IRONPORT

A Multi-Layered Approach to Preventing Viruses

WHITE PAPER

TABLE OF CONTENTS

Executive Summary

A high-performance preventive security system protects your network from infections.

As virus writers create increasingly sophisticated malicious code and find ever more effective methods to propagate, enterprises find themselves scrambling to keep their networks, servers, and end-user computers safe from new threats.

Traditional anti-virus applications work by searching the contents of files and looking for a recognized pattern of data (a “signature”) that is the virus program itself. However, virus writers have come up with various methods to escape detection by changing their programs, making it harder for virus scanners to recognize them as viruses. Today’s viruses are either polymorphic or metamorphic and can actually change themselves as they propagate. The increasing sophistication of malicious code is therefore making pattern recognition technologies less and less effective.

This decline in effective virus defense is taking a toll on businesses. The often long delay between the time when a virus attack is launched and when a signature is available can result in hundreds of thousands of infected messages being delivered to enterprise networks and communities of ISP users. Even when the end effects of the virus are minimal, such widespread infection results in major costs. Productivity is lost as employees try to understand what’s wrong with their computers and seek help. Clearing computers of viral infections requires both manpower and other resources to aid in the clean-up. That translates into tens or even hundreds of thousands of dollars in desktop clean-up costs for each virus outbreak at each corporation. If there has been actual data destruction, the costs can be immense, possibly immeasurable.

"For a typical mid-sized enterprise, per disaster recovery time rose from two to seven person-days and clean-up cost was $130,000 per network—an increase of over 40 percent from 2003."

ICSA Labs 2004
Virus Prevalence Survey

Another factor contributing to the increasing seriousness of computer virus attacks is the motivation of today's virus writers. Although teenage hackers looking for ego gratification still exist, anti-virus research groups are seeing an increasing number of viruses designed to bring in money—sometimes as part of criminal activities. Political and social extremists have also turned to computer viruses as one way to accomplish their goals.

Spammers—the people who send out millions of unsolicited commercial email messages a day—realized at some point that virus writers could help them overcome spam-blocking measures on corporate and ISP networks. Some viruses are now designed to turn network-connected PCs into robots for sending spam. Most of these robot PCs (or "zombies") are in homes, but many also get created in enterprise environments. Such hijacked computers now make up the BotNets responsible for most of the world's spam email messages. Some of those are fraudulent or "phishing" email messages that trick unsophisticated recipients into revealing personal information, such as passwords for financial accounts.

There are also organizations in the world who wish to disrupt Western economies. They realize that a virus that could potentially wipe out the hard drive of every infected PC could cause an economic impact of billions of dollars in a matter of hours. See the appendix for a case study of a virus that may foreshadow future politically motivated attacks.

An estimated 900 million virally infected messages a day are currently coursing through the world's email networks, and the problem is increasing dramatically. As a result, many companies and vendors are looking beyond today's signature-based anti-virus solutions and exploring preventive systems that can stop virus outbreaks before they happen.

EMERGING ANTI-VIRUS STRATEGIES

With the decline in effectiveness of traditional pattern recognition technologies, developers of anti-virus solutions are combining several new approaches to address the problem of increasingly sophisticated computer viruses. These new technologies include heuristic filters, behavioral analysis, and traffic data analysis.

- Heuristic filters are based on artificial intelligence techniques, so they become more accurate as they learn which messages contain viruses and which do not. Unlike pattern scanners, heuristic filters can detect a virus that hasn't been identified yet, so they can stop infections before a signature is released. However, their catch rate is significantly below 100 percent, and they are subject to false positives, which can prevent organizations from receiving vital legitimate business email that has been incorrectly identified as having a virus.

- Behavioral analysis systems actually load and execute a program attached to an email message (or downloaded from a Web link embedded in a message) and analyze its behavior as if it were running on an end-user's computer. The system can either emulate execution of the program or run it on a separate virtual computer (usually called a "sandbox"). The behavioral approach can be effective, but it is very resource intensive and not easily scaled to enterprise levels.
- Traffic analysis solutions are based on the fact that virus outbreaks come in waves of email messages, so there are patterns of email traffic anomalies associated with an outbreak. Experienced computer security personnel can detect these anomalous traffic patterns and relay the information to security devices. Because this approach requires a large, global dataset in order to identify patterns as they emerge, only security companies that are monitoring a significant number of large networks for enterprise and ISP email traffic are capable of using this technique.

