WHITE PAPER

E-Mail and Viruses

Trend Micro, Inc.
Complete Virus Protection for the Enterprise
10101 N. De Anza Blvd., Suite 400
Cupertino, CA 95014

Phone: 1-800-228-5651 / 408-257-1500
Fax: 408-257-2003
Web: www.antivirus.com

March 1998
Trend Micro, Inc.

©1998 by Trend Micro, Inc., 10101 North De Anza Blvd., 4th Floor, Cupertino, CA 95014

All rights reserved. No part of this publication may be reproduced, photocopied, stored on a retrieval system, or transmitted without the prior written consent of the publisher.

ScanMail, InterScan VirusWall, and MacroTrap are trademarks of Trend Micro Inc. All other company and product names are trademarks or registered trademarks of their respective owners.

Table of Contents

ABSTRACT.....4

BACKGROUND.....4

MACRO VIRUSES TAKE ADVANTAGE OF MESSAGING TECHNOLOGIES.....5

ELECTRONIC MESSAGING SEES STEADY GROWTH.....5

PROPRIETARY COMMERCIAL MESSAGING SYSTEMS GAIN POPULARITY.....6

GLOBAL COMPUTING ENVIRONMENT DEMANDS INTERCONNECTIVITY.....6

ALL MESSAGING SYSTEMS ARE VULNERABLE TO VIRUS ATTACK.....7

SERVER-BASED VIRUS PROTECTION PROVIDES MANAGEABILITY, FLEXIBILITY.....8

SCANMAILò WORKS WITH MAIL SERVERS OF PROPRIETARY MESSAGING SYSTEMS..9

TRANSPARENT VIRUS SCANNING.....10
AUTOMATIC VIRUS PATTERN UPDATES.....10
ROBUST ACTIVITY LOG.....10
FLEXIBLE CONFIGURATION AND MANAGEMENT.....10
DECOMPRESSES FILES.....10
INTERSCAN E-MAIL VIRUSWALL.....10
THE TREND MICRO FAMILY OF PRODUCTS.....11

REFERENCES.....12

ABOUT TREND MICRO.....12

Abstract

Commercial proprietary messaging systems have quickly evolved over the last decade to become a core infrastructure and application of collaborative computing. But with increased use of the Internet for collaborative computing comes increased threat of virus attack. In fact, the International Computer Security Association estimates that 80 percent of viruses these days enter networks via the Internet.

Analysts are urging corporations to complement desktop virus protection with server-based solutions that stop viruses before they reach the desktop. All messaging systems work differently, however, which means a "one size fits all" approach to virus protection isn't effective.

Trend Micro's ScanMail is the first solution designed specifically to work with the mail servers of Lotus Notes, Microsoft Exchange, Lotus cc:Mail, Microsoft Mail, and Hewlett-Packard OpenMail. All ScanMail versions provide enterprise-wide, real-time protection from infected e-mail attachments at the Internet gateway, server, and desktop.

Background

We're not there yet, but we're heading toward one vast networked system. Already more people can communicate through electronic mail than any other networked computer application. But although millions can seamlessly send and receive mail regardless of the messaging system on the other side, it's not enough for the electronic messaging community. Its goal is simple: to connect all e-mail systems so that they function together as one network.

According to some estimates, there are over 50 million e-mail users worldwide today, but that figure is probably conservative. Industry reports suggest that annual e-mail user growth rates have not fallen below 35 percent since 1992. (1) And some intranet surveys, which say that e-mail is the leading intranet application, show that there will be 133 million intranet users worldwide by the year 2001. (2) You can count on these numbers growing.

But there's a downside to all this interconnectivity. A computer industry adage perfectly describes the current virus landscape – when you connect to another computer, you link to every machine that computer has ever connected with. Viruses spread via e-mail attachments – already epidemic – are predicted to become pandemic as more and more e-mail users communicate.

