



Netsweeper Inc.
Corporate Headquarters
104 Dawson Road
Suite 100
Guelph, ON, Canada
N1H 1A7
CANADA
T: +1 (519) 826-5222
F: +1 (519) 826-5228

Netsweeper Inc. Europe
41 Marlowes
Hemel Hempstead
Hertfordshire
HP1 1EP
UNITED KINGDOM
T: +44 (0) 1442 355 160
F: +44 (0) 1442 355 001

Netsweeper Inc. India
Apt. No.: 9J, Block 2
Ceebros Shyamala Gardens
136, Arcot Road, Saligramam
Chennai – 600 093
INDIA
T: +91 44 426 426 25
F: +91 44 426 426 35

Netsweeper Inc.
Australia/New Zealand
13 Bareena Drive
Mt. Eliza, Victoria
3930
AUSTRALIA
T: +61 (0) 3 9787 2284
F: +61 (0) 3 9787 0965

www.netsweeper.com

Netsweeper Whitepaper

The Evolution of Web Security

June 2010

©1999-2010 Netsweeper Inc.

All rights reserved.

Every effort has been made to ensure the accuracy of this document. However, Netsweeper Inc. makes no warranties with respect to this documentation and disclaims any implied warranties of merchantability and fitness for a particular purpose. Netsweeper Inc. shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this document or the examples herein. The information in this documentation is subject to change without notice.

Netsweeper and Netsweeper Inc. are trademarks or registered trademarks of Netsweeper Incorporated in Canada and/or in other countries. Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are the sole property of their respective manufacturers.

Table of Contents

INTRODUCTION	4
WEB 2.0	4
FUTURE OF WEB SECURITY	6
NETSWEEPER SOLUTION	6
PROACTIVE WEB SECURITY.....	6
CONCLUSION	7

INTRODUCTION

The increasing velocity of communications, information sharing and collaboration is growing to create a complex environment with numerous external parties and partners. As quickly as security evolves, the techniques of hackers and other malicious individuals evolve even faster. Hacking has become quite a lucrative business. The days of teenagers defacing websites are over – now the objective is to steal private and financial information and remain undetected. What has emerged is really an arms race between electronic criminals and security teams, with content integrity and the privacy of personal information hanging in the balance.

As Web 2.0 shapes the basis for today's generation of Internet browsing, portal interaction, social networks, Web-based messaging, and other content and program rich sites, organizations are now also adopting Web 2.0 technologies for legitimate business reasons. The business benefits of using Web 2.0 technologies with customers, partners and employees are extensive, but so too are the risks and threats.

The introduction of Web 2.0 has opened the flood-gates to new vulnerabilities, malicious code, compromised networks, phishing attacks, spyware, and inappropriate content. Web 2.0 is interactive and collaborative, and is now the primary infection point for malware or malicious code, and increasing in volume by 40% annually. The Analyst community reports that over 75% of enterprises are infected with spyware and malware - and malicious code is contained in 32% of the Web.

Clearly, organizations of all sizes must adopt and advance their Web security for protecting the network from inbound threats of viruses, malware, spyware, and other hazards with a scalable, high-performing solution that is purposely-built to manage real-time data flows.

WEB 2.0

In the early days of the Internet, many people using this collaborative network realised the increasing need to be able to find and organize files and information. The primary way of utilizing this to 'surf' in these days was utilizing Gopher, a distributed document search and retrieval system which was implemented across the Internet and utilized a simple text menuing system.

A system of indexing in the contents of the text, Hypertext, was developed across many platforms and in 1989, whilst working at CERN, Tim Berners-Lee invented a network-based implementation of the hypertext concept. The name that he gave this new technology was the World Wide Web.

The turning point for the World Wide Web as a generally accessible technology that anyone could use began with the introduction of the Mosaic web browser in 1993, a graphical browser developed by a team at the National Centre for Supercomputing Applications at the University of Illinois at Urbana-Champaign (NCSA-UIUC), led by Marc Andreessen. Mosaic's graphical interface soon

became more popular than Gopher and the WWW became the preferred interface for accessing the Internet.

Since then we have seen many innovations in this technology and the capabilities available to the user through the browser. However, the little discussed, or even contemplated, result in this evolution is the complexity increase of the content entering our trusted networks.

As mentioned the early 'surfing' was a simple text based content system. Over the years with the advances in technologies and availability, and also the ever increasing demands of Internet users, we have seen these simple text searches now becoming increasingly complex content displayed on our screens. From simple request and response interactions, where the user initiated all the communications, the web has become a bi-directional communications media, with all the inherent security issues.

The generation today that has grown up with web pages that have more and more capabilities to display pictures, sounds, streaming media, interactive content, have pushed the content into what we commonly refer to as Web 2.0. While the functionality behind the web is always increasing, the term Web 2.0 is not referring to a new revolutionary technology; it is referring to a trend in web usage to enhance creativity, information sharing and collaboration among the users. In fact, most of the technology or technical concepts utilized in Web 2.0 have been around since Tim Berners-Lee envisaged the WWW!

