

I need  
complete network security  
that's affordable....  
and  
I needed it yesterday.

# Malicious Software Defense:

Have we moved beyond the need for anti-virus and spyware protection software?

Kevin Prince  
Chief Security Officer  
Perimeter eSecurity  
May 2007



Complete. On Demand. Affordable.

## Introduction

With the decrease in the total number of viruses, some have theorized that the need for virus protection is becoming less and less necessary. Protecting systems such as servers and workstations is nothing new. In fact, using anti-virus software was the first method enlisted to stop malicious code from infecting and propagating between these systems. However, the sophistication of viruses and malware in recent years has dramatically changed the playing field. The purpose of this paper is to help individuals understand the scope of the problem, and specific strategies available to combat this continually changing threat.

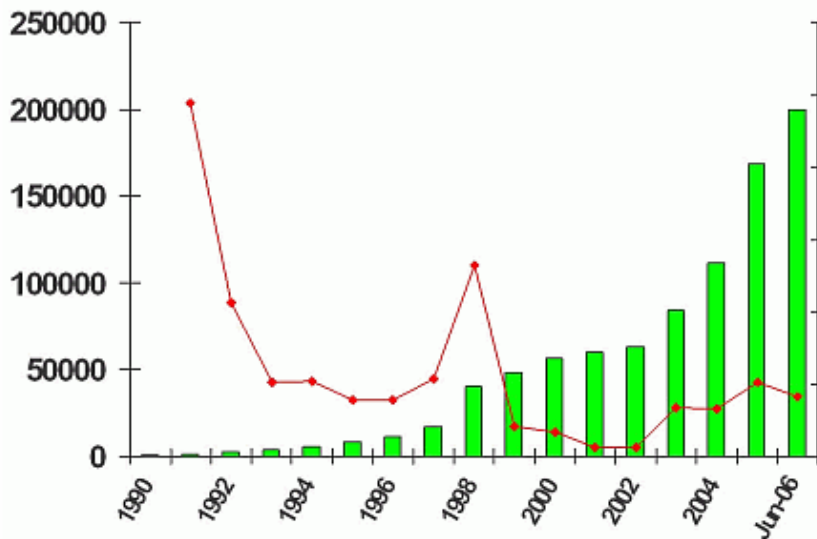
## History

A program called "Elk Cloner" is credited with being the first computer virus to appear "in the wild" — that is, outside the single computer or lab where it was created. Written in 1982 by Rich Skrenta, it attached itself to the Apple DOS 3.3 operating system and spread by floppy disk. The first PC virus was a boot sector virus called (c)Brain, created in 1986 by two brothers, Basit and Amjad Farooq Alvi, operating out of Lahore, Pakistan. The brothers reportedly created the virus to deter pirated copies of software they had written.

In the early 90's, companies such as IBM, McAfee, and Symantec released the first software to protect systems from these infections. As networks began to emerge, these viruses could spread between systems without the use of removable media. This same concept was then used at a macro level with the adoption of the Internet in the 1990's. Since that time, thousands of viruses have been released into "the wild" with many stories and data casualties. Few individuals have not been touched by the tentacles of a virus at one time or another.

The software used to detect and stop these viruses was installed directly on the system it was intended to protect. Other strategies such as Gateway Anti-Virus has also been used in recent years to detect and stop viruses before they enter a network, but these systems were never intended, and shouldn't be used as a replacement for anti-virus software that resides on the individual systems.

### Malware Growth vs. Virus Decrease



### Malware Count and Rate of Growth

<http://www.avertlabs.com/research/blog/?cat=2>

Later, other malicious code was written that had slightly different properties from a virus. A computer worm (one such example) is a self-replicating computer program. It uses a network to send copies of itself to other nodes (computer terminals on the network) and it may do so without any user intervention. Unlike a virus, it does not need to attach itself to an existing program. Worms always harm the network (if only by consuming bandwidth), whereas viruses always infect or corrupt files on a targeted computer. The name 'WORM' comes from *The Shockwave Rider*, a science fiction novel published in 1975 by John Brunner. Researchers John F Shoch and Jon A Hupp of Xerox PARC chose the name in a paper published in 1982; *The Worm Programs*, Comm ACM, 25(3):172-180, 1982), and it has since been widely adopted. Though it was technically a Trojan horse, the Christmas Tree EXEC Worm was likely the first worm on a worldwide network, spreading across both IBM's own international network and BITNET in December 1987, bringing both networks to their knees.

