

Traditional antivirus software unable to thwart Sasser threat Network VirusWall Helps Acer Stop Sasser Attack

The Sasser attack on May 1, 2004 targeted not only servers but also individual users, causing anyone who did not install security updates promptly to become an outbreak liability. Any employees who brought laptop computers into their office after the holiday on May 1 posed another potential threat to their company network.

Although Sasser did not spread through email as with most viruses, the speed and extent at which it spread was sufficient cause for alarm. Sasser exploited a Microsoft Windows vulnerability that gave a hacker complete remote control of any infected computer, and like the Blaster virus before it, it had the potential to cause extremely significant damage across the Internet.

Traditional antivirus software uses a "blacklist" method of collecting virus patterns and matching them with suspected files on a computer's hard disk. However, the speed at which today's viruses spread makes the process of developing a pattern file and updating each computer individually too slow to keep up.

Also, using traditional antivirus software, administrators are often powerless to stop many of the Trojan or Backdoor programs associated with modern network viruses. The reason for this is that antivirus programs only scan and clean infected files stored on hard drives – they are unable to clean Trojans or Backdoor programs resident in memory or restore altered registry settings. Even after the virus has been cleaned, the malware it leaves behind is often much more difficult to completely eradicate.

When the latest Sasser virus outbreak occurred, Acer Group was prepared. What does Acer use to protect its corporate networks from virus outbreaks?

The answer is Trend Micro Network VirusWall™. Network VirusWall™ is an outbreak prevention appliance that helps organizations stop network viruses like Internet worms, block high threat vulnerabilities during outbreaks, and quarantine and clean up infection sources including unprotected devices as they enter the network, using threat specific knowledge from Trend Micro deployed at the network layer.

Acer Group CIO Eric Lee said, "There are many antivirus solutions on the market with essentially similar features. In the past we had to wait on new pattern files to be released and then install them on each and every computer to be sure we were protected. But now, with the growth of the Internet, every computer is connected and viruses are spreading so fast it is impossible to keep up."

Trend Micro™ Network VirusWall™ is an outbreak prevention appliance that helps organizations stop network viruses (Internet worms), block high threat vulnerabilities during outbreaks, and quarantine and clean-up infection sources including unprotected devices using threat-specific knowledge from Trend Micro deployed at the network layer, to help reduce security risk, network downtime, and outbreak management burden.



Traditional antivirus software unable to thwart Sasser threat Network VirusWall Helps Acer Stop Sasser Attack

Lee continued, "For a supplier like Acer who operates 24 hours a day, if even one region is attacked, the entire network could be infected within five minutes. Therefore, what we needed was a way to reduce the scope of damage. From our many years of battling with viruses, Acer knows that it is impossible to be completely safe from virus attacks. But what we can do is limit the damage they do when they do sneak in. What we needed was a way to instantly isolate infected regions from the rest of the network."

A means of protecting corporate networks during an outbreak, but before pattern files have all been updated, a solution that provides outbreak status monitoring, and a method for completely rooting out the remnants left behind are sorely needed.

Network VirusWall™ works by instantly and automatically scanning data packets for viruses at the network layer to prevent viruses from spreading. The major features include:

- Scans entire network for system vulnerabilities, and restricts access by vulnerable machines.
- Automatically deploys security policies and prevents easily attacked machines from accessing the Internet.
- Prevents virus attack and spread directly on the network device level.
- Automatic Damage Cleanup Service provides effective recovery for the entire network.
- Detects and prevents Internet viruses.
- Instantly restricts individual machines from accessing the Internet.
- Instantly conducts cleanup and system restoration of affected machines.

Another benefit of Network VirusWall™ is protection from other computers who occasionally enter the network. Companies often receive visitors who bring laptop computers into the office and connect to the LAN.

Traditionally, these visitors were a major security issue because companies had no way of forcing them to install antivirus software or scanning each visitor's computer before they connected to the network. As soon as the visitor's notebook connected to the LAN, it could begin spreading viruses throughout the company.

With Network VirusWall™, companies can now restrict visitor access to a designated network segment, use Network VirusWall™ to isolate and protect that segment, and prevent visitors from infecting the entire network. Not only is the corporate LAN protected, but also the company's reputation is protected from unwittingly infecting important customer's or potential partner's computers.

For more information on network virus prevention, please see: www.trendmicro.com

TRENDLABS™

Trend Micro products are backed by timely, high-quality service from TrendLabs, a global network of five regional antivirus research and support centers with an ISO9001:2000-certified and COPC standards-certified headquarters. A team of more than 300 engineers and antivirus specialists operate around the clock to monitor virus activity, develop information on new threats, and deliver prompt, effective strategies.

For more information about Trend Micro service and support, contact TrendLabs at www.trendmicro.com/trendlabs.

TREND MICRO, INC.

Trend Micro, Inc. is a global leader in network antivirus and Internet content security software and services. The company led the migration of virus protection from the desktop to the network server and the Internet gateway, gaining a reputation for vision and technological innovation.

Today, Trend Micro focuses on providing customers with comprehensive security strategies to manage the impacts of known and unknown threats to information, through such initiatives as Trend Micro Enterprise Protection Strategy. Headquartered in Tokyo, Japan, Trend Micro has grown to over 1,800 employees in 25 countries, with stock traded on the Tokyo Stock Exchange and NASDAQ.



TREND MICRO INCORPORATED

10101 N. De Anza Blvd.
Cupertino, CA, 95014, USA
toll free: 1+800-228-5651
phone: 1+408-257-1500
fax: 1+408-257-2003

www.trendmicro.com