While all three of these approaches hold some promise of greater virus control, traffic pattern analysis is widely regarded as the most promising technique. It works regardless of message or program content, and eliminates dependence on the ability of a certain computer system to recognize a virus program. This is important because virus writers use morphing algorithms to confuse pattern or signature-based systems by changing how they look and behave, and even where they are housed. Ironically, the more effective a virus is at avoiding detection by traditional signature-based filters, the faster it will propagate globally, and the more quickly a recognizable viral traffic pattern will emerge.

A COMPREHENSIVE APPROACH

Traffic data analysis is emerging as the best technology for detecting viruses quickly and accurately. However, it must be supplemented by the right infrastructure and supporting technologies if it is to offer truly effective virus defense for organizations around the world.

An accurate and efficient predictive virus solution should include:

- A mechanism for gathering global data on email traffic.
- A threat operations center with highly trained personnel who can detect emerging threats from analyses of traffic patterns.
- The ability to quarantine suspicious email messages based on dynamically changing rules.

Global Traffic Data

The key ingredient in creating an effective traffic-based virus detection system is a world view of email traffic patterns. The best solutions have a very large database of email traffic. These databases need to have messages from ISPs, enterprises, small and mid-sized businesses, education, healthcare, and government, just to name a few.

Morphing viruses such as Sober, SoBig, Netsky, and Bagle have propagated rapidly because there were no preventive signatures in place for a long period of time. They caused major disruptions to corporate and ISP networks, and in the process, created huge anomalous patterns in worldwide email traffic. It is impossible for normal human email messaging to create traffic patterns like those in which a single virus program spreads around the globe in two hours or less. So gathering real-time data from around the world is an essential foundation to detecting new attacks.

Threat Operations Center

A predictive system, by definition, is responding to unknown threats. Global data and sophisticated algorithms are very powerful tools to combat these threats, but there is no substitute for human oversight in helping to identify new anomalies and new outbreaks. The most sophisticated preventive solution will include a fully staffed 24x7 threat operations center that has multi-lingual analysts and statisticians reviewing dynamic email traffic data.

Dynamic Quarantining

The key concept behind predictive virus systems is that they can take action earlier than traditional systems, but with lower confidence. Thus, a sophisticated quarantine system is an essential ingredient to mitigate false positives. The quarantine software should have tools to allow administrators to easily address exceptions, release certain messages, or “opt-out” certain users.

More advanced systems use a new and very promising technology called dynamic quarantining. This approach offers continuous, automatic rescanning of all messages in the quarantine area. It makes possible the powerful combination of traffic-based anti-virus systems (which are highly accurate but take some time to detect patterns) and heuristic filters (which can react to new viruses immediately but are more subject to false positives).

Dynamic quarantining uses the coarse rules of a heuristics system to stop an outbreak as soon as it occurs, before enough anomalous traffic has appeared to develop a traffic-based rule. Because it quarantines rather than deletes messages, it mitigates the false-positive issues associated with heuristic methods.

At time zero, many messages may get quarantined, adding a slight bit of latency to the mail flow. However, within minutes, new data will emerge that narrows the quarantine and returns known good messages back into the mail flow. Because email is an asynchronous medium, most users will be unaware of the small added latency; it is a small price to pay for extremely robust virus protection.

As soon as additional data on the outbreak becomes available, new outbreak rules are issued in real time. The quarantined messages are immediately rescanned, and the system releases all messages that do not match the

newer, more fine-grained outbreak rule. Additional anomalies and observations will spawn updated rules, which will further narrow the quarantine to only infected messages. An example of a quarantine sequence is shown in Table 1

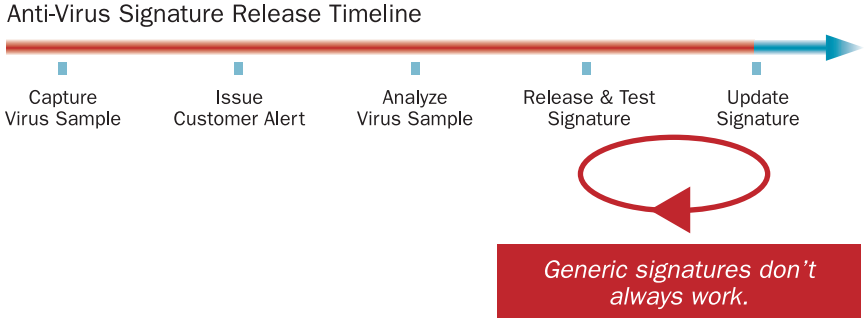
Table 1. Sample Rule Sequence for a Dynamic Quarantine

