WHITE PAPER
ANTIVIRUS SECURITY

JULY 2003

TREND MICRO, INC.
10101 N. DE ANZA BLVD.
CUPERTINO, CA 95014
T 800.228.5651 / 408.257.1500
F 408.257.2003
WWW.TRENDMICRO.COM

BEYOND LAYERS AND PERIPHERAL ANTIVIRUS SECURITY

TABLE OF CONTENTS

July, 2003
Trend Micro, Inc.

BEYOND LAYERS

Whenever a virus hits, everything shuts down. Power grids go down, cities go dark, chaos ensues. *This is not what really happens.*

People expect a virus to do dramatic and destructive things. They believe that a computer virus is supposed to destroy their hardware or cause something dramatic to happen. But, in general, when a computer virus attack is underway it is invisible and silent. When most viruses accomplish what they were designed to do, you won't even see them. That's because the main job of a virus is to make little copies of itself. Self-replication is the defining characteristic of a computer virus, not destructiveness – or at least not the kind of destruction most of us think of. Anything other than the replication aspect of a virus is actually optional and called the "payload" of the virus.

Not every virus has a payload. Consider the recent SQL Slammer worm virus — it did nothing but replicate. It attempted to replicate itself so rapidly that it clogged the Internet and resulted in a Denial of Service (DoS). The same was true of the Melissa virus, another of the most infamous viruses of our time. While neither of these malicious code threats had a payload, both of them caused damage in other ways.

Regardless of the real or perceived nature of the computer virus threat, people are very aware of them. It is hard to find someone with a computer who doesn't have antivirus software. In many companies, employees can be fired for tampering with the company's antivirus software or for doing anything else that might expose the business to a virus attack.

So it is worth asking the question, "If everyone knows about the threat, and everyone is using antivirus software, how is it that viruses can continue to cause so many problems?" This white paper reviews different aspects of virus behavior, human behavior, and antivirus solutions as they would fit and operate within a typical network, from the Internet gateway down to the desktop. The information shared in this document will help you develop an effective strategy to prevent and respond to the threat of malicious code.

SECURING THE DESKTOP — THE LAST LINE OF DEFENSE

We are all familiar with viruses at the desktop, or laptop, because that's where they are most visible. That is where most of the replication takes place and, typically, where the "payloads" are designed to execute.

Much of this white paper will focus on how to address the inefficiencies of a desktop centered antivirus strategy. For one, most viruses today spread faster than many companies can deploy a solution. For example, when a new virus appears in the world, you may have to send an update that is 200K, 300K or even 1/2MB in size to hundreds or even thousands of desktops. Besides the impact that such a large distribution may have on network bandwidth, the "solution" will likely arrive after many of the systems have already been compromised.

And even though this and other scenarios related to new virus outbreaks are not well addressed through desktop antivirus security solutions, desktop protection remains critical. Based on Trend Micro customer reports, most of the viruses that threatened their systems were older viruses. In fact, 7 of the top 10 virus attacks reported in 2002 were from viruses that had been in existence for over one year!

And with the popularity of laptops, telecommuting, and other aspects of a highly mobile work force, the desktop may be the only option to protect a computer from a virus attack. Therefore, this discussion is in no way meant to imply that desktop antivirus can be neglected. The intent of this white paper is to help you understand the strengths and weaknesses of both the threats and the solutions at various points throughout the network, even when operating remotely.

The desktop remains a potential entry point for viruses coming from various sources: Commercially sold CD-ROMs still, occasionally, ship with a virus on them. And the Internet poses threats from web downloads or even from imbedded ActiveX or Java scripts in web pages that can run quietly in the background while the user surfs the web.

Regardless of the source of infection, the impact viruses can have on a desktop typically falls into three areas: unique data, personal data, and applications.