The International Computer Security Association (ICSA) quantified the problem in its 1997 Virus Prevalence Survey. According to ICSA, the current likelihood of an organization encountering a computer virus is on the order of 35 virus encounters per 1,000 PCs per month – more than double the 1996 rates. The leading method of transmission? E-mail, of course. (3)

Macro Viruses Take Advantage of Messaging Technologies

No one knows exactly how many viruses exist, due to differences in counting methods used by various individuals and organizations. But it doesn't matter. While there may be many virus types, macro viruses overwhelmingly dominate the scene, accounting for approximately 80 percent of all infections, according to ICSA.

To give an idea of how quickly the virus landscape can change, macro viruses are relatively new creations. From the mid 1980s – when viruses first appeared – until about 1995, boot sector viruses, which infect the master boot record or boot sector on hard disks and are spread only via floppy disk, were the predominant virus type. Then, as people stopped using floppy disks and started sharing files via e-mail, macro viruses quickly took over the lead and have been snowballing since.

"Macro viruses are incredibly successful viruses," says Eva Chen, CTO for Trend Micro, Inc., a leading developer of server-based anti-virus solutions. "They hitch-hike on document and spreadsheet files, so they can travel on floppy disks and across computer networks as e-mail attachments. Then they spread quickly by taking advantage of e-mail, groupware, and Internet traffic."

Specifically, macro viruses conceal themselves in macro commands in documents and primarily infect Microsoft Word and Excel files. When the file is opened, the macro virus can execute any instructions supported by the application's macro language. For example, it can insert random characters, prevent saving the document, or corrupt styles. [4]

This migration of virus distribution from floppy disk to e-mail attachment only mirrors the evolution of technology, and in fact is continuing as Internet use explodes in companies of all sizes. Attention is turning toward future threats, namely Java and ActiveX as the next malicious code carriers. But while it's important for companies to start arming themselves against new threats, virus experts predict – for the foreseeable future – macro viruses will continue to rule.

Electronic Messaging Sees Steady Growth

To consumers, e-mail seemed to come out of the blue. One minute they were on the phone long distance, the next they were sitting at their home computer composing messages. E-mail and Internet usage have not only revolutionized the way people communicate, but also the way they *think* about communicating.

In the corporate world, however, LAN-based electronic messaging has been utilized since the late 1960s. A few proprietary host e-mail systems such as IBM's Professional Office System (PROFS) and DEC's VMSmail were widely used until the early 1990s for facilitating communication between users on the same network. The only problem was that users on these systems were isolated from other messaging systems.

With the popularity of such proprietary messaging systems came a growing awareness within the industry that these systems would eventually need to be connected into an infrastructure and that standards would have to be created. As a result, standards emerged in the mid-to-late 1980s from two sides of the electronic mail environment: the Internet community and the commercial messaging industry. (5)

From the Internet community came Simple Mail Transfer Protocol (SMTP), the Request for Comment (RFC) 822 format, and Domain Name System routing. The commercial messaging industry likewise first developed the X.400 Message Handling System (MHS) and then the X.500 Directory Services standards.

While these standards were being developed, other events would eventually make a great impact on the messaging industry as a whole. The personal computer made its debut in the 1980s, connecting users to public e-mail systems for the first time, and local area networks (LANs) blossomed into wide use.

LAN-based commercial e-mail systems weren't far behind, and by the early 1990s, a burst of these new proprietary messaging systems began permanently changing the way businesses and individuals communicate worldwide. E-mail had moved beyond esoteric data processing environments into the realm of the mass market.

Proprietary Commercial Messaging Systems Gain Popularity

The first popular commercial LAN-based e-mail system was Lotus cc:Mail, which has one of the largest installed bases, with over 11 million users. Although now considered a legacy system, cc:Mail's cross-platform functionality still attracts many large corporate and governmental customers.