TIME	RULE	ACTION
T=0	Quarantine all attachments whose file type does not match the extension names. (For example, a file that says it's a .doc but is really a .zip.)	Implements a heuristic rule built from profiles of known outbreaks.
T=2 mins.	Quarantine all .zip attachments that contain an exe file.	Releases from quarantine any files with mismatched file type and file extension, except for .zip (exe) files.
T=1 hr.	Quarantine .zip (exe) files that are greater than 50 KB.	Releases from quarantine any .zip (exe) files that are less than 50 KB in size.
T=2 hrs.	Quarantine .zip (exe) files between 50 KB and 55 KB that have "price" in the filename string.	Releases from quarantine any .zip (exe) files that are smaller than 50 KB or larger than 55 KB, or which do not have "price" in the filename.
T= 8 hrs.	Scan against new signature.	Scans all remaining messages against the latest signature file from AV vendor.

The Essence of Time

Today's aggressive, intelligent viruses—especially when they're propagated via sophisticated spamming techniques—can infect hundreds of thousands of computers in a very short amount of time. Figure 1 shows the series of actions necessary to get a virus signature out to customers. Even the fastest virus sleuths take the better part of a day to get a new virus diagnosed and create a signature for it. Then it takes more time to distribute the signature file. Even aggressive signature update schemes leave users and enterprise networks vulnerable to virus attacks for anywhere from twelve hours to three days—more than enough time for a virus to do serious damage.

Figure 1: Anti-Virus Signature Release Timeline



AVERAGE RESPONSE TIME (HOURS:MINS)	VENDOR
06:51	Kaspersky
08:21	Bitdefender
08:45	Virusbuster
09:08	F-Secure
09:16	F-Prot
09:16	RAV
09:24	AntiVir
10:31	Quickheal
10:52	InoculateIT-CA
11:30	Ikarus
12:00	AVG
12:17	Avast
12:22	Sophos
12:31	Dr. Web
13:06	Trend Micro
13:10	Norman
13:59	Comman
14:04	Panda
17:16	Esafe
24:12	A2
26:11	McAfee
27:10	Symantec
29:45	InoculateIT-VET

Average Response Times of Anti-Virus Vendors

According to AV-Test, a German virus research group at the Otto von Guericke University in Magdeburg, the response times of anti-virus vendors to the emergence of a new virus vary dramatically. The group studies vendor performance by measuring the time from when a new virus is first spotted by a British consulting group, to when each vendor makes a signature file available. AV-Test checks anti-virus databases every five minutes for the presence of a new profile. The results shown in the sidebar were based on four virus outbreaks: Dumaru.Y, MyDoom.A, Bagle.A and Bagle.B.

As the sidebar shows, the results for those four viruses vary from nearly seven hours to more than a day. In the virus outbreaks monitored by IronPort® Systems, as much as three days have passed for some vendors to find the correct profile. The data does not reflect the fact that heuristic techniques used by some of the vendors allow viruses to be detected and blocked before signatures are developed and published. Nonetheless, even in the quickest case, the potential for a serious amount of destruction to occur while waiting for virus signature files is considerable.

IRONPORT SYSTEMS EMAIL SECURITY SOLUTIONS

IronPort Systems offers highly effective email security solutions. Our state-of-the-art preventive anti-virus product combines the following IronPort technologies and services:

- *SenderBase®*, the world's largest email and Web traffic monitoring network. SenderBase tracks more than 25 percent of the world's email traffic from over 100,000 contributing organizations, including eight of the ten largest ISP networks and some of the largest enterprise networks in the world. It collects information on more than 120 different parameters, including global volume data, message composition data, spam traps and complaint data, blacklists, third-party email accreditation, open proxy data, and much more. Because of its size and diversity, the SenderBase dataset provides a statistically significant view into the world's email traffic.
- *IronPort Virus Outbreak Filters™*, which use the SenderBase database to spot viruses before they strike, provide a critical first line of defense. To detect viral messages at all times, the filters use both Adaptive Rules and Outbreak Rules. Only IronPort Virus Outbreak Filters have Adaptive Rules, which continuously adapt to subtle changes in email traffic and structure to provide updated protection to IronPort customers. Unlike Outbreak Rules, Adaptive Rules are "always on," catching viral messages even before the full anomaly has formed. Adaptive rules are developed by training IronPort's Context Adaptive Scoring Engine™ (CASE) on profiles of historic outbreaks. The CASE is very effective at catching viruses at first sighting, before enough anomalous traffic has developed to create a traffic-based rule. The usual downside associated with this type of heuristic-based rule is an unacceptably high false positive rate. However, because the IronPort security appliances uses dynamic quarantining, the unacceptably high false positive rate normally associated with this type of heuristic-based rules, is mitigated.

