IronPort

IronPort Web Reputation: Protect and Defend Against URL-Based Threats

WHITE PAPER

TABLE OF CONTENTS

1 Executive Summary

2 Introduction

3 IronPort Web Reputation—an Innovative Approach

3 Web Reputation Inputs

4 Web Reputation Calculation

4 Quantity, Quality and Breadth

6 Web Reputation in Use

8 Summary

Executive Summary

IronPort Web Reputation is an innovative method that analyzes the behavior and characteristics of a Web server, providing the latest defense in the fight against spam, viruses, phishing, and spyware threats.

Email threats are no longer just nuisance spam that clutter a user's inbox. Today's dangers are blended threats – that are not only increasing in volume, but also in the level of sophistication and the potential damage to an organization or an individual. Malware writers are motivated by the desire to profit from these attacks. That often means invading end-user privacy and stealing both corporate and personal information. In order to protect against these threats, IronPort® has developed a new solution that does not simply rely on content analysis, but incorporates a more fundamental approach – analyzing both the behavior and characteristics of a Web server.

IronPort Web Reputation uses real-time analysis on a vast, diverse, and global dataset to detect URLs that contain some form of malware. Web Reputation is a critical part of IronPort's security database, which protects customers from blended threats – whether email or Web traffic.

DOC REV 02.08

INTRODUCTION

The explosive growth of spam, viruses, phishing, and spyware attacks (and the increasing capability of attackers to invade end-user privacy to steal personal and sensitive information) is a trend that threatens to undermine the stability of the Internet. The overall growth is undeniable: spam, for example, has seen an annual 200 percent increase in volume since 2002 and spyware websites have quadrupled in 2005. Even more worrisome than the sheer rise in malware is its increasing virulence. Several years ago, a typical virus infection resulted in a temporary reduction in PC performance or a system crash. Today, spyware and viruses regularly take over infected systems, steal personal and financial information from them, and use them as launching pads for further attacks.

Malware continues to flourish in part due to the constantly changing tactics of malware developers. In December 2005, the FTC issued a report concluding that spammers have abandoned brute force tactics and have developed more sophisticated, targeted attacks – which traditional content filters have limited protection against. Virus writers have responded to attachment filters that block all attachments by inserting malicious URL links into otherwise benign, attachment free email messages. The user clicks on the URL and inadvertently downloads a virus. Phishing websites have evolved to the point that they are now virtually indistinguishable from the real banking and e-commerce sites they spoof.

Not only has malware become more sophisticated, but attackers have begun to combine multiple forms of malware to create a “blended threat” that increases the potency of the overall attack. The recent Sober-Z outbreak used spam, viruses, and spyware to propagate. The attack was initially launched through spammed emails with viral attachments. Once a user’s machine was infected, it was hijacked with spyware and became part of a “bot network” of zombie PCs. These PCs sent out spam, collected credit card and bank account information and launched denial of service attacks. Sober-Z is not unique: 75 percent of all viruses contain spam delivery engines and 60 percent of the top ten viruses in 2005 had some type of spyware functionality.

Typical point anti-virus, anti-spyware and anti-spam solutions react to various symptoms of these blended, changing threats. But, they do not analyze the separate components of an attack in its entirety and are therefore forced to constantly react to threats, well after they occur. A new solution that analyzes a threat in a holistic and innovative fashion is needed to effectively stop an attack, in whatever form it is disseminated.

IRONPORT WEB REPUTATION—AN INNOVATIVE APPROACH

An increasingly common characteristic of malware is the presence of a URL that a user must visit to be attacked. Spam, URL-based viruses, phishing attacks, and spyware all direct the user to a malicious URL. If these URLs can be accurately analyzed, and a reputation associated with them, then stopping these attacks can be done much more quickly and accurately – and the URL can be avoided, in whatever method it is disseminated.

IronPort Systems realizes the importance of URLs to detect malware, and has responded by introducing IronPort Web Reputation – an innovative approach that helps protect against a broad range of URL-based threats. This solution asks a simple but powerful question —"What is the reputation of the URL?" When assessing the trustworthiness of a URL, a great deal can be determined by analyzing data that is hard to forge, such as how long the domain has been registered, what country the website is hosted in, is the domain owned by a Fortune 500 company, is the Web server using a dynamic IP address and more. By examining a broad set of (close to 50) parameters from an extremely large population, IronPort's Web Reputation technology can draw a very accurate picture about the trustworthiness of a given URL.

