



This E-Book is brought to you by **Gas4Free** Technologies at TripleGasMileage.com
Download Powerful **Top Secret Water Car Hybrid Technology** eBooks
and Convert Your Car to **Burn Water + Gasoline** Today!

Detecting and Eliminating Computer Viruses at the Gateway

By CIPHERTrust

Detecting and Eliminating Computer Viruses at the Gateway by CIPHERTrust

Traditional anti-virus software only stops known computer viruses - stopping undefined computer viruses requires a different approach.

In the past, network administrators scrambled to apply new virus signatures whenever new computer viruses were discovered. While these signatures will stop a known threat, it takes time for anti-virus vendors to develop them. Unfortunately, the newest and most damaging viruses are able to spread so quickly that the damage is done before a signature can be developed and distributed.

In fact, the independent testing laboratory AV-test.org found the response times for major anti-virus software publishers to range from just under 7 hours to almost 30 hours, with the four leading vendors (Sophos, McAfee, Symantec and Trend Micro) clocking in at no less than 12 hours.

In January 2004, the computer virus known as "MyDoom" created mass disruption to corporate resources and reputations as it quickly spread through e-mail networks worldwide. At its peak, MyDoom infected one in every five e-mails transmitted over the Internet. The worm broke records set by previous malware, such as Sobig.F, to become the fastest-spreading virus ever. This incredible propagation speed left many networks vulnerable - despite the presence of anti-virus software - because of the lag time between when the virus outbreak began, and when a virus definition became available.

As a result of recent malware threats, corporations and organizations have learned a painful but important lesson: simply deploying a signature-based solution is no longer enough. Detecting and eliminating computer viruses requires a multi-faceted, rapid-response approach that traditional

Detecting and Eliminating Computer Viruses at the Gateway

anti-virus protection cannot provide. Even a single unprotected computer on an enterprise network can bring down the entire system in just minutes, rendering even the most expensive and up-to-date software useless.

Why E-Mail is Particularly Susceptible

In many organizations, e-mail has replaced the telephone as the most useful business tool available. Unfortunately, e-mail has also been a victim of its own success and presents a unique threat to the enterprise network as a whole.

Detecting and eliminating threats has traditionally been the combined responsibility of firewalls, virus scanners, and intrusion detection systems (IDS) set up by enterprises to defend against attacks. Firewalls prevent unauthorized programs from accessing the network, virus scanners scan each PC in the network for malicious code, and gateway servers lock down extraneous ports to protect against unauthorized access.

But key Internet-facing applications, including e-mail are unguarded by firewalls. In order to function, e-mail must expose firewall ports, including port 25, the port used by SMTP (Simple Mail Transfer Protocol) and port 110, the port used by POP (Post Office Protocol).

When a firewall receives a connection on port 25, it generally assumes that the transmission is e-mail and allows it to flow through to the e-mail server. The transmission may very well be a valid e-mail; however, it could also be a virus, spam or something much worse. Firewalls are not able to distinguish between "good" mail and "bad" mail and therefore they are unable to protect the e-mail application.

Stop E-Mail Threats at the Gateway

Therefore, some sort of protection is needed specifically for e-mail and, since the best place to stop a threat is before it gets inside the network, the protection should be at the e-mail gateway. Protecting the e-mail gateway requires a coordinated effort to combat a host of issues, including spam, viruses, corporate policy infringements, directory harvest attacks, denial of service attacks, phishing, spoofing, and snooping. As e-mail threats evolve, the distinction between each of these types of threats becomes blurred.

Furthermore, accuracy in identifying "bad" e-mails is crucial. Extreme care must be taken to avoid filtering out legitimate e-mails (false positives), which could contain important information from customers or partners.

Historically, enterprises have turned to multiple vendors to solve their e-mail security issues. They have relied on anti-virus vendors to protect them from viruses. They use a separate anti-spam vendor to help cut back on the spam. Then, there are the issues of content filtering, policy enforcement, encryption, and network security. Unfortunately, attackers are now highly adept at exploiting these non-integrated solutions. This "Swiss cheese" defense has not only been costly, but increasingly ineffective at protecting corporate email systems.