Unique data can be corrupted or destroyed by a virus and represents one of the primary concerns for businesses today. Executives and other senior managers often have the only copies of reports or other mission critical work on their systems. And many companies have specialists and company recognized "gurus" who are always working on various presentations, reports, or other documents that everyone depends on. If any of these desktop systems were compromised, and the files contained locally within them were destroyed, then the data is likely to be irrecoverable and in some case irreplaceable. Regular backup of this information, perhaps to a network resource, may be the best proactive measure to prepare for this scenario.

Personal data can be as simple as a local copy of company documents, phone lists, presentations, etc. It can be unique compilations of information from other sources as well, or it may be truly personal data that, if corrupted, while an inconvenience to the user, does not represent a serious issue to the company. The only response for the loss or corruption of this data is to recover it from a recent backup and/or to find the originals elsewhere.

Applications are a reasonably descriptive category and, when affected, may require reinstalling one or more of the affected applications. The recovery of a lost application can be a very difficult and cumbersome process that typically requires an IT resource, the source CD, and sometimes a scavenger hunt for the application's serial number. But viruses in recent years have begun to cause other application and system damage by modifying Windows™ .INI files or corrupting the Registries. So the system may require more than just a reinstallation of the application; it may require a completely new installation of everything. If the desktop system is remote, then the situation can become even more complicated.

Computer Economics and the Gartner Group recently conducted independent studies to determine where the lion's share of the money is being spent on network security. They both found that the majority of the expenses related to a virus attack are incurred on the back end of an attack – during the repair efforts. Most of the money is spent on technicians cleaning and repairing infected computers. So it is important to consider your preparations for addressing cleanup and repair when, not if, a system gets infected.

Clearly, desktops cannot be ignored. They require a solid antivirus solution that protects them. Equally important, office desktops must have a manageable antivirus solution that provides real-time status and allows administrators to take immediate action and/or control when necessary. The solution must also be flexible. A recent development for desktop antivirus is the ability to detect when it is or is not connected to the corporate network so that it can automatically adjust its behavior to ensure it continues to maintain itself and provide the appropriate level of protection for each situation.

In addition to providing an ICSA certified solution to detect 100% of viruses in the wild, Trend Micro™ OfficeScan™ supports the Trend Micro Enterprise Protection Strategy at the desktop with two key features specifically designed to address the latest generation of the ever-evolving virus threat. Outbreak Prevention Services is a combination of technology and expertise that enables OfficeScan to block many virus threats before a pattern file update becomes available. When a new virus is discovered to be spreading in the wild, Trend Micro is able to release a policy designed to stop the virus before a more traditional pattern file is available. This small, compact policy could instruct the desktop to temporarily block specific ports, just as a firewall might do. Or it could, for example, prevent files of any specific name from being written to the local hard drive, a technique used by many email viruses as well as the first "Instant Messenger" virus that made headlines in late 2002.

The second, yet perhaps most important feature of OfficeScan is its support for Trend Micro™ Damage Cleanup Services. Some antivirus vendors, including Trend Micro, post standalone utilities that can be used to repair a system from the damage caused by a specific virus. However, IT must then figure out how to deploy the utility, have it properly executed, and then gather information to ensure that it has been used everywhere necessary. Damage Cleanup Services provides an automated method for accomplishing all of this, including real-time reports of which systems have received the Damage Cleanup Template, which ones have successfully used it, as well as which systems are encountering additional problems and need special attention. This helps IT effectively direct limited resources to where they are most needed.
You can visit Trend Micro's web site at www.trendmicro.com for more information on its Enterprise Protection Strategy.

As stated in the opening of this white paper, securing the desktop is a last line of defense. When you're fighting the war to protect your desktop, it is a highly recommended strategy to also setup first line defenses, at the perimeter of the network. If at all possible, you need to keep the virus from ever reaching the desktop by catching it at the firewall, the email servers, and at file and other servers.