WEB REPUTATION INPUTS

IronPort Web Reputation leverages data from IronPort's Common Security Database (SenderBase® Network), the world's largest email and Web traffic monitoring network. SenderBase tracks over 50 distinct parameters that are excellent indicators of a URL's reputation. Using sophisticated security modeling and malware detection agents, IronPort evaluates these URLs based on these inputs. Some of the parameters include:

- URL categorization data
- Presence of downloadable code
- Presence of long, obfuscated End-User License Agreements (EULAs)
- Global volume and changes in volume
- Network owner information
- History of a URL
- Age of a URL
- Presence on virus / spam / spyware / phishing / pharming blacklist(s)
- Presence on virus / spam / spyware / phishing / pharming whitelist(s)
- URL typos of popular domains
- Domain registrar information
- IP address information

WEB REPUTATION CALCULATION

The Web Reputation calculation works as follows:

1. Each of the above attributes is constantly re-tested to determine the probability that URLs associated with this particular attribute contain malware. In turn, a corresponding weight is placed on each of these attributes.

2. Each URL is evaluated, using each of these attributes, to determine the overall probability that it contains malware.

3. This aggregate malware probability is mapped to a Web Reputation score between -10 and +10, with -10 being the most likely to contain malware and +10 being the least likely to contain malware.

IronPort Web Reputation differs from a traditional URL blacklist or whitelist in that it analyzes a broad set of data and produces a highly granular score of -10 to +10, instead of the binary "good" or "bad" categorizations of most malware detection applications. This granular score offers administrators increased flexibility; different security policies can be implemented based on different Web Reputation scoring ranges. See Figure 1 for examples of the type of situations that result in each score.

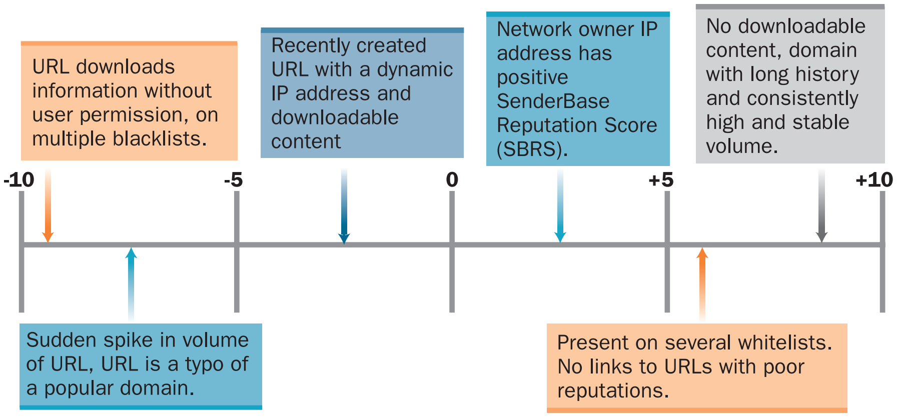

URL downloads information without user permission, on multiple blacklists.
Recently created URL with a dynamic IP address and downloadable content
Network owner IP address has positive SenderBase Reputation Score (SBRS).
No downloadable content, domain with long history and consistently high and stable volume.
-10
-5
0
+5
+10
Sudden spike in volume of URL, URL is a typo of a popular domain.
Present on several whitelists. No links to URLs with poor reputations.