Computer Virus Risks

Recent attacks from various types of computer viruses and worms have had profound effects on computer systems around the world. Enterprises have been brought to their knees and forced to spend billions of dollars cleaning up the mess and rebuilding their infrastructures. While the increased IT costs are clear, there are other risks corporations face with regard to e-mail borne viruses.

The No-Brainer Computer Network

System Downtime

E-mail has evolved to be the primary communication tool for most organizations and the loss of e-mail due to attack can severely affect enterprise operations. Beyond the immediate expenses involved in restoring the network, an attack on your enterprise e-mail system can also result in lost hours and days for employees who have come to rely on it to accomplish their daily tasks.

Resource Depletion

The costs of cleaning up after an attack are significant. IT teams are forced to spend considerable time and money repairing virus damage. The damage, however, is rarely contained to network servers. Once inside the network, viruses can quickly infect large numbers of relatively exposed client machines – all of which must be individually cleaned, patched and repaired.

Administration

In the past, when a new vulnerability was discovered, network administrators scrambled to apply security patches from the makers of their anti-virus software and manually reviewed quarantine lists for virus-infected messages. Software manufacturers release patches so frequently that network administrators cannot reasonably be expected to keep up with them all. As stated by Gartner Research, "Enterprises will never be able to patch quickly enough. After all, attackers have nothing else to do." The staggering damage caused by recent computer viruses and malware attacks is clear evidence that manual intervention to institute emergency measures or review quarantined messages is rarely effective against rapidly propagating threats.

Compliance and Liability

Recent Federal regulations such as the Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA) and Sarbanes-Oxley Act (SoX), require enterprises to protect data residing in mail servers and other internal systems. Security breaches violate these regulations, exposing sensitive data and opening the door to serious sanctions and costly litigation.

Credibility

Falling victim to a virus attack can also result in lost trust from business partners and customers. According to Gartner, "Enterprises that spread viruses, worms, spam and denial-of-service attacks will

find not only that malicious software can hinder their profitability, but also that other businesses will disconnect from them if they are considered to be risky." While an attack may not be your fault, it is most certainly your problem.

The Solution

Although signature-based anti-virus systems are inadequate to preventing virus attacks in the first few hours or days of an outbreak, it is possible to identify outbreaks before they infiltrate your

organization's network and become a problem. In fact, doing so successfully requires tight integration of several different technologies designed to analyze mail based on many different characteristics. One of the most innovative and important technologies for meeting these threats is known as Anomaly Detection.

Large-scale virus outbreaks create anomalies in mail flow which are identifiable by the message content, source, volume, attachment or any of a number of other indicators. When a particular message appears to be a part of a sudden surge of anomalous messages moving across the internet, the message can be quarantined until virus definitions can be developed to address the new threat.

Anomaly Detection

CipherTrust's IronMail utilizes a unique Anomaly Detection Engine (ADE), which dynamically identifies and responds to abnormal behavior in mail flow. By monitoring "normal" e-mail traffic rates across the Internet, the ADE allows IronMail to identify spikes in traffic that are often the first signal of a malicious attack. Once these spikes are recognized, IronMail units take appropriate action to prevent infiltration of the network.

CipherTrust is the leader in anti-spam and email security. Learn more by downloading our free whitepaper, "

" or

by visiting

.

Traditional Antivirus Programs Useless Against New Unidentified Viruses!

By Jason Frovich

Traditional Antivirus Programs Useless Against New Unidentified Viruses!

Copyright © 2005 Jason Frovich, All Rights Reserved Support Cave

Detecting and Eliminating Computer Viruses at the Gateway

Most traditional antivirus programs rely on their database. Potentially hazardous files are matched against the database to see whether they are to be considered safe or not. Since a new virus can spread world wide within a few hours it can cause severe damage to your computer long before the manufacturer of the antivirus program identifies the virus and updates the database. You also need to go online to import the manufacturers' database to you antivirus program, which means that your computer will be online totally unprotected. The new Panda Titanium Active Scan Anti Virus 2005 however, contains TruPrevent Technologies: a new system designed to protect your computer against unknown viruses and intruders.

