Corporate Anti-Virus Protection - A Layered Approach

Elizabeth Peyton

Corporate Anti-Virus Protection – A Layered Approach

Elizabeth Peyton
August 6, 2003
GSEC Practical Assignment – Version 1.4b, Option 1

Overview

Computer viruses are a force to be reckoned with for any network administrator. These malicious programs and scripts cause billions of dollars worth of damages to corporations in lost productivity and damages. Unfortunately, viruses are fact of life in today's computing environment, and they are becoming more and more common—and more sophisticated. According to a recent report by MessageLabs, the month of June 2003 "saw viruses increase by 13.6% over the previous month"[1]. Most experts agree that this trend is expected to continue.

In this practical I intend to demonstrate that in today's technological atmosphere, one must think creatively when trying to stay protected against computer viruses. The use of a simple out-of-the-box single-vendor or –application approach has become antiquated, and more and more it has become necessary to think "outside the box" and consider a more sophisticated, "layered approach". The suggestions contained herein are meant to offer a "defense-in-depth" solution for large enterprises and corporations where there may be thousands of entry points through which viruses can enter, causing possible system damage and information theft or loss.

History and Evolution

It has been almost thirty years since the computer virus "industry" began. In the mid-80's we saw our first strains--"Brain"[2], for example. Brain was a very simple virus by today's standards that infected the boot sectors of floppy disks while they were being accessed. Brain and its successors were somewhat harmless—perhaps they altered the display on the monitor, or played sounds or revealed a humorous pop-up window—they were more mischievous than malicious, and they required human interaction to execute. The rate of infection was minimal, in that they required the deliberate sharing of a file to replicate. However, as computers became more sophisticated, so have the computer viruses. Today's virus can wreak havoc on a computer and/or network in a matter of minutes. They can steal and/or damage information, enable remote control by malicious users, and replicate at such an alarming rate that it causes a complete overload of system resources (better known as a "denial of service" attack), bringing down entire enterprise networks, even spawning to other networks across the Internet. With the creation of the most damaging "mutation" to date, the "worm", viruses are now able to travel at an alarming rate because they no longer need human

assistance. They are designed to automatically and swiftly spread themselves, usually by exploiting a weakness in a particular operating system or application.

History has shown that viruses, like their "human" counterpart, continue to mutate into more sophisticated, injurious strains. And they will continue to evolve, with "hybrid" forms becoming more common and methods of delivery more varied. They will attack via the traditional methods—floppies and email attachments—and they will also spread in non-traditional media as well, using new technologies as they are developed, such as instant messaging. The worst case scenario, however, is the virus that arrives via several of these methods at one time—such as through email, shared network resources and web browsing simultaneously, as the Nimda[3] worm demonstrated. No matter how they are delivered, however, one thing is for certain—they are a network's worst enemy. As Arabella Hallowell, senior analyst with Garner Group stated, "Viruses are the most frequent security breach that enterprises face on a daily basis." [4]

Virus Types

Before entering into combat, it is important to "know your enemy" and anticipate potential methods of attack. Computer viruses use several different methods of injection in order to infect a computer. The following are the basic types, and a high-level description of each[5]:

File Infector Viruses

File infector viruses are delivered via "piggyback" with other programs. They are imperceptibly attached to other applications and are run when those applications are launched. Since they appear to be a component of the "legitimate" program, they are accepted into the system registry and memory and are given the ability to perform the same functions as the "legitimate" program under the current user privileges—i.e., copying itself to other shares, emailing itself, altering files, etc.

Boot Sector Infectors

Boot sector viruses are malicious programs that are created to run at system start-up. They arrive via a hard media, such as a floppy diskette or CD—whatever media is used to boot the computer--and then embed themselves in system memory. Modern-day operating systems offer some protection against boot sector viruses by limiting direct access to system hardware, but infection is still possible at startup before the operating system is loaded, such as when a system is booted from a floppy diskette.

Macro Viruses

Macros are simply a pre-programmed set of instructions meant to be carried out routinely to save time and keystrokes. Many commands can be entered into a macro and then quickly run in sequence, regardless whether the results are benign or malicious. Originally developed as a convenience meant to be helpful to both the developer and end user, the same characteristics that make macros so useful also make for handy tools for malicious program writers. Many of today's software applications allow (and even encourage) the use of macros, making a virus-writer's job even easier. In a macro virus, malicious commands can be run quickly; one of those commands usually involving copying or sending itself to another computer, either via the use of shared network resources or via email. An example of this was the "Melissa" virus. Melissa contained a set of commands that performed several malicious tasks--for example, to send itself out via email to 50 people in the victim's address book, disable any user-enabled macro protection within Microsoft Word and alter documents[6].

