The Critical Need to Secure the Web in Your Company

An Osterman Research White Paper

Published February 2010

SPONSORED BY

Osterman Research, Inc. • P.O. Box 1058 • Black Diamond, Washington 98010-1058
Tel: +1 253 630 5839 • Fax: +1 253 458 0934 • info@ostermanresearch.com • www.ostermanresearch.com

Why You Should Read This White Paper

THE WEB AND WEB APPLICATIONS ARE USED HEAVILY

Web2.0 usage is on the rise. A July 2009 Osterman Research survey[1] published found that 27% of email users consider Twitter to be valuable or extremely valuable in helping them to get their work done; 13% consider Facebook to be this valuable. More than one-half of Twitter users believe it will become more important to them over time. A September 2009 Osterman Research survey[2] found that 21% of email users regularly use Twitter at work, 43% use LinkedIn and 24% use Facebook. Further, a May 2009 Osterman Research survey found that the typical user in smaller organizations (up to 1,000 employees) spend 25% of their day using the Web; users in larger organizations spend 19% of their day using the Web.

THE WEB IS A DANGEROUS PLACE

Any organization, regardless of its size or the industry that it serves, is vulnerable to a growing variety of sophisticated Web exploits. While many of these can enter an organization through the growing number of Web 2.0 applications that are in use, exploits can be introduced into a corporate network by doing nothing more than surfing the Web. Consider the following:

- One source estimates that a large organization of 40,000 computer users will view 48 million Web pages on a typical day and 0.17%, or 83,000, of those pages will be infected with malware[3], an average of more than two infected Web pages per user each day.

- An Osterman Research survey conducted in 2009 found that 55% of mid-sized and large organizations had been infiltrated by a Web exploit during the previous 12 months; a year earlier, that figure was only 39%.

- Smaller organizations are particularly vulnerable to Web exploits because they often lack the IT staff and technical expertise necessary to detect and remediate these threats before they can do real damage. Examples of organizations that have been impacted include an auto parts supplier in Georgia that lost $75,000 to a banking Trojan and a county government in Kentucky that lost more than $400,000 to a similar exploit.

- Webroot[4] has found that 85% of malware is distributed through the Web; Blue Coat has pegged the figure at 65%[5].

- The Anti Phishing Working Group (APWG) received a record 40,621 phishing reports and 56,362 unique phishing sites detected in August 2009. The third quarter of 2009 saw more than 340 brands attacked – the previous high was 310 brands.

---

[1] *Results of a Survey on Twitter Usage*, Osterman Research, Inc.
[2] *Results of an End User Survey on the Use of Communications Tools*, Osterman Research, Inc.
[3] Infected "Legitimate" Site A Growing Threat, *Processor*, October 23, 2009
[4] Source: Webroot Software, Inc. survey
[5] Source: Blue Coat Security Labs

THE KEY TAKEAWAY

The Web and Web 2.0 applications, while very useful, also present a significant risk to any organization. The development of increasingly sophisticated exploits by hackers and other cybercriminals, coupled with the deployment of less robust Web-focused defenses compared to defenses for email, mean that Web exploits will grow in number and severity for the foreseeable future.

ABOUT THIS WHITE PAPER

This white paper discusses the key issues surrounding Web security and the need for organizations of all sizes to implement robust Web security processes and technologies – namely, a secure Web gateway. This document was sponsored by a leading provider of Web security solutions, Webroot Software. Information on the company is provided at the end of this white paper.

The Web is a Dangerous Place

MOST ORGANIZATIONS HAVE EXPERIENCED WEB MALWARE

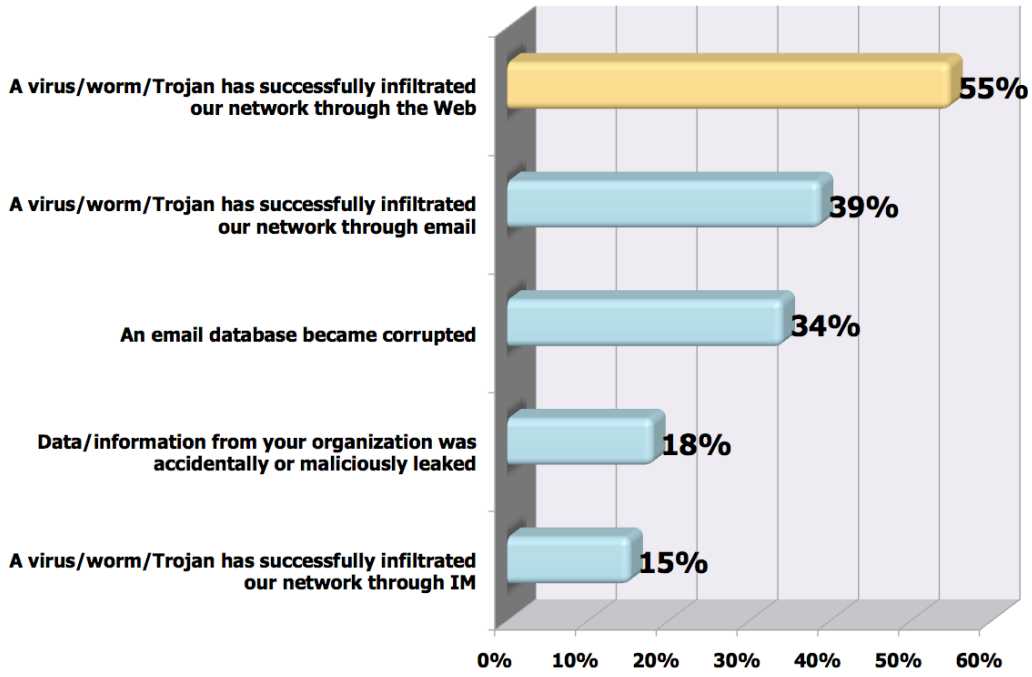
Consider the following:

