

The Failure of Web Filtering

A ScanSafe White Paper May 2008

TABLE OF CONTENTS

	Page
TABLE OF CONTENTS	2
2.0 YESTERDAYS PROBLEM	3
3.0 THE HISTORICAL APPROACH	3
4.0 WHEN GOOD SITES GO BAD	4
5.0 THE NEW GENERATION OF WEB THREATS	5
6.0 THE PROLIFERATION OF SECURITY PRODUCTS	6
7.0 REAL TIME SCANNING	7
7.1 SIGNATURE-BASED DETECTION	7
7.2 HEURISTICS	7
7.3 CODE ANALYSIS	7
7.4 CODE REPUTATION	7
7.5 URL REPUTATION	7
7.6 TRAFFIC BEHAVIORAL ANALYSIS	8
8.0 SCANSAFE SAAS WEB SECURITY	8
9.0 THE FURTHER BENEFITS OF SAAS WEB SECURITY	9
10.0 SUMMARY AND CONCLUSION	10
11.0 ABOUT SCANSAFE	10

1.0 INTRODUCTION

This is one of a series of white papers setting out considerations for the enterprise in relation to corporate use of the Internet, and concerns itself with answering the following question:

“Why has the deployment of URL filtering products ceased to be a secure and cost-effective way of ensuring productive access to the Internet?”

This paper will discuss why and how organizations deployed URL filtering software and why this approach is no longer effective. The implications of using older, Web filtering technology to address the new generation of Web threats will be examined, as will some of the new ways to meet this challenge. It will be seen that the deployment of Web filtering software by the enterprise can partially reduce the level of risk to which they are exposed from the Internet. However, solutions enabling real-time scanning of Web traffic are the most secure way of delivering productive access to the Internet. SaaS Web Security is the most cost-effective way of delivering real-time scanning.

“Why has the deployment of URL filtering products ceased to be a secure and cost-effective way of ensuring productive access to the Internet?”

2.0 YESTERDAYS PROBLEM

Until relatively recently, the biggest concern any organization had about the Internet was what their workers were using it for. The vendors of URL filtering software painted an alarming picture of employees merrily surfing away their working days. At best, employees spent precious working hours house hunting, booking holidays and checking their webmail. At worst they were gambling and spending hours in chat rooms. They were a drain on productivity and bandwidth.

There was also a wider problem emanating from this on-line party. It exposed organizations to significant legal risks. These could come from inside the organization in the form of employees suing their employers for failing to protect them from Internet material they perceived to be offensive. For example, unrestricted Web access enabling the viewing of pornography in the work place, has given rise to successful claims for sexual harassment and unlawful sexual discrimination. Copyright infringement, for example, if an employee illegally downloaded material from a file sharing site, was another serious concern.

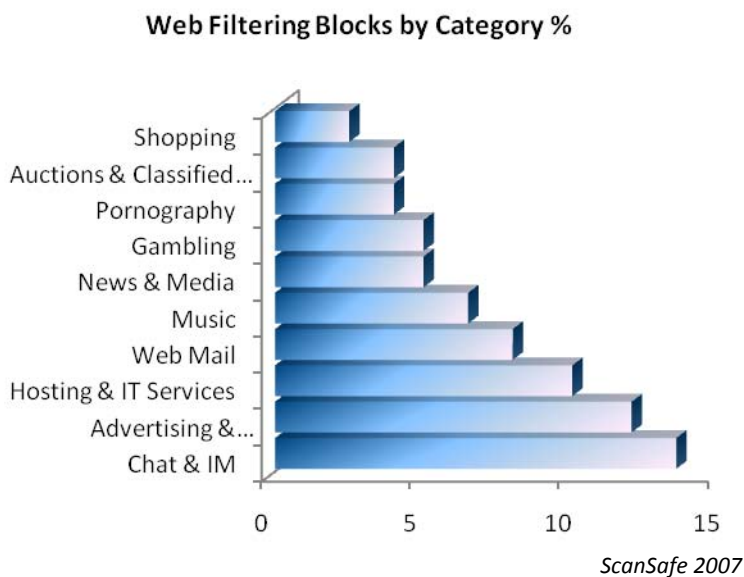
“Why 95 percent of enterprise networks use a URL filtering product of some kind.”