Every now and then you can read about a new virus and the damage it causes. The millions of viruses cost companies each time they strike. It is however not only companies that are suffering from the damages caused by viruses. A virus can be just as damaging if not more for a private Internet user by destroying important documents, family pictures and everything else you keep on your computer. Therefore should no home computer be without a good virus protection software. This way you can protect your computer and yourself from losing data, corrupted hard drives and a number of other problems. There are several anti virus programs available of which some are free and some are not. You should however always remember that you might get what you paying for, meaning that the service and the updates might be better for the paid alternatives and thereby protect your computer better.

When using a virus program you should try to find one that is fast, reliable and able to discover as many viruses as possible. Whether it is fast or not might seem unimportant if you don't use your computer that much, but you will find that an anti virus program that scans your computer faster will be used more frequently and thereby giving you a better protection. If an anti virus program should be effective when protecting your computer it needs to be able to recognise all viruses, and since new viruses are constantly created this means that the database for the program has to be constantly updated. You should therefore consider how often the different anti virus programs update their databases when choosing which antivirus program to get. You should always make sure to keep your virus program up-to-date.

One of the best anti virus programs on the market today is Panda Active Scan Anti Virus Software Online which has an unrivalled capacity for detecting viruses and other threats online which is the most common path for viruses to reach our computer. Almost all viruses today are spread through the Internet. Panda Titanium Active Scan Anti Virus 2005 is easy to install and once it is installed it finds and remove viruses automatically. Panda Titanium Active Scan Anti Virus 2005 also automatically updates itself if you want it to. In other words: Panda Anti Virus is an anti virus program that manages itself and makes sure that it is up to date and able to keep your computer safe from viruses. Panda Titanium Active Scan Anti Virus 2005 scans your entire computer, including the program itself, to make sure that a virus can't infect any part of the computer. Panda Titanium Active Scan Anti Virus 2005 doesn't just search for virus, it also search your computer for a number of other security risks like spy wares and Trojans.

Panda Titanium Active Scan Anti Virus 2005 contains TruPrevent Technologies. TruPrevent Technologies is a system designed to help Panda Anti Virus protect your computer against unknown

Detecting and Eliminating Computer Viruses at the Gateway

viruses and intruders. The user can choose whether they want to use TruPrevent Technologies or not. The technology has been implemented to allow Panda Anti Virus to protect your computer against new virus since a new virus can spread world wide within a few hours. The TruPrevent Technologies allows Panda Anti Virus to detect and block viruses even if they are not yet included in the virus database. This allows Panda Titanium Active Scan Anti Virus 2005 to keep your computer safe against all viruses and not only the ones that are already identified, since you might encounter a new virus despite the fact that Panda updates their database at least once a day. Old anti virus programs – and most of the modern anti virus programs as well – can only protect you against already identified viruses. The ability to protect against unknown viruses is what Panda Titanium Active Scan Anti Virus 2005 a superior choice for an anti virus program.

Panda Titanium Active Scan Anti Virus 2005 does not only offer superior security and very user friendly functionality. It also comes with tech support where experts answer any questions that might arise.

All personal computers should have virus protection since you otherwise risk losing important document, family pictures etcetera and if you are looking for user friendliness and a superior security Panda Titanium Active Scan Anti Virus 2005 is your best choice.

You can get panda antivirus at support cave.

Supportcave.com offers new and enhanced free Anti Virus Remover Software. Not only will these programs effectively check and clean your computer from Spyware, once installed they will also shield your computer from future Spyware intrusions and browser hijacks – before the malevolent software even have a chance to enter you PC! Anti Virus Remover Software is an important function all computer users should rely on to ensure their computer is free from nosey software and their privacy protected.

Traditional Antivirus Programs Useless Against New Unidentified Viruses!

No Operating System

Dirty Little Computer Viruses and How To Protect Yourself

Free Program Removes Spyware not Detected by Premium Security Scan

How To Keep Your Computer Virus Free

Newbie's Guide to Stop Spam

Tame Your Personal Computer

Super Charged Linking

Stretch Assistant Software

File Resource Meter Software

ReBrand this PDF eBook with your Name / URL / ClickBank Affiliate ID for Free



This E-Book has been brought to you by **Gas4Free** Technologies at TripleGasMileage.com
Download Powerful **Top Secret Water Car Hybrid Technology** eBooks
and Convert Your Car to **Burn Water + Gasoline** Today!