ARE YOU "INFECTED" OR "AFFECTED" BY A VIRUS

Before we discuss virus security beyond the desktop, it is important to understand that the primary reason people tend to associate viruses with desktops is because the desktop is where they see the impact of the viruses. We tend to notice that we have been "infected" when the virus starts to "affect" the system. Perhaps data has been deleted, a back door has been opened to allow a hacker access, or system performance or data has in some other way been "affected". This is different than being infected since being "infected" simply means the virus has penetrated the system and can now use it for spreading.

A good case study for the difference between a virus infection and the affects it can have is the Melissa virus. This email borne virus spread from desktop to desktop via email. As soon as a user unwittingly opened the infected email, the virus took control of their system and sent copies of itself to people in their address book. This "affect" was minor, and a one-time event for the user (unless they opened another infected email, which would then repeat the process.) However, Melissa had another "affect" on a system which it never "infected"... the email server. Because Melissa generated so much email traffic, email servers found themselves filling up at a dramatic pace with auto-generated, virus infected emails until many of them ran out of disk space and crashed.

Another way to think of this is that the "affects" of a virus impact the ability to do your work, the "infection" is just an exercise in "how did it get here?"

This is an important point to understand. IT security teams who fail to grasp this concept often end up with "holes" in their virus prevention and response plans. In some cases, even if a virus only infects a single desktop, it could "affect" the reliability and performance of mission critical servers, including email servers, as well as pose a serious risk to data stored on any servers that the desktop has access to.

So when reference is made to a "virus attack", keep in mind that the attack includes the potential to "infect" systems, as well as "affect" them.

STOPPING VIRUSES AT THE EMAIL SERVER

In the fight against viruses, antivirus strategists have made it a priority to include the email server in their defensive periphery. The International Computer Security Association (ICSA) recently published an update to their Virus Prevalence Survey, in which they report that 86% of all viruses can spread through email So it makes sense to review options for securing this virus superhighway first.

And since it is much faster to deploy an update to only a handful of email servers than it is to update hundreds or thousands of desktops, having defenses at the email server can be critical when responding to a new virus threat.

In the most common email virus scenario, the threat enters an email system disguised as legitimate, trusted content. The actual content of the email is just a disguise to deliver the virus. In a number of recent attacks, we have seen viruses that can automatically reply to existing emails, so that they are carried on non-legitimate "copies" of originally legitimate email. So, if you had a legitimate email in your inbox that you had not yet replied to, this virus might have replied to it for you -- but with an added surprise for the recipient.

This example raises one important aspect in calculating the "cost" of a virus attack. What does the above scenario do to your personal credibility with the recipient? What if you could be tracked as the "source" of an infection that caused damage within the network of one of your customers? Any return on investment (ROI) analysis for an antivirus strategy investment needs to include the cost of future lost business due to damage to the image of your company. For some organizations, such as financial or medical organizations, customer trust is the foundation for doing ANY business.

The purpose of many viruses is not to attack the email server, but to invade your email address book and email itself to each address in it. A virus might also find other assets on your desktop and send itself to those as well. When it does that -- when the virus delivers itself to the desktop -- it usually asks you to click on something like a picture or a fake offer and then continues to "spread itself" that way.

Much of the activity needed to get the virus past your defenses, opened, and read/activated is referred to as "social engineering." The virus writer's primary objective might be to get the end user to simply click on a link — which in turn downloads and executes a part of the virus which enables it to spread to others from the end user's system.

If you believe that you can minimize the effect of social engineering by educating your end users, you might want to think again. While Trend Micro is a strong supporter of end user education, end users will continue to make potentially costly mistakes as evidenced by a survey done by the International Data Center (IDC) in February of 2001. Less than one year after the ILOVEYOU virus, and with Melissa and numerous other highly publicized virus attacks still in the news and in water cooler conversations, IDC asked customers if they would open an email with a specific subject line and found the results to be startling (see figure 1 below).

