Global Information Assurance Certification Paper

Basic Virus Protection of the Future
Vincent Sullivan
October 24, 2000

In today's environment viruses are emerging at an increased rate that has never been seen because of the increase in which we are connected and communicating over the Internet. What are we protecting our computers with in today's hostile environment scanners, heuristic disinfections, locking down our operating system, integrity checkers, or even active monitoring is used? Well then the question comes up, what should I use for protection of my own network? The goal is to limit the destructive power, denial of service, and reduce the time and effort needed to remove or repair what the virus has done. Looking at the different types of virus protection and what other products we can use will allow for defense in depth and greater understanding of what is out there.

In the United States market you have the big two McAfee and Symantec (Norton) for virus protection. We know that McAfee and Norton are based on scanners, which is the best-known way to look for viruses. What scanners do are search for "scan strings" like signatures or algorithms to look for viruses. The big known problem with this type of defense is that they are only looking for a certain type of style of virus, so of course the new or unknown viruses out there will not be detected by such systems. The other big problem is that there are over 54,000 (1) viruses threats that exist in today's environment, which means you can not have all of them, listed in the scanners otherwise they would be huge. The next type is an integrity checker, which computes checksums or hash values of the original files and stores the result in a database. Then the program recomputes this value and compares it with the original. This type can also be looked at effectively a virus detector. The last basic type is the activity monitors which look for virus type activity like writing to .exe, .ini, or sys files and functions like formatting disks. The major problem with this type is there are tunneling viruses out there that just bypass active searching. We have looked at the general flow, which was from the passive to the active looking methods in use for virus protection, and they're basic down falls.

What are we protecting our selves against now and in the future is a challenging question that security professionals always have in the back of their minds? The general theme right now is Active-X control, Java applets, Malicious Microsoft Office Macros, E-mail attachments, Internet Worms and JavaScript or VBScript is that these are the types that we are facing and will be facing in the future. To verify this trend going to the wild list http://www.wildlist.org/WildList/ and look at the different types of viruses like W97M/Class.D, VBS/Stages.A-mm, X97M/Laroux.CF, VBS/LoveLetter-mm or W32/Funlove.4099. Also by looking at the wild list the numbers for 2000 and correlating them with 1999 we see that the change in viruses seen in the wild has increased from 6% to 22% based on the difference between January and September of each year. This gives a greater understanding of what the network environment looks like and an idea of what it will look like in the future.

Since this threat is growing one check would be to verify that the product you are using has been certified by an outside agency like http://www.icsa.net ICSA.net which has its own criteria for testing of vendors products. Their criteria was last revised in April 1999 for Anti-Virus Scanners is listed below for a quick glance at what we are talking about (3).

ON-DEMAND Module: Products to receive the ICSA Certified mark must:

Detect 100% viruses listed as In The Wild Test Suite (one Month old list)

Detect 100% viruses listed in the ICSA Common Infectors Test Suite

Detect 100% of ICSA's Polymorphic Test Suite

Detect 90% of the ICSA Virus Collection

Products achieving ICSA certification will not cause any false alarms. The False

Alarm tests will be conducted against the ICSA False Positive Test Suite.

ON-ACCESS Module: Products to receive the ICSA Certified mark must:

Detect 100% viruses listed as In The Wild Test Suite (Month old list)

Detect 100% viruses listed in the ICSA Common Infectors Test Suite

Detect 90% of macro viruses in the ICSA Virus Collection

Products achieving ICSA certification will not cause any false alarms. The False

Alarm tests will be conducted against the ICSA False Positive Test Suite.

The ICSA's certification testing main goal is to insure that the products never get out dated, so they retest once the product has been certified at least every 60 days. You can find a list of the certified products at the following location http://www.icsa.net/html/communities/antivirus/certification/certified_products/ (3). This is just for the software that we use to protect our selves from virus but what other techniques or other strategies can we use to secure our systems?

Lets look at another product that we could use to help secure our networks and systems from the threat of malicious logic or virus from writing to unwanted places or destroying valuable data within our network. Pelican Security has a new product called SafTnet that basically is a rules based sandbox concept around your system critical functions like .exe, sys, .ini files or the boot sector, basically places that should not be written too by programs automatically without permission of the user or administrator on a network. It detects a call to a system resource, it intercepts that call and applies a set of permissions or access controls around the suspicious code (6). The Dynamic Sandbox distinguishes between the actions of malicious mobile code or hackers, and the actions of the end user (6). This product looks at files or services we use over networks like Telnet, FTP, E-mail and HTTP as sources of the threats we see in today's dynamic Internet.

Since we are looking at networks as the transport mechanism for malicious logic or viruses what other protective measures can we take for our systems? Since we practice defense in depth we have protection at the Internet Gateway, E-mail, File, and Management Servers along with the desktop systems. Along the same lines as the putting a sandbox around your critical systems you should also look at securing them with policy as well for your servers as users workstations.

Being better informed about products that protect our networks will ultimately ensure we are better protected by making sure we not only have defense in depth with having protection on all our core network systems but also better quality products. Securing the network with scanners like McAfee or Norton, applying products like SafTnet to put a sandbox around services we use in our networks like Telnet, FTP, E-mail, and HTTP along with applying policy on our users. Will help secure our networks from being over run by malicious logic or viruses in the future.

By not just limiting our selves to just the big US two scanners I have listed all the certified scanners that ICSE has tested for more comparison.

Aladdin Security Portal:
URL: http://www.anti-virus.org/

Computer Associates International (CAI)
URL: http://www.cai.com/virusinfo/

Command Software
URL: http://www.commandcom.com/virus/index.html

Data Fellows
URL: http://www.datafellows.com/

GriSoft
URL: http://www.grisoft.com/html/us_index.cfm

Kaspersky Lab
URL: http://www.kaspersky.com/

Network Associates International (NAI)
URL: http://vil.nai.com/vil/default.asp

Norman Data Defense Systems
URL: http://www.norman.com/products_nvc.shtml

Panda
URL: http://cws.internet.com/virus-panda.html

Sophos
URL: http://www.us.sophos.com/

Symantec
URL: http://www.sarc.com/

Trend Micro, Incorporated
URL: http://www.antivirus.com/

Reference:

1. Network Associates International (NAI) (2000)
URL: http://vil.nai.com/vil/default.asp (22 Oct 2000)

2. Safetynet Antivirus and Security Center (02 Jun 1999)
URL: http://www.safetynet.com/ (22 Oct 2000)

3. ICSA.net Anti-Virus Certified Products (2000)
URL:http://www.icsa.net/html/communities/antivirus/certification/certified_products/ (22 Oct 2000)

4. The Wild List Organization. (1999)
URL: http://www.wildlist.org/WildList/ (22 Oct 2000)

5. Birdwell, Larry. ICSA.net Certification of Anti-Virus Products (18 Aug 2000)
URL: http://www.icsa.net/html/communities/antivirus/certification/index.shtml (22 Oct 2000)

6. Pelican Security. Pelican SafeTnet
URL: http://pelicansecurity.com/Products.html (22 Oct 2000)

Note: All sites verified on 23 Oct 2