3.0 THE HISTORICAL APPROACH

In response to these understandable concerns, Acceptable Use Policies (‘AUP’) for Internet use were quickly drawn up and URL filtering software deployed to enforce them. The customers of URL filtering software vendors paid one-time licensing fees and then ongoing, annual subscriptions to huge, categorized databases of websites. These databases were built as URL filtering vendors crawled the Internet, categorizing every site that was found. Organizations could decide which categories contained unsuitable, unproductive content, block it accordingly and consequently limit their legal liabilities. The graph on the following page illustrates some of the more commonly blocked categories. They could also enforce time limits on less productive content, allowing employees to visit on-line banking sites only at lunchtime for example.

“These databases were built as URL filtering vendors crawled the Internet.”

THE FAILURE OF WEB FILTERING



URL filtering software was usually deployed in the first instance on a standard specification Microsoft Windows server situated within the corporate network perimeter. This meant that the early adopters of Web filtering software faced the challenge of keeping Windows patched and up-to-date as well as the filters themselves. For these and other reasons such as low specification hardware, these early deployments of URL filtering software often caused slower Internet access. Consequently, later deployments tended to be on gateway appliances rather than Windows servers. These appliances had pre-hardened, Linux based operating systems and because they were designed to do nothing but act as a gateway to the Internet they were fast and relatively effective.

URL filtering therefore fulfilled its original objective of AUP enforcement.

4.0 WHEN GOOD SITES GO BAD

“As the threat landscape evolved URL filtering companies sought to remake themselves into security companies.”

Whilst organizations were now effectively policing the Web access of their employees, the threats generated by the Internet continued to evolve. The Web gradually moved to become the primary attack vector used by malware authors to distribute malicious code. Instead of being confined to sites that could be easily categorized as “bad”, this code also began to appear on popular, trusted sites such as MySpace, The Sun, USA Today, Tom’s Hardware and the Mercury Prize. This immediately rendered category based filtering ineffective at enforcing security.

Browser vulnerabilities were also exploited in ever decreasing time windows. As Trojans, keystroke loggers, root kits and other Web malware became a major security issue organizations found that they were fighting new battles with outdated weaponry. If a legitimate site was hosting malware then it really didn’t matter which category in a database it was filed in because the chances were that employees would be able to access it.

Unsurprisingly, URL filtering has struggled to keep pace with rapidly evolving threats. This is because it was never designed to do so. As the threat landscape evolved, URL filtering companies sought to remake themselves into security companies and their URL filtering products were

repositioned from Web *productivity* solutions to Web *security* solutions. These products often claim comprehensive protection from Web malware through their sizable URL databases and offer regular updates that are downloaded daily or more frequently from a central server. These claims do not stand up well to scrutiny.

URL filtering can only be as effective as its database of categorized websites, and the traditional solutions rely on visiting each URL or “crawling” the Web in an effort to categorize sites. In a recent advertisement, a leading URL filtering vendor claimed it crawled 40 million websites an hour for malicious code. This sounds like an impressive number until you consider that the April 2008 Netcraft Survey put the total number of URL’s in existence at approximately 165 million. This means that even with a best-of-breed Web filter in place the information being used to determine whether a site represents a risk is likely to be at least a number of hours old. Using URL filtering to defend yourself against malware is like reading yesterdays newspaper to find the current price of your favorite stock.

Another challenge is the growing remote workforce. In order to try to enforce their AUP for workers outside of the corporate headquarters, organizations most often use end-point solutions to create an IPSEC or SSL VPN to ensure a secure connection to the corporate network. This is coupled with a desktop anti-virus solution to secure the host. However, backhauling traffic via a VPN often creates severe network bandwidth congestion and significantly impacts user experience which is, understandably, never popular.

Unfortunately, the only alternative until recently has been to create exceptions and allow remote users to alter their proxy settings and access the Web freely, with no content filtering being applied. This throws the door wide open to all of the threats that the whole Web security strategy has been put in place to prevent.

“This means that even with a best-of-breed Web filter in place the information being used to determine whether a site represents a risk is likely to be at least a number of hours old.”

5.0 THE NEW GENERATION OF WEB THREATS

In addition to the challenges set out above, URL filtering software has had to adapt again to a whole new generation of Web threats.