Figure 1.
Source: International Data Center

Subject Heading	Percent of responds who 'open' it
I LOVE YOU	37%
Great Joke	54%
Message	46%
Special Offer	39%
"no title"	40%

The best way to counter a socially engineered virus is to make sure that the virus, and the email that contains it, never even makes it to the end user (i.e. desktop).

A serious misconception held by many organizations is that email virus threats are somehow "Microsoft" exclusive. The truth is that although a virus may be designed to attack through Microsoft™ Outlook™ or some other Microsoft technology, the virus will still pass through an email system regardless of the operating system or email application running on it. So if the objective is to block the virus before it gets to the end user, you have to scan for viruses at every point they may pass through – email systems, Internet gateways, file servers, portals, and so forth.

ISPs regularly survey their subscribers to understand how they use email and the Internet overall. These reports indicate that most business professionals have three or more email addresses, and that they check their non-company email systems while at work. The problem

is that these non-company email accounts are being accessed via the Internet. So keep in mind that even after you go through the effort of securing your email server to protect your business from email-borne (i.e. SMTP) viruses, all of those viruses may still penetrate the company network through the Internet (i.e. HTTP).

To provide a faster response in the event of a new virus outbreak, the Outbreak Prevention Service technology discussed previously in the desktop antivirus section can also be applied to email. For example, if a new virus called "I HATE YOU" came out today, a policy could be put in place quickly to block all emails with the word "I" "HATE" and "YOU" in the subject line. These policies can be manually entered by an IT administrator, or deployed automatically via Trend Micro Control Manager™ which delivers policies developed by TrendLabs™ -- the same global, dedicated virus research team who develops the pattern file and scan engine updates to detect, remove, and clean viruses from infected systems. In 2002, the average time to prepare an Outbreak Prevention Policy was just 18 minutes, far faster than any antivirus company has been able to respond with traditional technologies.

WHAT IS THE EMAIL PERIMETER?

This is not an easy question for some companies to answer. Even if we ignore the threat from end users accessing non-company email systems at work, is it better to place the antivirus solution on the email server itself? Or should it be placed at the gateway to monitor all of the email traffic as it comes in from the Internet as SMTP traffic?

The primary purpose of an email antivirus solution is to scan for viruses as they attempt to enter your email server in real-time. Powerful antivirus solutions exist today to scan email as it enters your network from the Internet as SMTP traffic. An added benefit of these solutions is that they can also address certain kinds of mass mailer viruses, "relay abuse," Denial of Service (DoS), and other attacks that may seriously affect the email system from the outside. But what if the virus arrived before you updated your antivirus solution? Currently, these solutions do not scan the email that has already entered the email storage system.

An antivirus solution tightly integrated with the email system itself, such as Microsoft™ Exchange, Lotus Notes™ or Sendmail™, does provide for the scanning and cleaning of all emails currently in the email storage system including public folders. They also scan the real-time inbound email traffic like their SMTP cousin. Many are integrated using standard methods and Application Programming Interfaces (APIs) provided by the email system manufacturer. This makes them highly stable and reliable. But because they are so tightly integrated, and operate "inside" the email system, they cannot easily address threats such as DoS or relay abuse.

Many organizations reach their security objectives with only one of these two approaches. Indeed there are strategies for dealing with any apparent weaknesses in either one of these approaches, although the strategies vary based on the strength, reliability, and flexibility of the individual antivirus solution.

Trend Micro offers both kinds of solutions through InterScan™ Messaging Security Suite, which is an SMTP scanning solution, and the ScanMail™ product line, which is available for either Microsoft Exchange or Lotus Notes/Domino. Many organizations purchase both, typically as part of an economical suite offering, so they can get the most coverage. In addition to antivirus scanning, InterScan Messaging Security Suite offers industry leading content security capabilities.

Specific strategies for how these can be implemented will not be discussed in this white paper since there are almost infinite varieties in the objectives and priorities that an organization may have. There are also options for implementing email security through a number of appliances that have imbedded Trend Micro antivirus and/or content security solutions. You may contact Trend Micro customer service, a Premier Reseller Partner, or other authorized representatives for assistance.