Other malicious programs created further variation. Trojan horse programs, spyware, and adware are just a few examples. Often times, any software that is installed on a system without the owners informed consent is known as malicious software, or "malware". Although other terms such as scamware, crimeware, and badware are used to describe similar types of software, malware at this time seems to be the most dominant.

## Trojan Horse Programs



2. Increase in TrojWare.

<http://www.viruslist.com/en/analysis?pubid=178949694>

## Spiraling out of Control

Recently there have been some major shifts in the use of malware. Prior to 2006, most viruses and worms could be classified as things that the author or developer wanted everyone to know about. The recognition for writing the “fastest spreading worm”, or “most damaging virus”, etc. was one of the major reasons this software was written. This movement has almost completely shifted from bravado, testosterone driven, alpha male behavior to financially motivated. Most of these tactics are now used in combination with other attack types to commit fraud and identity theft.

Malware has been a key ingredient for those who wish to commit crime ever since the major security shift brought about by Microsoft Windows XP service pack 2. Most people remember this time in late 2004 when many of their applications stopped working. What happened is that Windows XP SP2 now had a built-in firewall that was enabled by default blocking inbound connections. Prior to this time, connections were relatively easy to make to a remote system. Prior to XP SP2, a hacker, virus or worm would simply attempt to compromise a system through a direct connection. With the system based firewall now installed, the hackers would find alternative methods of getting to those highly coveted systems. The malware that came out subsequent to XP SP2 was designed to make outbound connections back to the attacker rather than inbound connections. Everything from viruses and worms to malware web sites and Trojan horse programs were used to compromise the systems. This updated malware was often designed to allow full remote control of the system by the attacker; and because the infected system can create an outbound connection back to the attacker, most traditional network based security systems can be averted. These infected systems are referred to as zombies, or systems that are under the control of another. These zombie systems are often collected as part of a botnet army to be used in a variety of attacks.

Worse yet, in the “old days” (a few years ago), you knew right when your system was infected. Your processor would be pegged at 100%, the hard drive light would be going crazy, you would have difficulty opening up programs and doing any work. Now, the malware is often written in such a way that it is very difficult to detect. Often special software or network analyzer tools would have to be employed to see malicious activity from an infected system.

## Sources of Malware

Traditionally, an infection from malware would be from opening malicious email that contained a virus or Trojan horse. Later there were more self-propagating worms. Today, malware can infect systems from any number of sources including the Internet, partner connections, virtual private networks for remote users and site-to-site connections, USB drives and other media, malicious web sites and more.

## Risk Reduction Strategies

As all security professionals will tell you, there is no silver bullet to the threats of malware. There are, however, some very good security best practices that can drastically reduce the overall exposure your organization has to malware. A good layered security practice would include many of these:

System Anti-Virus & Spyware – host based software designed to detect and stop malicious code from infecting the system

Web content filtering (aka URL content filtering) – disallow your employees from accessing malicious web sites.

Patch management – often, a known bug is exploited to infect the system. Patching systems for known vulnerabilities can reduce the number of targeted exploits on any given system.

IDS/IPS – both network based, as well as host based, intrusion detection systems (NIDS/HIDS) can detect some malicious code attacks. Employing this technology with a prevention component can stop these identified attacks in their tracks.

Firewall – a solid stateful inspection firewall with strong rules and policies.

Gateway Anti-Virus – a network based anti-virus system detecting viruses before they enter the network. These systems can often detect viruses coming from web based email systems.

SPAM filtering – block email messages that may contain malicious content, or links that lead to malicious web sites. This should take into account email messages designed for phishing attacks.