- For most of August 2009, Trend Micro found roughly 250 bad Web sites per one million queries; for most of June 2009, this figure was between 100 and 150[6].
- In April 2008, ScanSafe found that a single wave of SQL injection attacks resulted in the compromise of 524,000 healthcare-related Web pages, 185,000 travel-related pages, 35,000 government pages, 25,000 education-related pages and 17,000 financial services-related pages[7].
- ScanSafe found a 300% volume ratio increase in Web-based malware from January through December 2008[8].
- In November 2009, Symantec MessageLabs found a mean of 241 new spyware-laden Web sites and 2,749 sites with Web-based viruses per day[9].

There has been an enormous increase in malicious Web-borne content, including user generated content posted to traditionally good Web sites, email messages that contain links to dangerous or newly compromised Web sites, attachments that are little more than stage-one downloaders of other malicious code from the Web, malware that installs and opens a communication channel to the attacking source, and other exploits. Typically, these malware sites succeed in creating more zombie bots that keep feeding the vicious cycle of malware. Illustrating the scope of the problem is the following figure from a study that Osterman Research conducted in 2009.

[6] http://us.trendmicro.com/us/trendwatch/current-threat-activity/threat-level/index.html
[7] ScanSafe *Annual Global Threat Report* for 2008
[8] *ScanSafe Annual Global Threat Report*, March 2009
[9] *MessageLabs Intelligence* report, November 2009

Infiltrations and Problems That Have Occurred Between 2008 and 2009



Spam and Web-based threats are being used together increasingly in coordinated, blended attacks. For example, there are millions of unique URLs on hundreds of thousands of Web sites that automatically install malware on visitors' machines – spam often is used to drive traffic to these sites simply for the purpose of installing malware for later use.

Further, Web 2.0 Web sites that include dynamic content, such as complex mashups that change continually, make it difficult to accurately determine whether a particular site is safe or risky at any point in time. This makes the need for real-time assessments and reputation more critical than ever before.

WHERE DO THE PROBLEMS COME FROM?

There are a large number of sources from which Web-based threats come:

- Users install malware or compromised code on their systems, mostly often inadvertently. This occurs when they install ActiveX controls, download codecs or various applications that are intended address some need (they perceive have some value), or respond to scareware and fake anti-virus software.

- Another source of Web threats is the growing use of Web-enabled smartphones. Osterman Research has found that few organizations require any sort of malware protection on these devices, making networks vulnerable to malware that enters through a mobile device. Compounding the problem is the fact that mobile devices are widely used (59% of corporate email users also have an employer-provided

mobile device) and 13% of email users employ their mobile device as their primary client for checking work-related email from home[10].

- Off-network users, such as those working from home, are another source of Web-based threats. An unprotected user using a corporate asset, such as Outlook Web Access that is not accessed via a VPN, or a laptop computer that becomes infected and later is connected to the corporate network, can constitute a serious threat.

- The Secure Enterprise 2.0 forum[11] found that hackers exploit a large number of Web site and Web 2.0 vulnerabilities, including SQL injection as the most common exploit (21% of vulnerabilities), insufficient authentication (18%), content spoofing (11%) and cross-site scripting (11%), among other exploits. WhiteHat Security, in a report published in December 2008, found that 65% of Web sites were vulnerable to cross-site scripting attacks[12].

  For example, Yahoo! Hotjobs came under a cross-site scripting attack in October 2008 – attackers obfuscated JavaScript in order to steal a victim's session cookies that were used across Yahoo!'s sites. By stealing the cookies, the attackers were able to gain control over every service accessible to the user within Yahoo!, including Yahoo! Mail. (Yahoo! fixed the problem on October 28, 2008). Similar attacks have also been used to attack Twitter, to spoof offers on eBay, and to launch attacks on the Web sites of anti-virus vendors.

- Compromised search engine queries are another method for criminals to distribute malware. This form of attack relies on users making typographical errors when typing search queries, resulting in their being presented with malware-laden sites.

- Search engine poisoning occurs when hackers target Web sites that rank very high in search results in an attempt to target a greater proportion of users.

- Blended threats, as noted earlier, are an increasingly common threat vector in which spam contains a link to a malicious Web site. Users will often click on a link in a spam message and get infected from the malware-laden Web site that opens in their browser.