As a final note of warning about email viruses, a new virus category has evolved in the new millennium called a "mixed-threat" virus, meaning that the virus may carry several "payloads" and multiple methods of spreading. So even if you fully secure the email perimeter, a mixed-threat virus would still have other ways to get in.

PROTECTION AT THE FIREWALL

The firewall's primary purpose is to make sure that the traffic going through it is from/to authorized sources/destinations. In essence, a firewall provides "access" security. But it does not scan "content" for malicious code. As long as an email is properly addressed, or a web page is the one requested by an end user on the network, it's allowed through. Therefore, viruses hidden in email or downloaded from the Internet by an end user on the corporate network can only be addressed by an antivirus solution.

IT typically overlooks gateway virus protection for a number of reasons. Most common is the belief that by securing email servers and desktops, they have covered all the necessary bases. The flaws in this strategy have already been mentioned. For one, most business class computer users have multiple email addresses and they regularly check their non-company email while at work or on their company computer. If only half the employees in your organization do this,

it means that an email scanning solution alone will leave half your systems unprotected from an email virus. And once a single system has been infected, it may spread to other users "internally," bypassing the email antivirus solution in place. It may infect other documents as the user accesses them, including those on file servers, shared document servers, portals, and so forth. Then, other users may become infected as they access files on those shared company resources. Trend Micro was the first company to ever offer HTTP and FTP scanning for viruses, and continues to be the leader in this area. InterScan VirusWall™ scans content as it passes through the firewall, working as either a proxy or leveraging the API standards provided by leading firewall vendors. However, as Internet usage has grown, large businesses are using caching appliances to improve the performance of their Internet gateway. Trend Micro capitalized on this trend and became the first to provide an antivirus solution that supports the Internet Content Adaptation Protocol (ICAP) API for integrating with these appliances. The result is a solution that is five times faster than a non-cache integrated solution.

STOPPING VIRUSES AT THE FILE SERVER

Of course, there are viruses that both infect and affect servers directly. But many IT security personnel fail to understand the full impact of this fact. They install email antivirus software to scan for potential threats within the email system itself but fail to notice that the email system is running on a "server," which could be directly attacked (i.e. infected or affected) by a virus in many other ways.

Servers serve a variety of functions, most of which are mission critical or related to the company's intellectual property. A server is typically where your company assets reside; including accounting information, customer lists, contracts, projects currently in the works, email systems, manufacturing information, and so forth. And that doesn't even take into account all of the applications that your business has come to depend on for daily operations.

While most users on the network do not have access to the actual email server, only their email on the email server, there are those in IT who occasionally operate on the network with high levels of access. If they were to visit someone with an infected system (knowing only that it was behaving "weird", not that it was infected) they might log on with their administrative privileges to investigate a problem and unwittingly give the virus free reign of the system.

The recent Slammer worm is a good example. It was actually designed to travel only from SQL Server to SQL Server. Nimda and CodeRed were also both designed with specialized code to penetrate and attack different kinds of gateway servers (among other things that were less publicized).

It is worthwhile at this point to recall that the operating system involved may or may not have a lot to do with the threat posed by a virus. If you are using a Linux server for a file server, a Solaris system for your Internet gateway, and an AS/400 or S390 mainframe for you email system, a virus still poses a real and substantial threat to the data either stored or passing through those systems.

However, many IT security plans often focus too much on the potential loss of irreplaceable data. Admittedly this is anything but negligible, but business interruption costs can quickly swell to a level sufficient to actually drive a business to bankruptcy. Business Contingency Planners, Disaster Recovery Planners, and others in the disaster recovery industry deal with this regularly. And since "interruptions" occur more often than "total loss," it would not be appropriate to spend too much time on "total loss." IT departments are well aware of how much every hour of email downtime can cost their company. But, other than the email case, they often fail to understand the business interruption potential from a virus attack.

