

IronPort Virus Outbreak Filters: A Preventive Security System

WHITE PAPER

TABLE OF CONTENTS

- 1 Executive Summary
- 2 Introduction
- 3 Virus Outbreak Detection
- 3 Virus Outbreak Filtering
- 5 Summary

Executive Summary

IronPort Virus Outbreak Filters detect and stop viruses before any other technology.

Email viruses are becoming increasingly more complex and faster spreading. Today, viruses spread in a matter of hours, often completely disrupting email service for corporations and creating an all-hands emergency situation for IT staffs around the world.

In these times of fast proliferating viruses, traditional anti-virus defenses that rely solely on signature-based filters are no longer adequate. While these solutions are very accurate at detecting known viruses, they depend on receiving regular signature updates to protect against new threats. This makes them vulnerable to reaction times that can vary from hours to days. And during that “vulnerability window”, a modern virus can propagate globally, bringing email infrastructure to a halt.

IronPort Virus Outbreak Filters™ work proactively to provide a critical first layer of defense against new outbreaks. By detecting new outbreaks in real time and dynamically responding to prevent suspicious traffic from entering the network, IronPort Virus Outbreak Filters offer protection until new signature updates are deployed. Integrated into IronPort’s C-Series™ email security appliances, Virus Outbreak Filters have two principal components: the outbreak detection technology and the intelligent quarantine system implemented in the IronPort C-Series appliances.

INTRODUCTION

To fully comprehend the value of additional protection against email viruses with a predictive security technology, it is necessary to understand how viruses have changed over time and where the gaps exist in traditional anti-virus solutions.

The International Computer Security Association (ICSA) Labs 9th Annual Email Virus Prevalence Survey reported that, not only was there an increase in the total number of viruses in 2003, but the viruses were more destructive and costly than their predecessors. And this was despite an increase in anti-virus defenses at the desktop, mail servers and gateways.

The primary reason for this issue is that newer viruses are spreading faster than those in the past. Modern virus writers are using increasingly clever “social engineering” including, provocative subjects or obfuscated file types, such as password protected zip files, to lure users into opening the payload attachments. These techniques combined with automated mass-mailing mechanisms propel new viruses to propagate globally in a matter of hours.

At the same time, most anti-virus defenses are inherently reactive, relying almost entirely on solutions that employ signature-based filters. These solutions operate by looking for patterns in data streams, and stop messages that match known viruses. As a result, with these mechanisms there is a substantial gap—anywhere from several hours to days—between when a new virus breaks and when the updated signature to block the virus is deployed. The entire process of identifying a new virus, analyzing it, creating a signature for it and deploying that signature requires a finite amount of time and the new generation of email viruses is clearly exploiting this flaw, spreading much faster than the signatures to block them can be distributed.

VIRUS OUTBREAK DETECTION

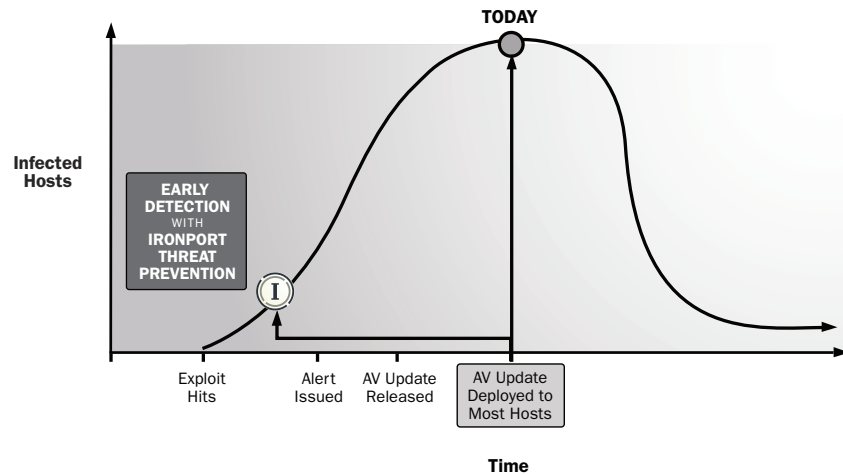
Automated Detection Using SenderBase

New email virus outbreaks can be detected by analyzing global traffic patterns, and blocked before they are able to exploit the reaction time vulnerability of traditional signature-based filters. IronPort® Systems has developed SenderBase®, the world's largest email and Web traffic monitoring network. An open database, SenderBase collects data from over 100,000 ISPs, organizations and universities around the world to provide a view into a remarkable 25 percent of global email traffic patterns. SenderBase tracks a variety of parameters including global sending volume, message composition, complaint levels, activity in “spamtrap” accounts, open proxy and relay data, country of origin, and more. Today, SenderBase processes more than five billion queries per day on more than 20 million IP addresses.