- Related to the blended threat is a "drive-by" download that occurs when a user visits a Web site and has malware automatically downloaded to his or her computer. In some cases, a user will visit a Web site and see a popup window – upon clicking the "OK" button in the popup, a Java applet, an ActiveX control, etc. will be installed on the user's computer without their consent.

- Direct hacker attacks can include a variety of exploits, including hackers attacking a known vulnerability in a Web browser, or exploiting an older version of a browser or ActiveX control.

[10] *Results of an End User Survey on the Use of Communication Tools*, Osterman Research, Inc., September 2009
[11] *Web 2.0 Hacking Incidents and Trends, 2009 Q1*
[12] *WhiteHat Website Security Statistic Report*, Spring 2009, 7th Edition

- With Cross Site Request Forgery (CSRF) attacks, innocent-looking Web sites generate requests to different sites. CSRF attacks have exploited vulnerabilities in Twitter, enabling site owners to acquire the Twitter profiles of their visitors.

- Insufficient authentication controls will sometimes enable cyber-criminals to crack administrative accounts in order to gain access to sensitive information.

- As Web 2.0 applications often leverage XML, XPath, JavaScript and JSON, those applications are frequently vulnerable to injection attacks using these environments.

GROWING USE OF SOCIAL NETWORKING AND WEB 2.0 APPLICATIONS

While email continues to provide an inroad for viruses and Trojans, increasingly organizations are finding the Web – and Web 2.0 applications in particular – to be a major source of malware infiltration. Many social networking and Web 2.0 applications are growing rapidly in popularity. For example in December 2009[13]:

- Facebook had 132.1 million unique visitors, up 121% from the previous year.
- Twitter had 22.8 million unique visitors, up 414% from the previous year.
- LinkedIn had 14.9 million unique visitors, up 59% from the previous year.
- Skype had 3.8 million unique visitors, up 64% from the previous year.

A key part of the problem is that many organizations allow the use of various tools that IT does not consider to be legitimate. For example, in the table below taken from an Osterman Research survey[14] conducted in 2009, it was determined that IT departments are allowing use of applications that they do not consider to have legitimate business value. The disconnect between IT and the business is most noticeable around Facebook and Twitter. While one-half of organizations allow Facebook, only 28% of respondents thought the application to be legitimate. The same goes for Twitter, which was allowed by 49% of the organizations and yet viewed as non-legitimate by 28% of respondents.

Applications That Organizations Consider to be Legitimate and Which They Allow

Application	Consider to be Legitimate	Allow to be Used
LinkedIn	61%	70%
Consumer-grade Webmail	47%	79%
Skype	35%	39%
Facebook	28%	50%
Twitter	28%	49%
MySpace	20%	39%

The concern over the use of Web 2.0 applications, and the Web in general, often focuses on a variety of things: the potential for information leakage, the growing

[13] Source: Compete.com
[14] *Email, Web and IM Security Market Trends, 2009-2012*, Osterman Research, Inc.

variety of security threats and the operational cost of remediating infected endpoints among them.

However, both Facebook and Twitter, along with many other Web 2.0 tools, offer potential value for organizations and have a deep foothold into businesses today. Yet, IT and compliance still remains suspect of the technologies. Perhaps this is related to a deeper understanding of the vulnerabilities that these applications expose. Regardless, as marketing departments embrace blogging, micro-blogging, wiki's, Web 2.0 applications and other capabilities, organizations must find a way to close the gap around these applications. Either by providing corporate-sanctioned versions of these applications, as was done with file transfer; block these applications if they really do pose a threat to the enterprise; or adopt the applications with appropriate security controls as part of a broader IT solution set.

LEGITIMATE WEB SITES ARE ALSO A PROBLEM

The problems associated with Web exploits are by no means limited to the use of consumer-oriented Web tools; Web 2.0 applications that IT might find objectionable; or gambling, adult, shopping or other sites that are unlikely to have business value. On the contrary, a large number of legitimate Web sites with real business utility have been the source of malware. A report published in late 2009 found that 5.8 million individual Web pages locate on 640,000 Web sites were hosting some sort of malware designed to infect their visitors[15]. For example:

- In late 2009, the Fox Sports Web site had malicious code injected into a customized error page from two separate infections.

- The RockYou Web site was hacked in late 2009 via a SQL injection flaw and more than 32 million records were exposed, including a list of customer passwords stored in plain text.

- Also in late 2009, the Intel Corporation Web site was the victim of a SQL injection attack that allowed personal information on the site to be exposed.

- Guardian Jobs, based in the United Kingdom, was hacked in late 2009 and an unknown number of customer records were exposed.

- Paul McCartney's Web site was the victim of the LuckySploit toolkit in early 2009, infecting visitors' computers with a rootkit.

- The Web site of CBS was infected by an iFrame attack in late 2008.

- In mid-2008, the Web site of Kaspersky in Malaysia was hacked using a SQL injection attack.

- The Wal-Mart Web site was the victim of a SQL injection attack in mid-2008. The attack resulted in Flash files on the site infecting visitors with malware.