IRONPORT®

- The IronPort Threat Operations Center (TOC). Using advanced security modeling algorithms developed by IronPort, the TOC analysts continuously examine the massive and diverse SenderBase database looking for anomalies in real-time message traffic that could indicate a virus outbreak. Such patterns might include an increase in messages of a particular size with a particular attachment file, messages with a similar attachment size coming from a single IP, or a sudden increase in mail from an IP address that has never sent mail previously. When a suspicious traffic pattern is discovered, the TOC generates outbreak rules that are pushed to customers' IronPort security appliances. The appliances then begin quarantining mail that matches the anomaly of the outbreak. This expert analysis of abnormal traffic patterns is critical in providing virus protection at the perimeter of an organization's network.

IronPort Virus Outbreak Filters have consistently identified outbreaks anywhere from one to 48 hours before virus signatures have been released by anti-virus vendors. In the first year of its release, this technology stopped more than 100 virus outbreaks an average of 16 hours ahead of traditional signature availability. At a typical Global 2000 company, that would translate to more than 5,000 infected messages being blocked per outbreak. A sample of response times is provided in Table 2.

VIRUS	DATE OF DETECTION	VIRUS THREAT LEVEL RAISED*	FIRST ANTI-VIRUS SIGNATURE AVAILABLE*	OUTBREAK FILTER LEAD TIME (HOURS:MINS)
Sober.N	5/2/2005	15:58	17:19	1:21
MyTob.J	3/25/2005	23:30	22:38 (next day)	23:08
Bagel.BB	2/27/2005	10:39	4:22 (two days later)	41:43
MyDoom.bb	2/15/2005	18:08	22:54 (next day)	28:46
Sober.J	1/30/2005	23:01	10:04 (next day)	10:57
Atak.d	12/3/2004	16:29	21:04	4:35
Mugly.a	11/30/2004	2:57	9:08 (next day)	30:11
NetSky.AG	10/21/2004	21:34	11:42 (next day)	14:08

**Times are in UTC (Coordinated Universal Time)*

GET PROTECTED

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.

The IronPort Virus Outbreak Filters offer protection that overcomes the time-to-response limitations inherent in traditional anti-virus solutions. IronPort 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.

APPENDIX: THE SOBER VIRUS/WORM/TROJAN

In 2003, the first SoBig worm appeared. The objectives of the SoBig family of worms were to create a network of robotized computers that could launch massive denial of service (DoS) attacks and also be used for spam attacks. The most significant variant was SoBig.f, which created the largest viral attack that had been seen to date. At one point, SoBig.f accounted for three percent of all email messages.

As significant as SoBig was, its notoriety has been superseded by Sober, a family of worms based on the SoBig model that first appeared in October, 2003. Sober has also at times generated well over three percent of email traffic. The original Sober was a relatively simple worm, but it evolved into a complicated program capable of morphing so as to make itself unrecognizable, moving itself to various locations, and spreading via both email messages and Web downloads. One perniciously clever version of the program deletes anti-virus update files that contain new Sober signatures.

In May, 2005, the Sober.q variant sent out neo-Nazi-tinged spam in both English and German. Most of the messages contained links to extreme right-wing news stories, but some had links to a website that tried to infect visiting machines with the virus. The infected computers could then be used to send out new rounds of spam.

Virus programs such as Sober, which use BotNets to send spam, do no great harm to the computer on which they run. However, the spam they generate creates an enormous drain on worker productivity and computer and network resources. That's why it's so important for organizations to prevent virus attacks that create BotNets.

Sober-N Timeline

An examination of the spread of Sober-N demonstrates how important it is for every organization to have a comprehensive anti-virus system that can respond quickly to new threats.

May 2, 2005—15:58 UTC	IronPort Systems saw an increase in traffic for Sober-N and began to quarantine customer email messages that met the Sober criteria.
May 2, 2005—17:19 UTC	The first signatures were released by traditional anti-virus vendors, and organizations started deploying them. After that, all was quiet for nearly two weeks.
May 14, 2005	Computers installed with Sober-N began "phoning home" to download a Trojan that installed a mass mailing spam engine. The Trojan also began monitoring servers on the Internet to synchronize the computer or server to another time source.
May 15, 2005	The Trojan enabled the coordinated activation of the zombie computers and initiated a massive surge in polymorphic spam.

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