The main driver behind Web 2.0 is primarily the end user. Expectations of the content they view, the method of viewing it and the delivery of that content is driving the use of the web. The expectation of using the web to request and view information is outdated. Users now expect complexity of content and an interaction with that content

Web 2.0 has also brought us dynamic websites, a term used to describe a website that aggregates information from multiple sources and displays the result to a single request. This new advancement has made the creation of sophisticated websites very easy and the results very pleasing to the end user, but introduces a new vector of threats that increase the complexity of protecting a network. A recent example of attack utilizing the complexity of websites and the inherent difficulty in protecting your network was the hack of Trend Micro's website.

Trend Micro is itself a leading security vendor but one of the pages on its website was hacked and a rogue JavaScript introduced. This script redirected a portion of the web request on the aggregated page to a server system which returned a script, downloaded to the user's machine through vulnerabilities in the web system, which then searched the end users machine for passwords for online games. This same method was used previously when the Miami Dolphins website was similarly hacked just prior to their playing the 2007 Superbowl and just a few months earlier for an attack on another security vendor CA.

FUTURE OF WEB SECURITY

Obviously, with the mass adoption and use of the Internet, the communications infrastructure has become an integral part of the overall security strategy, by virtue of the risks these communications channels are now subject to from internal and external sources. With blended threats and Web 2.0 risks, the integration of content for security is required for full vigilance and protection of communications. That said, we should consider a two-part communications security solution that integrates all channels. First, we must protect the inbound communications with threat prevention tools that block, viruses, malware, spyware and network attacks from entering the network, ensuring the viability of the network and communications infrastructure. Secondly, we must proactively scan the content and data most popular across a user base to ensure continuous intelligence on the security risks.

NETSWEEPER SOLUTION

New viruses, Trojans, worms and malware continue to appear at a rapid rate, with several thousands of new malware or variants detected each month. With the proliferation of signature based solutions on endpoints, gateways, and even firewalls, attacks today are more targeted and utilize multiple variants, with techniques such as time based obfuscation. This new approach from the cyber criminals makes it very difficult for traditional signature based solutions to effectively block the new waves of malware from proliferating. Each new outbreak has to be analysed bit by bit and signatures developed. A new, proactive security approach is needed to protect against the growing number of new, unknown malware threats.

PROACTIVE WEB SECURITY

Netsweeper's Web security provides a solution that detects zero-hour and known malware threats. By correlating a combination of current traffic and request trends, multiple detection technologies, automated machine-learning heuristics, and the industry's largest data set of web content, Netsweeper provides the most effective solution against new and known Web malicious content.

Netsweeper's signature-based scanning detects known Web malware residing on both reputable and uncategorized Web pages. As is expected in a signature based solution Netsweeper's solution utilizes multiple anti-malware scan engines which cover all known spyware and viruses with regular updates hourly and immediate updates for outbreaks. Every new URL requested is automatically scanned utilizing this engine and the current URLs in the database are regularly scanned to ensure their current legitimacy.

Netsweeper's heuristic engines utilize non-signature detection techniques and are based upon Artificial Intelligence engine technologies used to traverse the content and make decisions based upon thousands of inputs trained from years of collected information and trends.

However, utilizing this signature-based scan engines, the heuristic detection engines and correlating this with the real-time trends of requests provides Netsweeper with an unparalleled advantage in providing zero-hour response.

Netsweeper systems filter approximately 3 million requests a second for information from around the world in multiple languages, multiple sectors and for multiple areas of information. Of this, nearly 10 million requests per day are for brand new URLs which have never been seen before. With over 10 years in operation, our database of current URLs is over 3 billion items giving Netsweeper an unrivalled view of demographically accurate web history and usage.

Netsweeper immediately sees outbreaks of malicious code through the trend of requests, independently of the initial vector of propagation. If a new SPAM message or IM chat traverses the Internet with an image, document or link sending users to a web based threat, the traditional approach of scanning at the endpoint has shown vulnerabilities with lagging signature updates, lack of worldwide visibility and little trend information. In this case, a correlation of the immediate rush of requests, the history and a real-time content analysis to this link will allow the Netsweeper heuristic engines to block the malicious content in real-time, before any of our customers get infected.

CONCLUSION

Traditional approaches to web security have been almost rendered obsolete with the advent of Web 2.0. However, many of the new techniques in zero-hour defences have missed a key component of Web 2.0. It's not a new technology; it's a new paradigm in the use of the Internet facilitating communication, information sharing and collaboration. In other words, it's a real-time, interactive, content sharing platform.

Without the ability to correlate huge amounts of end user information and recognise usage trends as they happen, a web security solution is not going to be able to deal with the primary driver of Web 2.0, the real-time interaction. A security outbreak from a social media site will be widespread within minutes with today's user usage patterns.

Netsweeper offers a solution which is capable of dealing with massive amounts of web requests and correlating this information worldwide. With this real-time information of usage and patterns combined with both heuristic and traditional security techniques, Netsweeper provides a zero-hour web security approach which has protected our customers from every outbreak.