[15] *CyberInsecure.com*, October 28, 2009

- Also in mid-2008, the Nature.com Web site was infected with a SQL injection attack.

- In early 2008, the shopping site for Major League Soccer (MLSgear.com) was hacked and customer financial data was exposed.

- Many other legitimate Web sites have also fallen victim to various types of exploits, including those operated by the US International Trade Commission, *Business Week*, *USA Today*, Target, the US Forest Service, Audi Taiwan, ABC News, CheckFree, Britain's National Health Service, the *New York Times* and the Virgin Islands Housing Finance Authority.

- In early 2007, an iFrame/redirect attack on the Miami Dolphins Web site installed malware from a Chinese server onto visitors' PCs.

The Fundamental Problem

USERS NEED TO ACCESS THE WEB AND WEB 2.0 APPS

Organizations have long struggled with how they should – or should not – police the use of the Internet and, more specifically, the Web and Web 2.0 tools. The emergence of social media applications and services makes that question more relevant and more difficult. Given the range of security threats that can be launched from social media sites, organizations need to be extraordinarily careful about their employees' use of those sites in a work-related context.

The problem is one that absolutely must be solved. The Web and the growing variety of Web 2.0 applications make employees more productive and efficient. Further, these capabilities support the greater concept of mobility – allowing employees to work from home or on the road with the same capabilities they would have in the office. Mobility in its larger context will become increasingly important as organizations look to drive down the cost of real estate, taxes and power by operating with the same number of employees, but with less office space.

WHY DEPLOY A WEB MANAGEMENT SOLUTION?

As shown in the following table, the most important reasons that decision makers cite for deploying a Web management solution are to block sites that contain malware, adware or spyware; and to block new Web threats.

Importance of Various Reasons for Deploying a Web Management Solution
% Responding Important or Extremely Important

Reason	%
To block adware / spyware / malicious sites	88%
To block new Web threats	83%
To block unwanted content like porn or gambling	77%
To block unwanted downloads	76%
To block peer-to-peer file sharing (P2P)	68%
For caching and Internet bandwidth optimization	57%
To log and report on user Web surfing behavior	48%
To minimize surfing for personal reasons	44%
To remove annoying ads from useful Websites	39%
To block personal Webmail	32%
To enforce a time limit for Internet access to particular category of Web sites	31%

Some companies will choose to block users from accessing the Internet for personal use as the US Defense Department did in 2007 when it blocked access to 13 file- and video-sharing sites. Others will choose to monitor user access to the Internet with various types of tools.

Osterman Research believes, however, that before organizations resort to those measures, a very clear Internet usage policy needs to be formulated, as discussed later in this report. The policy should outline acceptable practices, identifying good and bad uses of the Internet, the rationale for classifying them as such, and the technology in place.

WHAT COULD GO WRONG?

There are a variety of problems that can result from the growing number of Web exploits, malware and other threats that exist on the Web and in Web 2.0 applications:

- **Scareware**
  A user that visits an infected Web site may be presented with a popup window that informs him that his computer is infected with a virus. If he clicks on the link, he can inadvertently download an anti-virus simulator that reports a large number of malware infections and offers "anti-virus software" for a one-time fee. Purchasing this software results not only in a direct financial loss, but also in the provision of a valid credit card number to a cybercriminal.

- **Keystroke loggers**
  A keystroke logger can be delivered either through a drive-by attack or in a spam message. If a victim's computer becomes infected, all keystrokes that she makes before the threat is identified and remediated will be sent to a cybercriminal. For example, in an alert sent to the Financial Services Information Sharing and Analysis Center, one such scam was identified that targeted key individuals in smaller organizations and made wire transfers from corporate accounts in increments of less than $10,000. "Mules" based in the United States then set up bank accounts to

receive these funds from which they were wired them to their primarily Eastern European counterparts. Victims of this attack included Texas-based Unique Industrial Products Company that lost $1.2 million, Western Beaver School District in Pennsylvania that lost $700,000 and an electronics testing company in Louisiana, JM Test, that lost about $100,000[16].

The growing variety of keystroke loggers, password-stealing Trojans and other threats means that corporate data is increasingly at risk. Data theft can include sensitive content like usernames and passwords, but also financial data, customer data, trade secrets and other types of confidential information. The increasing end goals of stealing information (personal and corporate), hijacking systems for a wide range of purposes and launching additional malicious attacks all have serious business implications, in addition to the more traditional (but still real) impacts to bandwidth, infrastructure and other costs.

- **Violation of statutes and compliance requirements**
  By not adequately monitoring and managing Web-based threats, organizations can run afoul of a wide variety of statutes that require data to be protected and retained. However, one study found that decision makers in one in five organizations do not know which compliance laws apply to their organization[17]. A small sampling of these statutes – but by no means an exhaustive list – include the following:

  - The UK Data Protection Act imposes requirements on businesses operating in the United Kingdom to protect the security of the personal information it holds.

  - Japan's Personal Data Protection Law is designed to protect consumers' and employees' personal information. It includes provisions for ensuring the security and disclosure of databases that contain this information, among other provisions.