The Internet is no longer a static one-way delivery device but rather a fully collaborative environment that allows website owners and visitors to interact in real time. The contributions of website visitors can now define and manipulate the website experience, both for themselves and other users. Third party content providers can also influence this experience through targeted advertising, newsfeeds, and other dynamic contributions. This multi-way flow of information is accomplished through Web 2.0 technologies, a collection of scripting languages and applications that have fundamentally changed the nature of the Internet from a one-to-many delivery device to a many-to-many global communication experience. Web 2.0 has generally been viewed as a positive development by CIOs with organizations harnessing wikis, blogs, Rich Site Summary (‘RSS’) feeds, podcasts, content tagging and social networking tools.

However, the symbiotic ideal of Web 2.0 has been tarnished by the harnessing of these applications for less wholesome purposes. It is now easier than it has ever been for cyber criminals to inject malware into unsuspecting sites. Malware is being inserted onto Web pages via insecure advertising servers, compromised hosting networks, straightforward user-

“The Internet is no longer a static one-way delivery device but rather a fully collaborative environment that allows website owners and visitors to interact in real time.”

THE FAILURE OF WEB FILTERING

contributed content, and even through third party widgets, commonly found on many legitimate sites.

Case Study – MySpace

In the past year there have been countless incidences of popular collaborative sites being found to host malware. One such example occurred last June when a fast-flux network, a disturbing advance in the development and use of bot networks, was used to spread malware via a flash movie on MySpace. Possibly 100,000 MySpace accounts were affected by the attack. In effect, this MySpace attack in June was a double-whammy, combining the insecurities inherent in many Web 2.0 sites with a powerful, new and incredibly stealthy distribution technique. Unlike traditional ‘bot’ networks, fast flux networks abuse DNS to dynamically resolve an address to any number of infected PCs, as well as using the same technique to hide the control servers, which make them much harder to shut down. This ensures that the offending site(s) are active for a much longer period of time.

“URL filtering and the associated Web security infrastructure is not addressing the new generation of Web threats.”

6.0 THE PROLIFERATION OF SECURITY PRODUCTS

Because URL filtering is only addressing a fraction of the overall Web security challenge, ways to address the remaining areas of weakness have had to be found. Increasing reliance has been placed on desktop anti-virus tools to block malware but these were, and still are, difficult to scale and keep updated. These tools are most often signature based and therefore leave organizations vulnerable in the “zero hour”. Given the speed with which browser vulnerabilities are exploited this blows a gaping hole in corporate Web security.

This proliferation of security products has brought other challenges which are financial and operational in nature. According to Gartner, the annual costs of owning and managing software applications can be up to four times the cost of the initial purchase. For example, in order to realize the full reporting functionality of traditional Web filtering software, separate databases have had to be installed. This means the purchase of more hardware, another Windows license and a database license such as Microsoft SQL Server. These databases are not easy to administer, and organizations are finding that significant chunks of IT budget and manpower are being consumed in the maintenance of this sprawling Web security software infrastructure.

It is abundantly clear that despite consuming an ever growing proportion of IT budget, URL filtering and the associated Web security infrastructure is not addressing the new generation of Web threats. It is an expensive failure.

7.0 REAL TIME SCANNING

There is only one way to enforce your corporate AUP *and* protect your network from Web based malware. This is to ensure that in addition to all Web requests being checked against a categorization database, all of your Web traffic is scanned in real-time.

Real-time scanning means that all content on a URL is scanned immediately, every time that it is requested. This is an important distinction from URL filtering which merely filters URLs and compares them to a limited database of known categorized URLs. Effective real-time scanning should be powered by a combination of multiple detection technologies. When used on their own to combat malware as they are by many Web security vendors these technologies can often fall short. However, when these techniques are combined in a cocktail approach, their strengths are leveraged and their shortcomings mitigated. These techniques are as follows:

“Real-time scanning means that all content on a URL is scanned immediately, every time that it is requested.”

7.1 SIGNATURE-BASED DETECTION

Signature-based engines are extremely effective at identifying and blocking known threats. Multiple signature-based engines form an important part of a multi-layered cocktail approach to real-time scanning. However, as we have seen signature-based malware detection only works for known malware. It is not useful for new threats. Additionally, in order to be effective signatures must be delivered and propagated quickly—a time consuming task.