Around the time that cc:Mail hit the market in the early 1990s, Microsoft came out with its own LAN-based e-mail system, Microsoft Mail. This legacy system hasn't been as successful as Lotus cc:Mail, but it has paved the way for Microsoft Exchange, a client/server groupware system developed in the mid-1990s with broad messaging and information sharing capabilities.

Exchange offers flexible management options to companies of all sizes and has an installed base of over seven million users. The system competes directly with Lotus Notes/Domino, currently the most popular groupware platform with over 12 million mostly corporate installed users. Also based on modern client/server architecture, Notes offers an ever-widening array of messaging and other options to both users and administrators and continues to compete well against newer systems.

Global Computing Environment Demands Interconnectivity

Against the backdrop of these messaging systems – and many more – the use of e-mail by businesses worldwide is increasing dramatically each year. Between the mid-1980s and the late 1990s – little over a decade – it has grown from being primarily a text-transfer application into an integrated messaging medium for multimedia mail, mail-enabled applications, and electronic commerce. In short, electronic messaging is now a core infrastructure and application of collaborative computing.

On the technical side, however, it's remarkable that many large companies manage to make even internal e-mail connections work. The merger and acquisition mania of the 1980s created a computing environment where it is not unusual for an enterprise today to run its systems on three or four distinct platforms, each with its own brand of e-mail.

For example, a typical Fortune 1000 corporation might be running Lotus cc:Mail, Microsoft Mail or Exchange, and PROFS. Each mail system consists of several servers, and a message switch connects to each system, indirectly connecting all systems. A component of the message switch, the message transfer agent (MTA), pulls the whole jerry-rigged network together by providing SMTP connectivity and direct communication with the Internet. (6) Given this scenario, it's no wonder that once monolithic information systems have become, in the words of some analysts, "architectural chaos." (7)

The problem persists, but in today's global business environment it's imperative that users are electronically available to each other. Internet technologies, and in particular intranets, are bridging communication gaps and facilitating contact between wide webs of businesses. It's no wonder intranets are considered by many analysts to be among the hottest technologies being developed today. In a recent survey, International Data Corp., an information technology research and consulting firm, reported:

"Intranets – private networks based on Internet and Web standards – can be found in a full 59 percent of U.S. and 38 percent of European organizations... Next year (1998), 77 percent of U.S. and 75 percent of European organizations expect to be using intranets. IDC predicts 133 million intranet e-mail users worldwide by the year 2001." (8)

Some companies are making more drastic use of Internet technologies to solve interconnectivity issues. A number of large corporations have actually ripped out their legacy or client/server mail systems altogether in favor of pure Internet mail. Although costly up front, some enterprises have saved significantly over the course of a year by trading features for flexibility and running thousands of users (as opposed to several hundred) per server on TCP/IP-based Internet messaging systems. (9)

All Messaging Systems Are Vulnerable to Virus Attack

In the long-ago days of floppy disks, viruses were more of a nuisance issue in the workplace than a drain on productivity. They spread slowly from floppy to floppy and were rooted out by primitive scanning engines that worked solely at the desktop.

But no messaging system, whether it is LAN-based or built on client/server architecture, is invulnerable to viruses. In fact, messaging systems are especially vulnerable because of what some analysts call the "leak factor." Many companies often use an array of mis-matched anti-virus software that doesn't effectively protect the desktop or the server, causing viruses to "leak" past the network server across the enterprise and often well beyond.

E-mail networks that rely solely on desktop virus protection are probably the most prone to virus leaks for two reasons. First, desktop anti-virus deals only with a copy of the infected file. The original stays at the mail server. If the server isn't protected, the virus can replicate itself into an enterprise-wide infection that could cost a company thousands, if not millions, of dollars in clean-up costs and loss productivity.

And second, virus protection installed on PCs often must be updated manually – a time-consuming and resource-burning endeavor requiring a bevy of IS staff to visit individual PCs throughout the enterprise. With literally thousands of machines to update, it's safe to say that no IS staff can effectively manage desktop virus protection without server protection as well.