  - The Gramm-Leach-Bliley Act (GLBA) requires financial institutions that hold personal information to transmit and store this information in such a way that its integrity is not compromised. GLBA requires financial institutions to comply with a variety of Securities and Exchange Commission and NASD rules. A keystroke logger or cross-site scripting attack, for example, that permitted sensitive financial data to be exposed to a third party could potentially violate GLBA.

  - The Payment Card Industry Data Security Standard (PCI DSS) encompasses a set of requirements for protecting the security of consumers' and others' payment account information. It includes provisions for building and maintaining a secure network, encrypting cardholder data when it is sent over public networks and assigning unique IDs to each individual that has access to cardholder information.

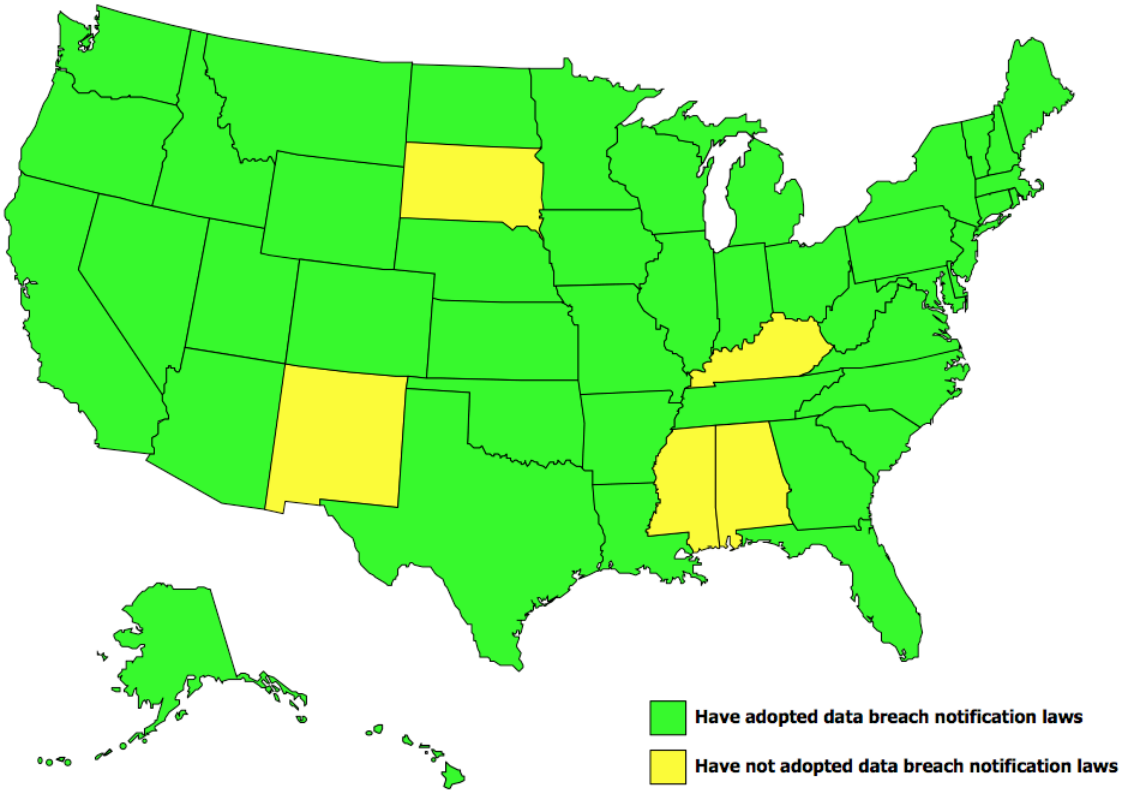
[16] The New Trojan War - Spike In Dangerous and Damaging Cyber Attacks against Small Businesses, *Think Security First*, September 14, 2009
[17] Source: Webroot Software, Inc.

- The Personal Information Protection and Electronic Documents Act (PIPEDA) is a Canadian privacy law that applies to all companies operating in Canada. Like many other privacy laws, it requires that personal information be stored and transmitted securely.

- California's SB1386 (the Database Security Breach Notification Act) is a far reaching law that requires any holder of personal information about a California resident to notify each resident whose information may have been compromised in some way.

- Since California passed this groundbreaking data breach notification law, most other US states have passed similar laws, as shown in the following figures[18]. These laws require organizations to notify customers and others for whom sensitive data is held if their data is exposed to an unauthorized party – an expensive proposition, as discussed later in this white paper.

Status of Data Breach Notification Laws in the United States
(as of December 2009)



Data Source: National Conference of State Legislatures

[18] http://is.gd/77jni

It is important to note that the regulations identified above represent only a limited set of currently applicable statutes. Further, it is important to view regulations at a variety of levels: geographically (state/provincial, Federal and global) and by industry sector. For example, some industries, such as some sectors of the financial services industry like broker-dealers, hedge fund managers and investment advisors, have specific requirements to which they must adhere. Some regulations, however, are cross industry and apply more generally, such as California's SB1386.