7.2 HEURISTICS

Using a rule of thumb to detect *variants* of known malware is an effective tool in the fight against malware. However, if your heuristics are too aggressive, you experience false positives. Also, heuristics are designed to increase the probability of detecting something that is similar to something that you have seen before. This means that a heuristic won't detect completely novel malware.

7.3 CODE ANALYSIS

The behavior of code can be determined by modelling program logic, behavioral rules, and contextual system call analysis techniques that suggest good or bad intentions.

7.4 CODE REPUTATION

Unlike URLs whose content can change, a binary can, in fact, have a reputation based on historical analysis. “Good” code can be treated differently to unknown or “bad” code.

7.5 URL REPUTATION

URL reputation is derived by examining parameters such as IP address information, country of the Web server, history and age of the URL, domain registration information, network owner information, URL categorization information, and types of content present. URL reputation provides a “credit history” of sorts for a URL, but it does not provide current information about the safety of a URL. When looking at Web safety, it is useful to bear in mind that past

THE FAILURE OF WEB FILTERING

performance does not predict future performance. As we've seen, "good" websites today may host malware tomorrow.

7.6 TRAFFIC BEHAVIORAL ANALYSIS

"The only way to provide Web security of this calibre in-house would be to deploy multiple layers of software."

Traffic behavior analysis identifies suspicious, atypical traffic which would suggest, for example, a new phishing scam or perhaps active malware communications from an infected notebook computer to a command-and-control computer. Unlike reputation techniques, which are based on past behavior and provide valuable historical context, actively monitoring Web traffic patterns and anomalies provides a real-time look into emerging threats. The important point to note here is that behavioral analysis of traffic is only effective if it is based on a large volume of real world traffic.

The only way to provide Web security of this calibre in-house would be to deploy multiple layers of software. We have established that URL filtering software is not up to this challenge. Although deploying it on a dedicated gateway appliance alongside gateway anti-virus and desktop protection suites might mitigate some of the new generation of Web threats it simply doesn't tick all of the boxes. Furthermore, these numerous products would be expensive and time consuming to integrate and manage. Inefficiencies would persist because these although these products might be the leaders in their particular field they cannot communicate with each other.

8.0 SCANSAFE SaaS WEB SECURITY

"ScanSafe Web security services are built on Outbreak Intelligence™ ('OI'), a proprietary security platform that detects new and known malware threats."

ScanSafe are the pioneers and global leaders in the provision of Software-as-a-Service ('SaaS') Web Security. Their award winning service protects organizations of all sizes from Web based malware attacks and enables safe, productive use of the Web without incurring up-front capital, hardware or management costs.

ScanSafe Web security services are built on Outbreak Intelligence™ ('OI'), a proprietary security platform that detects new and known malware threats. By leveraging its unique position at the Internet level and processing several terabytes of Web data each day, OI has unmatched visibility of global Web data to proactively identify zero-hour malware threats. OI uses multiple signature-based anti-malware scanning engines, multiple reputation and behavior-detection engines, and heuristics to detect new malware and avoid false positives. This combination of multiple, correlated detection technologies and the industry's largest Web data set make OI the most effective solution against new Web malware attacks.

Customers of ScanSafe receive a 360° view of the current Web threat environment compared to the very limited view given by those utilizing URL filtering alone. This is the difference between seeing the full picture and just one piece of the puzzle. This 360° degree view of Web threats that ScanSafe delivers allows the various, traditionally disparate, components of Web security to be connected. Simply crawling the Web for dangerous sites yields a random collection of "bad" sites that are seemingly unrelated. However, relying on the techniques above, real-time scanning can provide critical information on the source of malware infection and deliver immediate protection.

Case Study – Parked Websites

The ScanSafe Threat Center recently reported a number of sites hosting malware that was being delivered via a compromised advertising server. Through their analysis, they discovered the missing link: All the sites were “parked” with a service that uses inactive websites to host advertisements. Upon contacting the domain parking service and providing information on the source of the infection, over 100 similarly infected sites were blocked immediately. Without this deeper analysis, URL crawling and filtering simply marks what it finds. The net result would have been the blocking of a handful of sites, while the remaining sites continued to host malware and the advertising server continued to infect additional sites.