Figure 1: Web Reputation Score Examples

QUANTITY, QUALITY, AND BREADTH

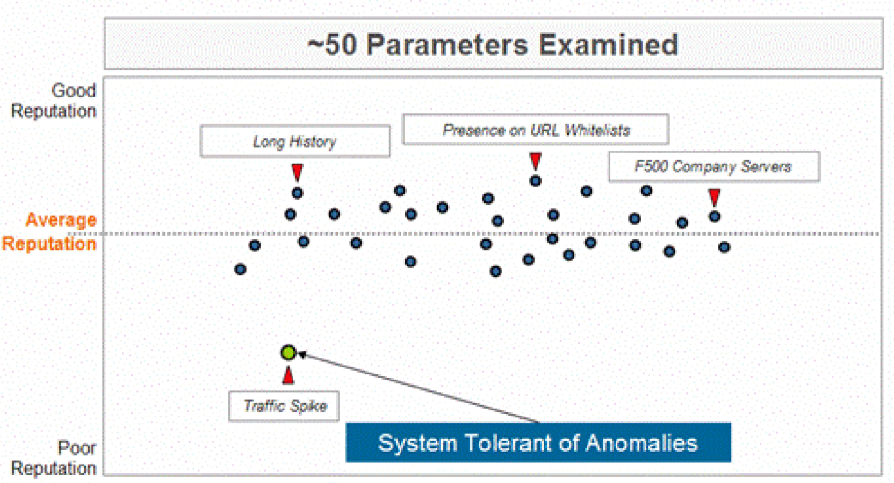
In order to drive efficacy, and accurately assess the reputation of a given URL, the underlying data must be robust in terms of quantity, quality, and breadth. This is where SenderBase leads the industry.

SenderBase tracks over three million domains on its global watch list and has an unprecedented insight into 25 percent of the world's Internet traffic. It is the only threat database that works with networks that are not limited to a specific vendor's customers. SenderBase data is fed by over 100,000 contributing organizations, including eight of the ten largest ISPs, Fortune 500 and Global 2000 enterprises, and sources from every major geography and customer category in the world. To augment this data, IronPort uses sophisticated Web crawlers that scour the Internet for newly created or modified URLs. IronPort also receives URL feeds from several thoroughly evaluated sources, which identify URLs that contain viruses, spam, spyware, phishing, and pharming.

The quantity and diversity of the networks contributing data, lead to the second critical database attribute – quality. Starting with the Sender Reputation system over three years ago, IronPort has had a great deal of operational experience managing data quality and integrity. To this end, IronPort has developed a Data Quality Engine that continuously assesses the reliability of a given source using sophisticated anomaly detection techniques against known references or benchmarks.

The final attribute of an email and Web traffic monitoring system is breadth of data. Looking at a narrow set of data can lead to high false positive rates. For example, a sudden traffic spike is a very interesting parameter. A traffic spike might correlate very well with a new virus outbreak that is using a URL to deliver the payload. But there are legitimate instances of traffic spikes such as BBC publishing breaking news on their website. Thus, if a traffic spike alone was the metric, many legitimate URLs would be blocked. But when a traffic spike is examined in addition to other parameters – such as a long history of hosting content, presence on URL whitelists, and Fortune 500 company IP range – a much more accurate conclusion can be drawn. By examining the broadest set of data in the industry (more than 50 different parameters), the IronPort Web Reputation technology prevents the overall Web Reputation score from being susceptible to inaccurate information from any one attribute. See Figure 2 for an example.

Figure 2: Global Efficacy for Broad Threats



WEB REPUTATION IN USE

IronPort Web Reputation increases the efficacy and catch rate of every URL-based type of malware. This powerful technology is currently being utilized by IronPort's C-Series™ email security appliance. Regardless of whether a bad URL is trying to enter via email or Web, the IronPort appliances will stop it, using Web Reputation.

Spam and URL-based Viruses: Traditional spam solutions evaluate whether an email is spam or not by answering the basic question of "what", such as "What is the nature of the content of a message?". The difficulty with this approach is that spammers have found a variety of techniques to fool these filters – such as adding blocks of legitimate text (called Bayesian busters) or using numbers instead of letters (e.g., L0ve). As a result, first generation anti-spam filter efficacy has decreased. Almost every spam message contains a URL – as a way to enable the reader to view the advertising website. Web Reputation adds another dimension to spam analysis by asking "Where" – where does the URL take me?

By accurately identifying the reputation of the URL, a more accurate analysis of the likelihood that a message is spam can be performed. Similarly, with messages that contain links to URLs which host viruses, Web Reputation prevents these messages from reaching end-users. Traditional anti-virus and attachment filtering solutions lack this capability.

