



astaro
internet security

Network Security Whitepaper

Virus Protection Strategies to Combat Electronic Attacks

Version: 1.00

Release date: November 3, 2003

Author: Al Cooley, BSEE: WPI, MBA: University of Michigan, Advanced
Studies in Computer Engineering: Boston University



Table of Contents

The Virus Epidemic.....	3
Approaches to Virus Protection.....	3
Recommendations.....	4
Selecting A Network Virus Protection Solution.....	5
Astaro Security Linux.....	5
Virus Protection Option.....	6
Conclusion	6
Further Reading	7
Appendix A: References	8

The Virus Epidemic

With the increasing effectiveness of firewalls and other protection against traditional hacking, viruses, worms and other forms of malware have become the preferred means of malevolently attacking enterprises. Organizations of all sizes and forms are subject to the onslaught. In fact, in 2002 82% of IT leaders reported experiencing a *successful* virus breach. Although the economic impact of a breach varies by organization and incident, ICSA Labs report that the average breach cost \$81,000 in terms of clean-up cost, lost productivity, lost data and other impacts. Given the cost and frequency of the attacks, clearly every organization needs an effective virus protection strategy.

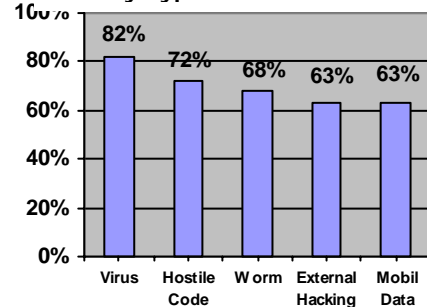
To implement an effective virus protection strategy it is necessary to understand the source of infections. Email has become one of the most frequent means of communicating with customers, suppliers and employees. Widespread adoption has also made it the number one vehicle for launching electronic attacks, using malicious code embedded in email or attachments. According to ICSA, email attachments were the source of 86% of all infections in 2002.

Approaches to Virus Protection

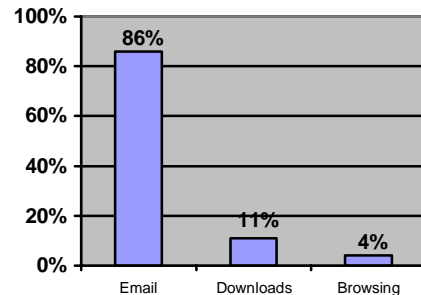
There are two common forms of virus protection available:

1. Host-based scanners: These are software applications installed on every computer in the organization, including mail servers and desktop PC's. They scan each file received or sent from that system. While they are valuable, they suffer several weaknesses:
 - Configuration problems or being powered down (disconnected) from the network can keep the software from getting the updates needed to catch current viruses. Due to the volume of computers, administrators cannot keep them all configured correctly.
 - Employees are known to turn off their desktop scanners to eliminate the processing slow downs and delays email desktop scanners can cause while in "receiving" mode.
 - A pure host-based approach to virus protection causes service calls to be generated across the organization. Whether it is a user asking for guidance when a virus is identified, the need to disinfect due to configuration issues, or the need

Percent of IT Leaders Experiencing Security Breaches By Type In The Last Year



Infections By Source



Network Security Facts:

Percent of IT leaders experiencing a virus breach in the last year: 82%

The average cost of an infection in 2002: \$81,000.

to manually filter a rapidly spreading new virus before updates are downloaded to the computers, a host-only virus strategy is labor intensive.

- Host-based systems typically act only on files written to the disk, leaving the system vulnerable to memory resident viruses.
2. Perimeter-based scanners: These are virus scanning programs, like Astaro's, which reside on a single computer (or gateway appliance) that sits at the Internet's point of entry to your organization, scanning all inbound and outbound email. Benefits of this network-based approach include:
- Single point of administration, meaning this first line of defense can easily be maintained. You can be sure the software is up-to-date, and operating properly 24x7.
 - In the case of new, rapidly spreading viruses, the administrator can create a filter at a single point to catch the virus before automatic updates are available. This enables a rapid response with minimal labor.
 - Viruses are stopped at the edge of the network, before they spread to numerous hosts. As a result, the risk of infection due to mis-configuration, memory resident viruses, local host clean-up calls, and so forth is eliminated.
 - Perimeter systems are specialized secure computers, while host-based systems run on standard computers that the viruses could attack to circumvent the scanners.