- **Other problems**
  There are a variety of other problems that can occur from malware and other threats delivered via the Web and Web 2.0 applications including:

  - Web sites being taken down for as long as necessary to patch the code in order to eliminate an exploit.

  - Service outages, which is a particularly serious problem for organizations that rely on the Web for cloud-based services like email, collaboration, CRM and the like.

  - Data leakage and lack of compliance with monitoring and archiving requirements when employees use personal Webmail systems to send corporate data.

  - The exposure of FTP and other login credentials to attackers and cybercriminals.

  - The download of malware that can turn corporate and home-based computers into zombies that can be used as part of a bot network.

  - Users downloading illegal content, such as copyrighted works or pornography using corporate assets. For example, a study published by ScanSafe found that the number of employees who had attempted to download MP3 files and illegally obtained software has recently increased dramatically[19].

THE COST OF COMPROMISE

Just what are the costs of Web exploits? That is not an easy question to answer, in part because there are a variety of intangible costs that are difficult, if not impossible, to quantify. Consider the following examples:

- At a minimum, any sort of Web exploit will require IT staff to address the issue as soon as possible after the problem is discovered. This can lead to IT staff working on weekends, the delay of various projects, rebuilding desktops, and other costs that may be difficult to estimate.

- However, as noted in one of the examples above, malware can cause easily identifiable losses, such as the loss of hundreds of thousands or millions of dollars enabled by keystroke loggers that will send login credentials to a malicious individual or organization.

[19] *Illegal internet downloads at work skyrocket*, IT Pro, January 13, 2010

- The Ponemon Institute has determined that the cost of a data breach in the United States was $202 per record breached in fiscal year 2008, up slightly from $197 during the previous year and up 46% from 2005[20]. The most significant component of this cost is lost business, accounting for 69% of the total cost of a breach.

- Malware that causes the loss of customer records, such as in the RockYou Web site hack noted above, can have widely varying costs. For example, some customers who learn about the exploit may decide not to do business with a company whose Web infrastructure has been victimized, leading to lost future revenue. The company may have to provide some remediation to its customers, such as offering credit reporting services for a year or more to let customers know if their records have been used for identity theft or some other purpose. Add to that the loss of reputation that may discourage some prospective customer from doing business with a victim of a Web exploit.

- At a minimum, most or all customers whose records have been breached will have to be notified at cost of at least several dollars per letter sent. The Ponemon study found that the cost of notification in 2008 was $18 per record.

In some ways, tools and technologies that are designed to protect against Web exploits should be economically justified in much the same way that insurance policies are justified. For example, an organization will spend tens of thousands of dollars annually on various types of insurance coverage in order to prevent losses that are far greater than the cost of the insurance itself. In the same way, avoiding even a single major breach through the use of the right Web security solution can prevent losses that are an order of magnitude or more greater than the cost of the solution itself.

Important Considerations in Solving the Problem

ORGANIZATIONS MUST ESTABLISH DETAILED POLICIES

First and foremost, organizations seeking to protect their users, data and networks from Web-based threats must establish policies about acceptable use of all of their online tools: email, instant messaging, Web 2.0 applications, collaboration tools, and the Web itself. Successfully addressing the problems associated with the Web must start with an acknowledgement of the threat landscape and corresponding policies about how tools will be used before technologies are deployed to address the problems.

Further, there must be buy-in across the organization in order for policies to be effective. For example, a blanket prohibition by IT on the use of Twitter or Facebook may seriously impact a marketing department's management or compliance effectiveness at building the corporate brand, or not allowing the use of unauthorized file transfer tools may prevent users from sending large files to prospects or customers in a timely manner.

[20] *Fourth Annual US Cost of Data Breach* study

URL FILTERING IS USEFUL, BUT ITS EFFECTIVENESS IS LIMITED

URL filtering can be an effective technique to help an organization reduce its exposure to Web-based threats. For example, using URL filtering can minimize employee access to obviously dangerous Web sites that have no legitimate business value, such as those focused on gambling, adult entertainment, shopping sites and other largely consumer-focused content.

URL filtering can also prevent employees from sending corporate content via personal Webmail accounts. For example, many employees will send work-related files using a personal Webmail account if their corporate email system is down or if they need to send a large file that exceeds a file-size limit. This can lead to a variety of problems, including providing an entry point for malware and bypassing corporate archiving systems.

However, URL filtering is limited in its ability to protect against Web-based malware and other exploits. Databases of inappropriate or suspect sites are continually out-of-date, resulting in potential access to malware-laden sites that are not in the database, or false positives – an inability to access a legitimate site that is mistakenly identified as off-limits. URL filtering does not provide a real-time defense capability, since URL databases are updated only periodically. Many Web sites are mashups that present content from a variety of sources – a single component on an otherwise safe site can expose visitors to malware. Further, URL filtering is largely incapable of protecting against exploits that may come through Web 2.0 applications or via short URLs. Most Web 2.0 applications circumvent URL filtering technology through a variety of means, from HTTP tunneling to port hopping. Equally, Web 2.0 sites such as Facebook, contain tens of thousands of applets that do not use the HTTP protocol and avoid Web filtering controls.