Regional offices can have worse problems. If IS staffing is minimal, the resources may not exist to maintain a strong anti-virus strategy at all. Remote users are an additional problem. How can administrators ensure that remote users are protected by anti-virus software when they can't always guarantee that office-based users are fully covered?

Server-based Virus Protection Provides Manageability, Flexibility

As scalability in messaging systems increases, so does vulnerability to virus attack. The reason is in the numbers. More e-mail traffic means increased chances of infected e-mail attachments slipping by the server and landing on the desktops of thousands of users.

Not all anti-virus vendors have been able to keep up to speed with the ever-changing virus landscape. The ones who have, though, are marketing server-based virus protection that gives across-the-board coverage – at the mail server and Internet gateway, as well as the desktop.

Gartner Group, a major information technology research and analysis company, recognizes this trend in its recent report "Maintaining Integrity and Catching Viruses: Effective Malicious Code Management." Gartner predicts that through 2000, "adoption of traditional (desktop) anti-virus products as the primary protection in enterprises will continue, but server-based second-generation products will provide the most reliable additional layer of protection against new threats." (10)

Trend Micro, Inc. was first to market with second-generation virus protection products for many proprietary e-mail and groupware systems, which deviated from the traditional desktop approach to virus protection. Based on a server-centric model, the scan engine blocks viruses at the mail server or router, where viruses are most likely to enter the network. For the first time, administrators can enjoy superior manageability options because they are able to deal with virus protection in the proprietary format of their own messaging system.

"Trying to stop viruses after they've already hit the desktop doesn't make sense anymore. It's 'after the fact,'" explains Trend's CTO Eva Chen. "Trend developed server-based virus protection technology so that companies could stop viruses before they even enter the network. Our experience shows that companies serious about virus protection should be using server-based anti-virus products."

ScanMail® Works with Mail Servers of Proprietary Messaging Systems

Since all messaging systems work differently, a "one size fits all" approach to virus protection isn't effective. Each system has its own proprietary format for storing mail, which requires server solutions tailored specifically for each system.

Trend Micro was the first anti-virus vendor to develop virus protection specifically designed to work with the mail servers of Lotus Notes, Microsoft Exchange, and Lotus cc:Mail. The company has subsequently developed solutions for Microsoft Mail and, most recently, Hewlett-Packard OpenMail.

ScanMail installs on the mail server or router and transparently detects and cleans viruses hidden in both Internet mail and internally circulating mail before infections can reach the desktop. Because ScanMail is server-based, it also can search the databases of old messages to remove existing infections.

Conventional anti-virus products sit at the desktop and react only when the virus has left the messaging system and been transferred to the local hard disk. Scanning occurs only when the user tries to open a mail attachment or save it to the hard drive – sometimes hours or even days after the message is first delivered to the mailbox. This means infected files can be floating around a network for days before the infection is detected and removed.

ScanMail, however, works in real time at the mail server or router, so e-mails with multiple recipients are scanned only once. If a virus is found, a customizable alert message is sent to the administrator, sender, and recipients. The original message isn't delayed; infected files are cleaned automatically and sent on to intended recipients. ScanMail intercepts and blocks mail differently for each messaging system, but the results are the same: ScanMail stops viruses from using any corporate network as a distribution mechanism.

"Since most viruses today are transmitted through messaging, it makes sense to employ a product like Trend Micro's ScanMail because it can stop viruses that travel through proprietary e-mail systems," says Jonathan Penn, an analyst at Ferris Research. "Environments that rely on messaging can no longer afford to be without e-mail virus protection, and Trend's ScanMail… is a smart choice."

ScanMail uses the open standards of the application programming interface (API) supported by each proprietary messaging system. This allows ScanMail to intercept mail, scan it, and send it along without delay on the same data path. Using these standard APIs results in product compatibility, easy maintenance, stability, and high performance.