In the end, IT security planners must look at every system and decide:
- How do we protect the content on this system?
- How do we protect the content passing through this system?

SECURING BEYOND THE NETWORK – EDUCATION

IT, employee and public education are needed to avoid problems due to a lack of understanding. There is no need to disconnect the email server from the Internet every time there is a rumor of a new virus. There is no need to reformat the hard drive if a desktop is infected. Many people, believe it or not, still believe that a virus can overload the circuits and make smoke and fire pour out of the back of their computer. And, since most viruses do not actually cause damage, much of the cost to business may come from over-reaction to the threat, rather than from the threat itself.

What is most at risk during a virus attack is data. Data is the main target of virus writers. In Future Shock, Allen Toffler says that our emotional intelligence has not yet caught up with the world we live in. Information is property and needs to be protected. Users must be taught to stop and think before they put their name and address on that sign-up sheet, respond to that urgent letter from a potentially rich heir in Nigeria, or click on a link in an email that promises to show scandalous pictures of Anna Kournikova. The Internet is not all that different from the world we live in, and valuable property exposed to the Internet needs to be locked up and securely protected.

Viruses are a very cheap fraud, but they're also very common. They're like graffiti or vandalism in most cases. They can be serious threats and should be treated as such to maintain privacy, security and safety, as well as the data that's in your computer and on your network.

STRATEGIES, NOT PRODUCTS

All of this information is meant to help you consider how your end users work, how they share information, and how email and other information travels through your network. With this understanding, you should be able to develop a plan for what solutions need to be put in place, where they need to go, and how you will be able to manage them. It should also help you avoid the common pitfalls that Trend Micro has seen since we began operations in 1988. As one of the oldest, largest, and most respected antivirus providers for corporate America and the world, we are the leaders in this field and have secured more gateways, email systems, and file servers than almost any other antivirus company.

APPENDIX A:

ABOUT DAVID PERRY

As Trend Micro's Public Education Director, Perry brings more than 25 years of experience in technical education and technical support to Trend Micro, particularly in virus and security-related fields. At Peter Norton Computing (now Symantec), McAfee Inc. (now Network Associates), and Cybermedia, Mr. Perry helped tens of thousands of individuals and corporations to recover from virus and hostile code attacks. At Trend Micro, David Perry continues to educate network administrators, computer users and the public at large about computer viruses and how to protect systems from them. "Technology can only win half the battle against computer viruses," said David Perry. "The other half will be won with user education."

ABOUT BOB HANSMANN

As Trend Micro's Director of Product Marketing for North America, Mr. Hansmann adds his 22 years of computer security and disaster recovery planning expertise, along with 8 years in the antivirus industry, to Trend Micro's team effort to understand the threats of tomorrow. In addition to representing the North American security needs, working with counterparts in Europe and the Asia Pacific region, he presents globally on how to minimize the impact of a disaster on an organization, and new strategies for dealing with the threats from malicious mobile code, including viruses. He specialized in analyzing the threats of new technologies, such as wireless, and the current overlap and integration of different but merging security technologies including antivirus, content security, and Spam.

APPENDIX B:

ABOUT TREND MICRO, INC.

Trend Micro provides centrally controlled server-based virus protection and content-filtering products and services. By protecting information that flows through Internet gateways, email servers, and file servers, Trend Micro allows companies and managed service providers worldwide to stop viruses and other malicious code from a central point before these threats ever reach the desktop.

Trend Micro's corporate headquarters are located in Tokyo, Japan, with business units in North and South America, Europe, Asia, and Australia. Trend Micro's North American headquarters are located in Cupertino, California. Trend Micro's products are sold directly and through a network of corporate, value-added resellers and managed service providers.

Evaluation copies of all Trend Micro products may be downloaded from Trend Micro's Web site, http://www.trendmicro.com.