EMPLOYEE DESKTOPS AND LAPTOPS CAN BE LOCKED DOWN, BUT THIS IS NOT EFFECTIVE EITHER

Osterman Research surveys have found that a large proportion of organizations lock down employees' computers, preventing access to various applications, denying them the ability to install unauthorized applications, not allowing them to have administrator rights, or preventing them from changing firewall settings.

The upside of locking down employees' computers is that it can prevent behavior that could allow malware to enter an organization. The downside is that it can lead to poor employee morale from individuals who feel they are being overly controlled, and it can lead to a loss of productivity by not allowing employees the freedom to be innovative.

ORGANIZATIONS SHOULD DEPLOY A SECURE WEB GATEWAY

Organizations should deploy a secure Web gateway (SWG) to protect against Web-based threats of all kinds. Any such gateway should take a layered approach and provide a variety of capabilities. A layered strategy is key to successfully detecting Web-based threats, since conventional Web gateways can be defeated by custom encryption wrappers and hackers' obfuscation techniques; and because client-side, standalone solutions often provide only a limited defense in and of themselves. Ideally, these layers will include:

- **Real-time capabilities**
  Any SWG must have real-time security capabilities that will determine if requests from users and applications comply with corporate security policies. This is a critical element given the large and growing number of zero hour threats that can infect Web sites and Web 2.0 applications.

- **Cloud-based threat intelligence**
  Cloud-based intelligence, such as reputation services, is a key element of a layered defense strategy. Because a cloud-based network of threat detection capabilities can offer a view into a dramatically larger threat landscape, the likelihood of detecting and remediating exploits, malware, etc. is far higher than when using conventional techniques, such as URL filtering alone.

- **Local content analysis**
  That said, local content analysis is also an important component of a layered defense strategy in an SWG. By detecting threats locally, organizations can protect against them, while at the same time feeding this information back into the community of threat detection capabilities discussed in the next point.

- **Feedback loops**
  Organizations should use a community-focused capability that permits Web pages and Web 2.0 tools to be monitored and tested continually as users in the network access them. The results can then be used to update a cloud-based ecosystem so that other users can take advantage of the recently tested Web sites. This allows tens of millions of Web pages to be monitored on a daily basis, allowing faster and more thorough detection of new exploits than conventional approaches.

- **Granular policy management**
  Organizations must enable the Web and Web 2.0 technologies in order to realize productivity gains for their employees, but at the same time they need to protect their users from the myriad threats that can be delivered through these capabilities. This requires that granular policy management be a component of any SWG so that users with specific requirements can be accommodated.

- **Monitoring and reporting**
  The ability to monitor what users are accessing on the Web and to report on this behavior is an important capability that can provide insight in three ways. First, it allows decision makers to understand how their employees are using the Web and Web 2.0 tools. Second, it allows these decision makers to adjust corporate policies in order to offer greater protection against threats and/or to make better use of the Web and Web-based tools. Third, when employees know they are being monitored they are more likely to reduce dangerous or inappropriate behavior that could lead to malware infections.

- **Integration with messaging security**
  A key part of the layered defense strategy for an SWG is integration with messaging security capabilities. For example, by integrating messaging security and the SWG,

organizations can provide a better defense against blended threats by stopping them in email before they reach end users.

- **Support for mobile users**
  Because of the increasing use of Web-enabled smartphones, being able to protect against Web-based threats that can come from Twitter, Facebook, other Web 2.0 applications, or simple Web browsing is becoming increasingly important. A key part of any SWG is the ability to integrate with mobile capabilities, or at least have this on the product roadmap.

- **Application controls**
  The use of application controls is essential to ensure that Web 2.0 applications like Skype, Twitter, peer-to-peer file-sharing software, streaming media and the like cannot be used in violation of corporate policies or best practices. These application controls should be sufficiently granular so that individual users or groups can be given access to specific applications while other users are blocked from accessing them.

DELIVERY MODELS

There are a variety of ways in which messaging and Web security capabilities can be managed, including:

- **Gateway-Based Systems**
  Gateway security stops threats at the earliest possible point in the on-premise infrastructure and is a best practice for organizations that manage on-premise defenses.

- **Server-Based Systems**
  On-premise solutions deployed at the server level, where most data often resides, resolve many of the problems associated with client-side systems by allowing easier deployment and management capabilities, as well as the ability to more easily enforce corporate policies and changes through a centralized management interface.

- **Client-Based Systems**
  Client-based systems, such as URL filtering tools, anti-virus tools, spyware blockers and the like provide useful capabilities and can be effective at preventing a variety of threats – client-side anti-virus tools, for example, are an important best practice for any organization.

  Client-side capabilities can be relatively inexpensive and are often provided as part of desktop protection suites that include anti-virus, anti-spam and other capabilities. While client-side systems are effective in smaller organizations, they often do not scale well. They are time-consuming to install and update for large numbers of users and can be quite expensive to deploy in larger organizations. Particularly for larger organizations, centralized management and deployment capabilities are essential to cost-effectively install, update and enforce corporate policies using client-based systems.