All ScanMail versions provide enterprise-wide, real-time protection from infected e-mail attachments at the Internet gateway, server, and desktop, and also include the following benefits. (Note that ScanMail for OpenMail has slightly different functionality than other ScanMail products.)

Transparent Virus Scanning

At the heart of ScanMail is Trend's powerful proprietary scanning engine, which uses rule-based and pattern recognition technology to provide detection and removal capabilities for thousands of known computer viruses – including all viruses "in the wild." It also includes Trend Micro's patent-pending MacroTrap™ technology, which detects and removes known and unknown macro viruses.

ScanMail's scanning is transparent unless a virus is detected. ScanMail then sends customizable warning messages to senders, recipients, and administrators and cleans infected files automatically before sending them on to the intended recipients.

Automatic Virus Pattern Updates

Any virus scanner is only as effective as its most recent update, which makes obtaining frequent virus pattern updates critical to maintaining a secure computing environment. ScanMail provides automatic Web-based updating that can be either prescheduled at specific intervals or accessed manually via a one-click function.

Robust Activity Log

ScanMail maintains a comprehensive and robust virus incident activity log, detailing for each infected file, the origin, name and destination of the file, date the file was received, identity of any virus found, and the action taken. It can be configured to respond to virus incidents in several ways: alert the administrator, isolate the infected file for later cleaning or other action, or delete the infected file.

Flexible Configuration and Management

ScanMail can be configured to respond to virus incidents in several ways: alert the administrator, isolate the infected file for later cleaning or other action, or delete the infected file. It also can be set to scan manually or automatically at pre-scheduled intervals depending on requirements. And because ScanMail is installed on the mail server, there is no danger that users can disable mail scanning to sneak unauthorized files past the system.

Decompresses Files

ScanMail decodes UUENCODED and MIMED attachments and decompresses files compressed with PKZIP, ZIP2EXE, ARJ, LZEXE, LZH, PKLITE, and Microsoft Compress.

