

Policies for appropriate use of the Web – no matter how specific they are, how well they are followed or how well they are enforced – cannot prevent most malware from entering a corporate network.

ESTABLISH WEB ANTI-VIRUS AND ANTI-SPYWARE PROTECTION

However, policies for appropriate use of the Web – no matter how specific they are, how well they are followed or how well they are enforced – cannot prevent most malware from entering a corporate network. As noted earlier, even legitimate, business-oriented Web sites have been subject to SQL injection attacks and other forms of infection, and so anti-virus and anti-spyware tools must be deployed throughout the network. Preferably, these capabilities will be deployed both at the server or gateway level and also at the end user level. Deploying these capabilities on individual desktop machines, laptops and mobile devices will provide the added benefit of protecting against threats that might enter via a USB storage device or from a CD-ROM that a user brings from home, for example.

BLOCK NON-BUSINESS-RELATED WEB SITES

Another option that should be considered is the deployment of URL filtering tools that will block access to non-approved Web sites. Many organizations have deployed these filters, albeit with varying levels of success. While URL filters can be useful, they can rarely keep up with the new threats that enter the Web on an hourly basis and for which no signature has been created in the tool. Further, URL filters can generate significant levels of false positives – blocking Web sites that appear to be suspicious but might have a legitimate business purpose.

FILTER CONTENT FOR UNWANTED FILE TYPES

Another capability that can be implemented in an effort to block Web-based threats is content filtering designed to block unwanted file types. Blocking file types based on their content can be useful in preventing some types of Web threats from entering a network, particularly files that are traditionally known to be associated with malware, such as .scr or .pif. These systems can also block file types that are generally not used in a legitimate business context, such as .mp3, .jpg or .mov files. In addition to preventing some Web

threats from entering a network, content filtering tools provide the added benefit of storage and bandwidth savings by blocking audio, video and other files that can consume large quantities of both.

USE A COMBINATION OF APPROACHES

No one solution will be the “best” approach to the problem of addressing Web threats. For example, a policy-only approach will simply not protect an organization from employees who forget the policy or choose to ignore it. Similarly, a systems-only approach without a clear, well-understood and well-enforced policy to support it could create confusion and anger among employees. Instead, organizations should use several different methods in a layered approach to ensure the highest level of protection.

A hosted solution can be very useful at blocking users from visiting non-business-related Web sites, thereby boosting user productivity and organizational compliance.

Does a Hosted Web Service Offer the Best Protection?

An alternative to the on-premise model is the use of a hosted Web security service. Among the benefits of the hosted service are:

- Highly proactive security against Web threats, particularly against the growing number of threats that can propagate very quickly.
- Efficacy at blocking users from visiting non-business-related Web sites, thereby boosting user productivity and organizational compliance.
- Ability to save bandwidth and storage by blocking large, bandwidth-intensive media files, such as .mp3s, audio files and image files. Because these files are blocked in the cloud, they cannot impact on-premise bandwidth or storage.
- Provision of the same level of granular controls as their on-premise counterparts, allowing individuals to have greater access privileges to certain types of Web content while preventing other users from accessing this content.
- Much better scalability than on-premise solutions can provide. For example, a dramatic increase in the amount of Web content scanned, or in the number of users and/or locations added to an on-premise Web-security solution often requires an increase in the number of appliances, servers and other infrastructure, or it requires architecting and deploying the solution to accommodate this increase when the system is initially deployed. A hosted solution, on the other hand, can scale very quickly with little more than a change of settings in a Web interface.
- Frees IT staff from the tasks associated with managing an in-house deployment.
- Lower and more predictable costs than is possible when using an on-premise solution. While the cost of on-premise can be less expensive for very large deployments, hosted solutions can be more cost effective, even for large numbers of users, when all of the lifecycle costs are taken into consideration.

Why MessageLabs Web Security Services?

MessageLabs leading Web Security Services for anti-spyware, web viruses and URL filtering operates at the Internet level, intercepting viruses, spyware and other web-borne threats before they get anywhere near your network or your remote workforce.

Global Infrastructure and Customer Data Reach

Equipment and servers inevitably break and staff members change. Supported by a global infrastructure, MessageLabs Web Services can provide your organization with mass redundancy and more complete business uptime so you can be more productive. All fourteen load balanced MessageLabs services data centers across four continents are monitored 24/7 by multiple Network Operations Centers to provide your network with superior protection. There is no hardware to configure; security updates and maintenance are managed centrally by MessageLabs, now part of Symantec.

In addition to MessageLabs services' robust infrastructure, your organization's network will also benefit from multiple layers of scanning with best of breed commercial scanners and patented Skeptic technology – a heuristics based engine that evolves as it scans email and web traffic in the cloud. With perimeter scanning, MessageLabs services observe global live threats as they happen and can flag any suspicious looking code for further analysis to block threats before they occur.

This further contributes to the MessageLabs services' continuously growing threat knowledge base accumulated from traffic of more than 21,000 clients (over 3 billion SMTP and 1 billion HTTP connections per day) – significantly more sites and more threats than appliance vendors who can only view threats captured in their "honey pots".

Skeptic Technology

The heart of MessageLabs services, Skeptic uses unique predictive technology to provide industry-leading protection against zero hour SMTP and HTTP threats. In continuous development since 1998, Skeptic learns from each traffic component it sees, updating and evolving ahead of every new threat, and constantly building on its already vast knowledge

A hosted Web security solution offers a number of advantages, including lower costs, easier maintenance and potentially better threat protection.

base. Its effectiveness increases with the volume and diversity of Internet traffic it sees. An industry first, MessageLabs services has introduced 'Converged Threat Analysis', taking recent threat and reputation information from one protocol, such as email, and applying that knowledge to another protocol, such as web traffic, providing an unparalleled level of knowledge and protection for MessageLabs services clients – that consistently sets new standards in the industry.

MESSAGELABS WEB SERVICES

Anti-spyware and anti-virus protection to ensure your business network remains free from malicious code designed to monitor and steal user information, degrade network performance or worse.

URL filtering to enable you to block access to unwanted websites, monitor and control Internet use and enforce acceptable Internet usage policies, keeping your business productive and compliant.

Summary

Web threats, such as keystroke loggers and other malware that is downloaded from infected Web sites have surpassed email as the primary threat vector with which most security-oriented decision makers must contend. The problem is worse than with email and will continue to become a more critical problem over time.

To protect against threats that are delivered via the Web, organizations should do a number of things, including develop policies focused on acceptable use of the Web and deploy capabilities that will block the URLs of malicious Web sites and filter content for various threats. They can deploy on-premise systems that offer the advantages of granular control and good threat protection, or they can opt for a hosted Web security model that can be more proactive in blocking real-time threats. A hosted Web security service offers a number of advantages, including lower costs, easier maintenance and potentially better threat protectio

¹ <http://www.internetnews.com/security/article.php/3771671/Hackers+Hit+BusinessWeek+With+Malware.htm>

² http://www.pcworld.com/article/128750/super_bowlrelated_web_sites_hacked.html

³ http://www.securityhome.eu/mailings/mailling_pdf.php?mid=272

⁴ <http://hackademix.net/2007/08/12/united-nations-vs-sql-injections/>

⁵ <http://www.domaintools.com/internet-statistics/>

© 2009 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

THIS DOCUMENT IS PROVIDED "AS IS". ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.