- **SaaS and Hosted Services**
  SaaS and hosted services are increasing in popularity and offer another option for organizations to implement a variety of threat-protection capabilities. The primary advantages of this model are that no investments in infrastructure are required, up-front costs are minimal, ongoing costs are predictable, and all management and upgrades of the system are provided by the SaaS or hosted service.

  The disadvantage of SaaS or hosted services, particularly for web traffic, is proxying all traffic to the host and addressing latency issues. Their costs can be higher than for on-premise systems in some situations, although they will not necessarily be more expensive. For example, SaaS vendors merely rent space on a server, providing a very inexpensive method for accessing software and infrastructure technologies. Although organizations may pay more to a SaaS or hosted security vendor than they would for an on-site solution, the value of the hosted infrastructure and administration provided by the third party vendor can provide a lower Total Cost of Ownership.

- **Managed Services**
  Managed services are similar in concept to hosted services, but a third party – either with staff on-site or via a remote service – manages the on-premise infrastructure, installs upgrades, updates signature files and the like. Costs can vary widely for managed services depending on the size of the organization, whether third-party management personnel are located on-premise or in the third party's data center, and other factors.

- **Hybrid Offerings**
  A newer approach that is increasingly offered by vendors is to combine on-premise infrastructure with hosted or cloud based services. For example, a vendor may provide a malware-filtering appliance on-site, but couple this with a hosted filtering service that acts as a sort of pre-filter; or they may rely on a hosted anti-virus service and desktop anti-virus tools.

  The fundamental advantage of this approach is that the on-premise infrastructure is protected from spikes and overall increases in the volume of malicious traffic over time, thereby preserving the on-premise investment and maintaining acceptable performance of their messaging and Web infrastructure.

Enterprises still prefer in-house over hosted solutions, although this is changing over time. Hosted solutions tend to do better in small- to medium-sized business with less developed IT staff and fewer resources. These organizations often need external expertise and can benefit from the CAPEX and OPEX savings of hosted solutions. Similarly, appliances also tend to offer the SMB the convenience of an integrated solution.

Larger organizations tend to have well-staffed IT departments, and so gain less from the benefits of appliances, unless those appliances are for remote or branch locations where there may be a lack of local expertise. What's more, large organizations tend to have extra server hardware enabling them to realize the CAPEX cost savings afforded by

service providers. Evidence to this point is the popularity of in-house managed server software. Given the size of their requirements, large organizations can also justify internal personnel and so may not be realize the OPEX savings of hosted services.

Having said that, while large organizations may not have been the ideal play for hosted service providers in the past, the market is definitely shifting. As IT continues to downsize and outsource, hosted service providers are gaining traction in larger organizations precisely because of the savings they can offer. This is particularly true when the buy discussion is conducted at the CIO level.

BALANCING COMPLEXITY, UTILITY AND EFFECTIVENESS IN A WEB SECURITY SOLUTION

When all is said and done, it is critical that any SWG a) be as effective as possible in identifying and remediating Web-based threats, b) impede (as little as possible) users' appropriate use of the Web and Web 2.0, and c) impose as little burden on IT as possible for the administration of the system. Being able to balance all of these is central to the task of protecting against Web-based threats. Further, understanding of the actual payloads and remediation is still a critical element of both gateway and endpoint protection, yet not all vendors possess the same level of expertise in this regard.

Summary

Web exploits are a serious issue for any organization and they are getting worse. Growing use of the Web and Web 2.0 applications, coupled with increasing corporate reliance on cloud-based systems that employees access via Web browsers, are making organizations more vulnerable to a variety of Web-focused exploits and attacks.

The cost of doing nothing to address the issue is enormous. An organization's losses from even a single Web exploit can be in the millions of dollars in hard costs, not to mention the ongoing costs of a damaged corporate reputation, lost business from existing customers that switch to a competitor, lost business from prospective customers that will no longer consider a firm that has been victimized, and loss of competitive advantage of not using Web 2.0 tools securely.

As a result, organizations of all sizes should deploy a secure Web gateway that will protect against Web exploits in real time, will use both cloud-based and local content analysis techniques, provide granular policy management and application controls, integrate with messaging security capabilities, and provide support to users who access the Web and Web-based applications on mobile devices.

Sponsor of This White Paper

Webroot Software
2560 55th Street
Boulder, CO 80301
+1 866 612 4268
www.webroot.com

Webroot provides industry-leading Internet security solutions for consumers, enterprises and small and medium businesses worldwide. Webroot products consistently receive top review ratings by respected third parties and have been adopted by millions globally. With a wide range of online security products for home and office, Webroot protects corporate networks and allows consumers to download music, store digital files, bank, shop, surf and search – safely.

Founded in 1997, the company provides best-of-breed security solutions that protect personal information and corporate assets from online and internal threats. Based in Boulder, Colo., the company is privately held and backed by some of the industry's leading venture capital firms, including Technology Crossover Ventures, Accel Partners and Mayfield. Webroot currently has more than 300 employees worldwide.