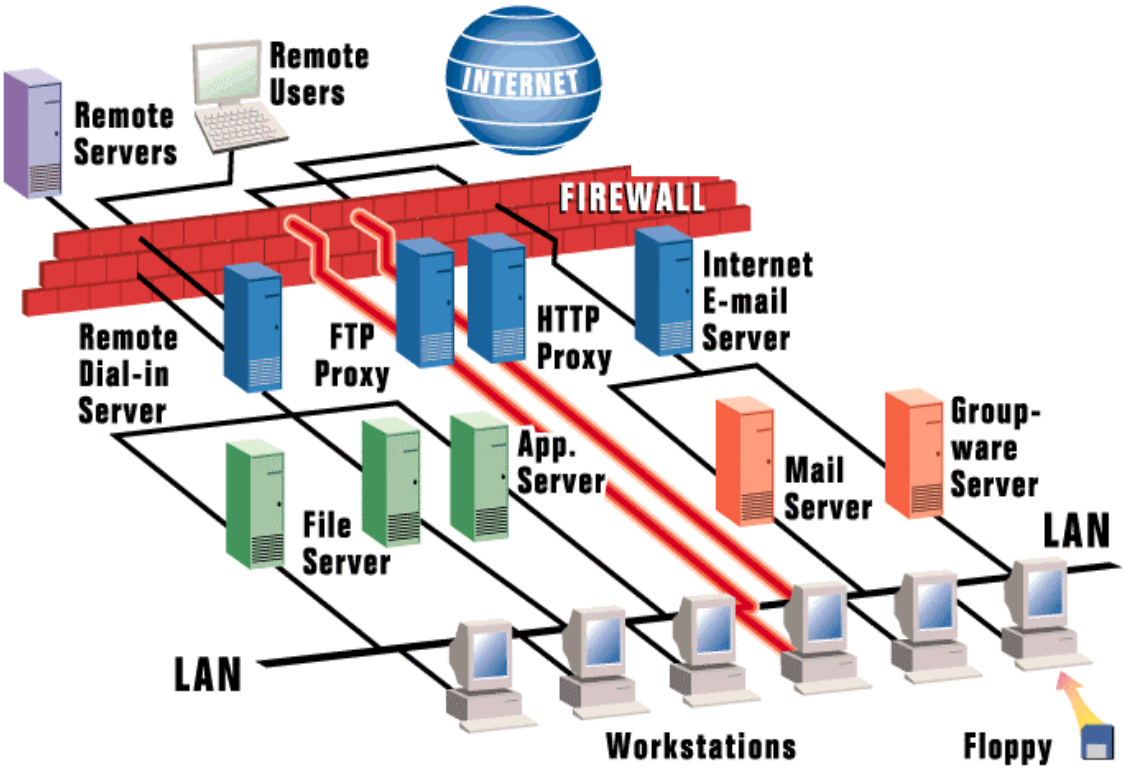
InterScan E-Mail VirusWall

An additional Trend product, InterScan E-Mail VirusWall, works as an integrated component in a three-product suite and detects viruses traveling via inbound and outbound Internet (SMTP) e-mail. E-Mail VirusWall works in tandem with InterScan FTP VirusWall and InterScan Web VirusWall, or can be installed and managed independently.

The Trend Micro Family of Products

Trend's product line is designed to protect all entry points into your network. Trend provides virus protection for:

- Unix and Windows NT-based Internet gateways (InterScan VirusWall)
- Microsoft Exchange, Lotus Notes, Lotus cc:Mail, Microsoft Mail and HP OpenMail e-mail servers (ScanMail)
- Windows NT and Novell NetWare servers (ServerProtect)
- Windows 95, Windows NT, DOS and Windows 3.x desktops (PC-cillin Corporate/OfficeScan Corporate)



References

1. Creative Networks, Inc., "Electronic Messaging Industry Overview," 1997 (www.creative.com)

2. International Computer Security Association, "Virus Prevalence Report," April 1997 (www.icsa.net)

3. International Computer Security Association, "Virus Prevalence Report," April 1997 (www.icsa.net)

4. Trend Micro, "Trapping the World's Most Prevalent Viruses," White Paper, May 1997 (www.antivirus.com)

5. ComputerWorld, "Leave a Message Please: Electronic Messaging Links," Sept. 1, 1997; David H.J. McKenzie, "An Overview of Electronic Mail" (www.computerworld.com)

6. Ferris Research, "Managing Internet Mail," (Report ID 1997 1103RP), November 1997, (www.ferris.com)

7. Creative Networks, Inc., "Electronic Messaging Industry Overview," 1997 (www.creative.com)

8. International Data Corporation, "The Pervasive Planet," (IDC #P14581) 1997 (www.idcresearch.com)

9. ComputerWorld, "Client/Server Mail Under Pressure from Internet Mail Savings," Barb Cole-Gomolski, August 25, 1997 (www.computerworld.com)

10. Gartner Group, Inc. "Maintaining Integrity and Catching Viruses: Effective Malicious Code Management," Strategic Analysis Report, Aug., 1997 (www.gartner.com)

About Trend Micro

Trend Micro, based in Cupertino, California, is the leading developer of high-performance server-based virus protection for corporate networks. Trend Micro technology protects more than 14 million users worldwide and has been chosen by Intel, Netscape, Lotus Softswitch, Sun Microsystems, WorldTalk, Wingra, Oracle, Hewlett-Packard, Control Data Systems, and SCO as a key server security solutions component.

Trend Micro's Web site, http://www.antivirus.com, features the most comprehensive enterprise-level virus protection information available on the Internet. Visit this Web site often for management advice, technology updates, and evaluation copies of all of Trend's products. Additional information about Trend's products can be obtained by sending an e-mail directly to sales@trendmicro.com.