IronPort has developed advanced statistical models to process this diverse, global data and look for anomalies. A key component of IronPort's detection technology, these models analyze historical traffic and create a statistical view of normal traffic patterns across the globe. At the same time, real-time data flowing in from the global SenderBase Network is captured and compared to this baseline to identify anomalies. Certain key anomalies are excellent predictors of a global virus outbreak. For example, if IronPort's detects a sudden surge in new IP addresses sending mail that have never sent mail before, and furthermore all of these new IPs are sending a certain email attachment type (such as a password protected zip file), that is an excellent predictor that a new virus associated with password protected zip files is breaking out.

Data from the IronPort virus detection system is used to alert the IronPort Threat Operations Center (TOC). There, technical staff review the anomaly and issue a virus threat level score. Threat level scores are dynamic and move up or down, based on traffic patterns and the corresponding availability of virus definition files from traditional anti-virus vendors.

Figure 1: IronPort Virus Outbreak Filters close the reaction time gap



IronPort Threat Operations Center (TOC)

Ensuring full protection from new outbreaks requires both speed and accuracy. To enable this, IronPort has built a 24x7 Threat Operation Center staffed by experienced analysts that closely monitor outbreaks through their entire lifecycle.

TOC analysts leverage sophisticated Web-based applications and tools to rapidly verify anomalies. These tools allow point and click visualization of complex real-time and historical traffic patterns including message volume, size, attachments, sources and more. This allows analysts to spot trends and potential problems quickly-helping make better decisions.

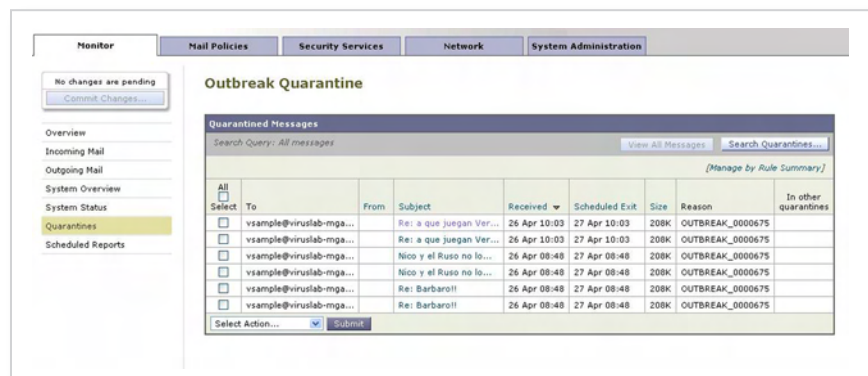


In addition, analysts have the ability to update threat levels and rules on a constant, rapid basis ensuring efficacy and countering the dynamic nature of threats. Analysts also ensure that a customer-facing website is continuously updated with data on current outbreaks.

VIRUS OUTBREAK FILTERING

IronPort appliances are typically deployed at the perimeter of a private network. These appliances are built on a revolutionary MTA platform that has advanced message handling capabilities. As mail is flowing into the IronPort appliance, a threat assessment (based on the IronPort threat level) is performed. If anomalous traffic patterns have been detected associated with a certain message characteristic such as attachment type, the threat level will be elevated and trigger preventative action.

Figure 1: IronPort Virus Outbreak Filters quarantine questionable messages until reactive virus definition files have been updated



The IronPort email security appliance will automatically filter all incoming and outbound mail and quarantine questionable messages when the threat level is raised. These messages remain in the outbreak quarantine until the reactive virus definition files have been updated. At that point, messages are released and re-scanned through the traditional anti-virus filters. By responding in a benign way, the Virus Outbreak Filters prevent serious damage without causing other issues.

System administrators have the ability to tailor the specific response taken when a threat level is raised. Certain users or LDAP groups can be opted out of the quarantine. Using the Web-based administration tools in the IronPort appliance, administrators can view quarantined messages and selectively release them. Administrators can also release a message and run it through a “trace” which provides a test of all of the system filters – anti-virus, anti-spam, content filters etc. Trace allows administrators to be sure the virus definition files are in place to maintain the integrity of their network.

SUMMARY

As email viruses evolve to become faster spreading and more destructive, corporations will need to expand anti-virus defenses to include solutions that proactively detect and dynamically respond to new outbreaks.

Today, most corporations implement a layered anti-virus defense using reactive anti-virus solutions at the desktop, mail server and gateway. However, the unavoidable window of time between when an outbreak starts and when updated signatures are deployed emphasizes the importance of including solutions that can prevent new virus outbreaks and dynamically trigger policies to protect networks immediately.

IronPort Virus Outbreak Filters offer protection that overcomes the time-to-response limitations inherent in traditional anti-virus solutions. Virus Outbreak Filters recognize email virus outbreaks, faster than traditional anti-virus solutions, allowing corporations to defend against new outbreaks before they escalate into damaging and costly incidents.



IronPort Systems, Inc.

950 Elm Avenue, San Bruno, CA 94066

TEL 650.989.6500 FAX 650.989.6543

EMAIL info@ironport.com WEB www.ironport.com

IronPort Systems is the leading email and Web security products provider for organizations ranging from small businesses to the Global 2000. IronPort provides high-performance, easy-to-use, and technically innovative products for those faced with the monumental task of managing and protecting their mission-critical networks from Internet threats.