Recommendations

In fact these two approaches to virus protection are complementary. According to IDC, a firm that studies the security industry, "...there will be a strong push toward a "layered security" ... The layered security approach will combine solutions such as desktop anti-virus, server and gateway (perimeter) anti-virus, content filtering...and firewalls. " However, if budgets are limited, the perimeter approach is easier to administer, more secure and more cost effective. According to the Yankee Group, another security specialist, "If you filter anti-virus as a network appliance (perimeter gateway), your risk gets shortened and you have less dependency to keep desktop anti-virus up-to-date."

Selecting a Network Virus Protection Solution

There are several major factors to be considered in examining and selecting a network virus protection solution:

1. Accuracy: How good is the solution at catching viruses, including brand new unknown viruses and deeply hidden viruses?
2. Security: How does the virus protection solution integrate with other necessary security solutions such as your firewall, web and spam filter, as well as performance management tools for caching, load balancing and traffic shaping?
3. Administrative burden: How much labor will it take to purchase, install, integrate, manage, update and reintegrate the solution?
4. Total Cost of Ownership: How much will it cost over the life of the product to purchase, learn, install, configure, integrate, manage, update and reintegrate the product into your perimeter defenses? Remember the cost of the product is only a small portion of the total lifecycle costs.
5. Automatic updates: Does the product provide automatic updates for all aspects of the software, not just the signatures?

Astaro Security Linux

Astaro Security Linux is a complete, integrated suite of network security software that protects against the major threats of connecting to the Internet. It is installed on standard PC hardware placed at the point where the Internet connects to an organization's network. Functions provided include:

- Firewall
- Virus protection
- Content filtering
- Spam protection
- Virtual Private Networking
- Wireless protection
- Performance management

By providing a single integrated security solution Astaro slashes the total cost of ownership, administrative labor and potential security gaps. There is no need to learn, install, integrate, manage and update multiple point solutions.

Virus Protection Option

Astaro Security Linux's Virus Protection option provides the capability to scan and eliminate inbound and outbound emails containing viruses and other dangerous content.

Unsurpassed accuracy in the identification of malicious code embedded in both bodies and attachments is provided by a combination of detection mechanisms:

- Virus signatures: Content is scanned for matches against known patterns contained in the virus database.
- Heuristics: Using proprietary rules, content is examined for behavior typical of different classes of viruses. Astaro's heuristics are able to detect up to 92% of previously undetected virus types.
- Emulation: Program actions such as unpacking, running scripts/macros and modifying files are emulated in a protected virtual environment to identify hidden malicious behavior.

Intelligent rules are used to select the fastest detection mechanism, or combination of mechanisms, for a particular file type. Extensive support for unpacking and file types allows the discovery of deeply hidden viruses. Messages containing specific file types or text strings can also be blocked, providing extra security and fast response to new threats.

A staff of 250 engineers constantly monitors the Internet to identify and automatically download information on new viruses to your local Virus Protection option. Signatures of new viruses, which average 300 a week, are added to the existing database of 60,000 as they are discovered. This same Up2Date service also downloads updates for all other security applications in the solution, as well as enhancements to the basic virus detection engine.

Conclusion

Today's Internet environment is increasingly hostile. Every organization can expect to be subject to multiple virus attacks during the coming year. To protect against costly losses both host-based and network anti-virus solutions should be deployed. Astaro provides an ideal network anti-virus solution that is highly accurate and extremely easy to manage. Being integrated into a comprehensive security solution it also provides greater security, lower total cost of ownership and simplified operation. A free 30-day evaluation version can be downloaded at www.astaro.com to verify operation in your environment. To simplify the evaluation process, a free 90-minute web-based workshop is available which steps users through the process of configuring and using Astaro Security Linux.



Further Reading

InfoWorld Magazine reviews Astaro Security Linux and reports "the most polished and easy to use Web-based management system we've seen to date." ([Read the whole article as PDF](#))

"A stylish-looking appliance that addresses the major internet-related security concerns of the small or medium business," says SC Magazine. ([Read the SC Magazine article as PDF](#))

Astaro named winner of the [product excellence award](#) at LinuxWorld.

A free 30-day fully-featured evaluation version of Astaro Security Linux can be downloaded at <http://astaro.com/php/download.php?lang=gb>



Appendix A: References

1. InfoWorld, 8/26/02, Countering The Greatest Fears
2. ICSA Labs 8th Annual Computer Virus Prevalence Survey, ICSA, 2003
3. IDC, World-Wide Internet Security Software Market 2002
4. InfoWorld, 5/21/03