Policies & Procedures – Any good security practice should include enforceable policies and procedures that are well defined and available to all personnel.

End user training – All employees should undergo some level of security awareness training.

The remainder of this paper will focus on the first from the list above. System Anti-Virus & Spyware system are often taken for granted these days. Everyone relies on basic AV software and assumes it is always doing its job. Unfortunately, this assumption can often come back to bite network administrators.

## The Problem with Traditional AV Software

Users that have the ability to load new software on their system may find that some software conflicts with anti-virus or spyware software and can cause their protection software to become ineffective. This can sometimes occur without the user ever knowing or even seeing a warning message of any kind.

Software and scanning engine updates are a necessity to keep the software up-to-date to identify the most recent viruses and spyware. All-to-often the software does not get updated as it should. Sometimes the software is setup to manually update, which doesn't occur. Other times it is scheduled to do updates ever night at 8:00pm, yet the user turns off the computer at 5:00pm each night as they leave the office. Licenses may expire which prevent updates. There are just a few examples of ways in which the software becomes less effective and creates increased exposure to malware.

Zero Day attacks are becoming more and more common. This is when malware of some kind is released in the wild, and an update to the anti-virus software is not yet available. This exposure to new attacks is often one-of-the-most dangerous and lethal.

Lack of holistic network management is a leading cause of malicious code infections. Network managers need to be able to review their network as a whole. IT staff need to quickly identify which systems do not have system AV and spyware software loaded, or where the current software is out-of-date. These same network managers need a console by which they can audit their system AV and spyware deployment against the company policies and procedures. Reduced detection methods can also lead to exploit. There are two common methods that an anti-virus software application uses to detect viruses. The first, and by far the most common method of virus detection is using a list of virus signature definitions. The disadvantage of this detection method is that users are only protected from viruses that pre-date their last virus definition update. The second method is to use a heuristic algorithm to find viruses based on common behaviors. This method has the ability to detect viruses that anti-virus security firms' have yet to create a signature for.

Lack of directory integration makes it difficult for IT staff to keep track and control the systems that they are required to protect. Especially in large organizations, it is critical to have your malware defense strategy be integrated with your user directory for ease of management. It is very difficult to update a system, or diagnose a problem when the system says the name is "host481" or "IP Address 192.168.1.179". A valuable system is one that can tell you that Bob in Accounting's software is out of date.

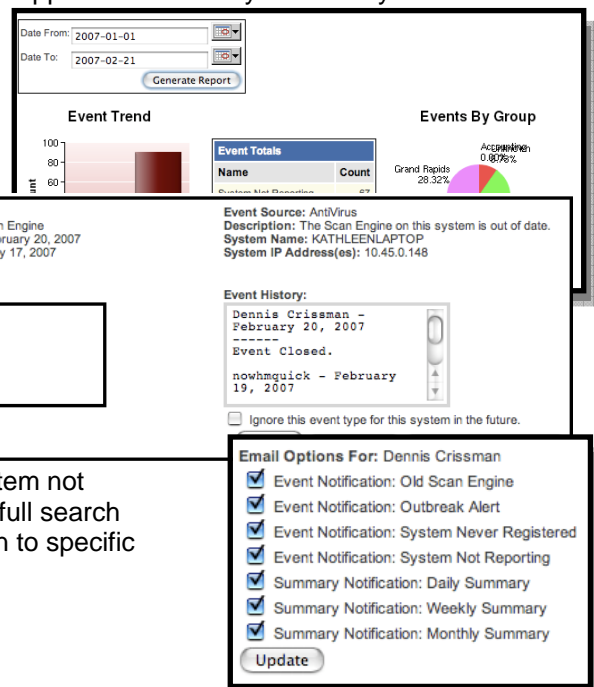
## Key's to a Successful System Malware Defense Program

*Authors Suggestion:  
If you are using a layered security approach, and you use gateway anti-virus in addition to the system anti-virus, it is a good security practice to use different vendors. This can decrease exposure when a single vendor is delayed on an update.*

The first key to a successful system malware defense program is to use a leading vendor of anti-virus and spyware software. At this time, there are three "visionary leaders" according to Gartner: Symantec, McAfee, and TrendMicro.