ScanSafe also provides SearchAhead, the industry’s first real-time scanning of search results that allows organizations to alert employees before they visit unsafe search results. SearchAhead scans results from popular search engines Google, Yahoo and MSN, providing advance warning of any malware and guidance on acceptable or unacceptable websites, based on the customer’s Web filtering policies. Organizations are therefore able to reduce AUP violations by 30 percent and also able to reduce further the likelihood of Web malware being chanced upon by hapless employees.

The ScanSafe service is implemented via a simple configuration change which routes organizations Internet traffic through ScanSafe’s global network of datacenters. Web requests are filtered in the Internet ‘cloud’ and malware is removed before serving clean traffic back to the user. Corporate AUP can be applied to all users regardless of location and management is also simplified because no endpoint updating is required.

9.0 THE FURTHER BENEFITS OF SaaS WEB SECURITY

The adoption of SaaS Web Security brings many benefits. These benefits allow an enterprise to “work smart” by focusing their energies on activities core to their business. Precious IT resource can concentrate on strategic activities and actually contribute to their organization’s bottom line rather than spending large amounts of their time solving problems generated by several products which together only deliver a partial solution. Service Level Agreements concerning up-time, latency, false positives and negatives are standard and SaaS Web Security is fully scalable. As the Web threat landscape shifts the enterprise can plan capacity and budget with confidence. In summary, the adoption of SaaS allows IT resource to *innovate* rather than *maintain*.

“The adoption of SaaS allows IT resource to *innovate* rather than *maintain*.”

” Implementation of SaaS Web Security is the most cost-effective way of delivering real-time scanning, and hence secure and productive access to the Internet for the vast majority of organizations.”

10.0 SUMMARY AND CONCLUSION

The conclusions reached by this paper are as follows:

- URL filtering software fulfilled its original objective of preventing workers from visiting websites that were deemed undesirable by their employers
- URL filtering has failed to address the growing challenge of keeping Web based malware off the corporate network
- In particular, URL filtering is ill equipped to deal with threats generated by the Web 2.0 collection of technologies
- The proliferation of Web security products and their ongoing management is now widely understood to be a poor use of expensive IT resource
- The only way to ensure that corporate AUP is enforced and that Web malware stays off the network is to ensure that in addition to all Web traffic being directed through URL filtering software, it is also scanned in real-time
- Effective real-time scanning should be powered by a combination of multiple detection technologies

Implementation of SaaS Web Security is the most cost-effective way of delivering real-time scanning, and hence secure and productive access to the Internet for the vast majority of organizations.

11.0 ABOUT SCANSAFE

ScanSafe is the largest global provider of Web Security-as-a-Service, ensuring a safe and productive Internet environment for businesses. ScanSafe solutions keep viruses and spyware off corporate networks and allow businesses to control and secure the use of the Web and instant messaging. As a SaaS solution, ScanSafe’s services require no hardware, upfront capital costs or maintenance and provide unparalleled real-time threat protection. Powered by its proactive, multilayered Outbreak Intelligence™ threat detection technology, ScanSafe scans more than 20 billion Web requests and blocks 200 million threats each month for customers in over 80 countries.

With offices in London and San Francisco, California, ScanSafe is privately owned and financed by Benchmark Capital and Scale Venture Partners. The company received the CNET UK Business and Technology award for Security Product of the Year 2008, a 2007 CODiE award for Best Software as a Service Solution, the 2008 and 2007 SC Magazine Europe Award for Best Content Security Solution and was named one of Red Herring’s Top 100 Technology companies. For more information, visit www.scansafe.com.

Contact ScanSafe

ScanSafe US
185 Berry Street
San Francisco, CA 94107

T: 415 692 2000
F: 415 536 5949
E: info@scansafe.com

ScanSafe EMEA

The Connection, 198 High Holborn
London WC1V 7BD

T: 020 7959 0630
F: 020 7959 0631

About ScanSafe

Founded in 1999, ScanSafe is the leading global provider of Web Security-as-a-Service, ensuring a safe and productive Internet environment for businesses. As a SaaS solution, ScanSafe's services require no hardware, upfront capital costs or maintenance and provide unparalleled real-time threat protection. Powered by its proactive, multilayered Outbreak Intelligence™ threat detection technology, ScanSafe scans more than 20 billion Web requests and blocks 200 million threats each month for customers in over 80 countries.

For more information visit www.scansafe.com