Spyware: Typical spyware solutions contain fairly static blacklists and spyware signatures. Spyware objects must be deconstructed and signatures must be written for these malicious pieces of software – a process which can take days. IronPort Web Reputation is constantly evaluating and re-evaluating URLs for the presence of spyware, and immediately adjusting scores of these URLs appropriately, dramatically reducing the reaction time gap. Unlike traditional spyware engines that focus solely on spyware, Web Reputation also protects users from phishing and pharming sites, as well as sites infected with viruses.

In order to maximize throughput and minimize latency, IronPort Web Reputation is used to determine what type of scanning needs to be done. A strong positive reputation may require no spyware scanning. A weak positive reputation may require scanning from only one engine. A weak negative reputation may require scanning from multiple engines. And a poor reputation may not require any scanning as it can simply be blocked. The intelligent scanning actions taken by the system come with recommended default settings. But, system administrators can fine tune the thresholds for scanning, based on their own aggressive or conservative anti-spyware policies.

Phishing / Pharming: Phishing site creators can spoof the content of their websites to perfectly replicate legitimate banking and e-commerce sites. However, phishing cannot spoof the URL at which they are located. IronPort Web Reputation has a detailed and up-to-date score for the vast majority of URLs and can therefore protect users from phishing attacks.

Blended Attacks: The recent Windows Metafile Vulnerability (WMF) highlights the increasing use of blended attacks and the power of Web Reputation to stop them in all of their manifestations. In late December 2005, a WMF vulnerability (that allowed the execution of potentially malicious code) was discovered. To become infected, a user merely had to browse to a site that had a WMF file (usually a picture) embedded in it. No explicit end-user action was required to download the malicious code. At first, this vulnerability was exploited by spyware vendors who placed spyware-infected WMF files on URLs that were typos of legitimate popular websites. Hosts initially infected by inadvertent visits to these spyware hosting sites, in turn, spammed out emails with links to these sites. This process repeated itself unabated and the problem became so severe that Microsoft took the unprecedented action of releasing a patch to fix the WMF vulnerability, several days before its regularly scheduled monthly patch update.

Traditional anti-spyware solutions were not quick enough to determine this new presence of spyware and write signatures for it. Anti-spam and antivirus solutions were not able to recognize that emails sent by infected hosts contained links to sites that exploited WMF vulnerabilities. IronPort Web Reputation, however, has the ability to quickly see the presence of new URLs on the Web, and immediately assign them a Web Reputation score – based on factors such as the use typos of popular domains, the rapid increase in volume, and presence of downloadable code. Only Web Reputation has the power to block users from accessing these sites, whether they were attempted to be viewed through a typo in a website query or by a link in a spammed email. Finally, the broad Web Reputation scoring range allows administrators to configure security policies to fit their specific security profile.

SUMMARY

Spam, viruses, phishing, and spyware threats are increasing in volume and sophistication. First generation anti-virus, anti-spam and anti-spyware applications primarily rely on content analysis and are therefore susceptible to advanced attacks that randomize and obscure the nature of the content. IronPort Web Reputation takes a more fundamental approach – by analyzing the behavior and characteristics of the Web server. Web Reputation uses real-time analysis of a vast, diverse global dataset to detect URLs associated with threats, and assign a highly granular score of -10 to +10 to each URL, based on the likelihood that it is malicious. Web Reputation is a critical part of IronPort's security database that allows the IronPort security gateways to stop malware and blended threats in whatever form they take – email or Web traffic.

IRONPORT®

IronPort Systems
950 Elm Avenue, San Bruno, California 94066
TEL 650.989.6500 FAX 650.989.6543
EMAIL info@ironport.com WEB www.ironport.com

IronPort Systems, a Cisco business unit, is a leading provider of anti-spam, anti-virus and anti-spyware appliances for organizations ranging from small businesses to the Global 2000. IronPort appliances utilize SenderBase, the world's largest email and Web threat detection network and database. IronPort products are innovative and easy-to-use—providing breakthrough performance and playing a mission-critical role in a company's network infrastructure.

IronPort is now part of Cisco.

CISCO™