Consider using this technology in conjunction with a managed security service provider (MSSP), who can help integrate this as part of an overall layered security strategy. One of the biggest benefits of using a MSSP is that some offer an integrated web portal that can allow you to see all of your security devices and technologies in an easy to view configuration and reporting tool. This integrated approach to security will allow you to better identify gaps and reduce exposure more quickly. It also helps in consolidating the reports for auditors and examiners. One suggestion

when selecting an MSSP, pick one that offers a variety of security services to reduce the total number of partners you need. Ensure that the system you use allows for directory integration for better management. Select a system that has a robust command interface for management. Elements of this interface should include: Complete reporting including event trends, event types (system not reporting, old scan engine, system not registered, virus outbreak alert), events by groups, and full search capabilities. The interface should allow you to drill down to specific event detail.



The screenshot displays a security management web portal. At the top, there are date filters for "Date From: 2007-01-01" and "Date To: 2007-02-21", with a "Generate Report" button. Below this, the interface is divided into several sections:

- Event Trend:** A bar chart showing event counts over time.
- Event Totals:** A table with columns for "Name" and "Count".
- Events By Group:** A pie chart showing the distribution of events across different groups, with "Grand Rapids" at 28.32% and "Acron/Allegro" at 0.87%.
- Event Details (Event # 3301):**
  - Event Type: Old Scan Engine
  - Last Addressed: February 20, 2007
  - Open Since: February 17, 2007
  - Event Source: AntiVirus
  - Description: The Scan Engine on this system is out of date.
  - System Name: KATHLEENLAPTOP
  - System IP Address(es): 10.45.0.148
- Event History:** A scrollable list of events, including "Dennis Crissman - February 20, 2007" and "nowhquick - February 19, 2007".
- Email Options For: Dennis Crissman:** A list of notification preferences, all of which are checked:
  - Event Notification: Old Scan Engine
  - Event Notification: Outbreak Alert
  - Event Notification: System Never Registered
  - Event Notification: System Not Reporting
  - Summary Notification: Daily Summary
  - Summary Notification: Weekly Summary
  - Summary Notification: Monthly Summary

Workflow process which should include full virus or spyware information, system identification information, event history, and the ability to update or add commentary to the event. This information should be available in a report that can be presented to auditors upon request.

Notification process for events such as an outbreak or other designated activity

Network trending and historical data for the entire enterprise that is maintained for at least 1 year.

## Conclusion

System security began with loading protective software directly on the system that needed protecting. With advent of networks and the Internet, additional security measures were deployed at the network level to protect all systems. As attackers have found ways of penetrating these outer layers, it is again critical to look at the individual systems. System AV and Spyware protection is a foundation layer of data security. More advanced and automated tools and software are now available to manage even the largest of networks to keep devices current without having to hire a staff of employees. We need to ensure we are using these tools that allow a holistic view of our network status with reporting and a workflow process. We need to employ a notification strategy that will help us keep all systems up-to-date and ready for the continuing barrage of attacks from all sides. Perimeter eSecurity can offer a wide variety of network, system and user based security tools and solutions for your enterprise including a robust System AV and Spyware program. Contact Perimeter eSecurity today for more information.

By Kevin Prince,  
Chief Security Officer  
Perimeter eSecurity  
[www.perimeterusa.com](http://www.perimeterusa.com)  
(800) 234-2175

Founded in 1997, Perimeter eSecurity, is the only provider of complete eSecurity on demand, which offers network security “in the cloud,” or directly to the network, for more than 4,000 growing companies nationwide. Headquartered in Milford, CT with seven geographically-distributed operations centers and three redundant data centers, the company is among the fastest growing network security providers. Its website, [www.perimeterusa.com](http://www.perimeterusa.com), offers a wealth of network security services and webinars that are available to businesses on demand.