Methods of Entry

I've described above how these types of viruses enter a computer, but how do they get *to* the computer in the first place? A virus is harmless until it reaches its destination and is activated; therefore, to be effective, it must find a way to get there. There are various methods, and the majority are initially performed (usually unwittingly) by the user—either by copying or launching from a floppy disk, by receiving and opening an infected file via email, by sharing infected files over network shares, and by downloading applications or infected files via the Internet. Potentially malicious applications are becoming more attractive to users, as they are frequently disguised as "helpful" tools, such as weather tickers, search toolbars, password managers ("Gator", for example), etc. Lately, however, many of these applications have revealed the presence of "adware" or "spyware", which is software that monitors user activity and reports that activity back to a third party, usually without the user's knowledge. By definition, this may be considered a "Trojan horse"—a program that performs additional tasks that the user does not typically detect, expect or want. Currently, most adware is used for marketing purposes only, but it is clear to see how this medium can easily be exploited for the transfer of malicious code and unauthorized access.

In order to cover all these points of entry, a multi-tier method of anti-virus protection is necessary.

The Layered Approach

> With an average of 500 new and increasingly sophisticated viruses each month, companies using traditional antivirus and content security products

> and practices remain vulnerable to attack.—Andrew Armstrong, UK Managing Director, Trend Micro[7]

As today's viruses become more sophisticated, they are capable of infecting computers and networks from a variety of attack points. As a result, the days of single-point detection and eradication are gone—today's viruses can most effectively be combated by using a multi-level anti-virus solution to ensure the best possible protection by covering all infection methods.

So where should you place your anti-virus detection? For the most effective defense, virus protection should be considered at **all** of the following network layers:

Desktop/Server:

The most common and obvious place to implement anti-virus protection is at the desktop/server layer. At one time, this was the *only* place where anti-virus software was found, for protection against the traditional macro and boot sector viruses. It is still the most essential place for anti-virus protection, because it is the only point at which viruses brought in from removable media such as floppy diskettes and CDs will be detected, and because the desktop/server is the last line of defense before a virus begins infection. Desktop scanning should be configured to run in "real-time", meaning that it runs constantly in memory, where it can scan files and disks every time they are accessed, as opposed to a scheduled scan, which may provide a window for virus activation between scans.

Desktop anti-virus protection is also absolutely necessary if you are using any type of email and file encryption. When data is encrypted, that data (including viruses) will travel stealthily through the Internet and internal network, wrapped in a virtual "tunnel", unreadable by anti-virus scanners until it lands on the desktop—the only place where it will be unencrypted and available to be scanned by an anti-virus product. (The exception to this would be networks utilizing full encryption, in which a key server may be set up to decrypt data and scan for viruses at a central location before passing on to the end user.)

In addition to having anti-virus protection at the desktop/server, it is also critical to keep all desktops and servers patched, applying all relative security hot fixes. The most damaging viruses to date have successfully propagated due to a flaw in software that could have been prevented by keeping the software up to date.

There is a disadvantage, however, to having anti-virus protection at the desktop/server layer only, and that is that it is difficult to centrally manage. Users with minimal technical knowledge can disable the anti-virus service, leaving the system (and the entire network, as a result—after all, a chain is only as strong as its weakest link), completely unprotected. Another disadvantage is that there is no way to ensure that each user always has the most up-to-date anti-virus

signatures. This is why you may want to also consider implementing anti-virus protection at the next layer, the email server/store.

Email Store (Server):

> Email transports all sorts of things, including documents with executable code—programs, scripts and macros. Email continues to be the number one source of virus infections in the enterprise.[8]
> –Fred Avoloio, President, Avolio Consulting.

Although newer methods of transmission are constantly being developed and perfected, email is still the most common means of introducing a virus into a network. And, considering how email has become such an integral part of a corporate network's communication (both internally and externally), there is a tremendous potential for virus infection via this delivery method, and, naturally, that potential increases proportionately with the size of the network.

Keeping a virus-infected file from ever reaching the end-user's desktop is an integral part of any virus-protection plan. All email attachments are intercepted and scanned at the information store level before the end user can ever access them, reducing the threat of launching by the end user. Taking this a step further, it is also at this level where email attachments with suspicious file extensions (such as .exe, .pif, .scr, .vbs, etc.) can be blocked entirely, drastically reducing the possibility of an end user opening an infected file and launching a virus.

Another benefit to anti-virus protection at this layer is the ability to centrally manage new virus signatures at the gateway, protecting many email inboxes at one time.

The disadvantage to this method, however, is potentially allowing infected email into your network and allowing it to sit on the email store before it is scanned. If it is intercepted and opened along the way, virus infection will still occur and spread rapidly. Also, this method will only protect against email attachments. What about viruses inserted within an email in "web" format, or viruses coming in from the Internet via browsing? This is where a third layer of anti-virus protection, at the Internet gateway, becomes critical.

Gateway Virus/Firewall:

Catching viruses as close to the security perimeter and as far away from the desktop as possible, of course, further reduces the risk of virus-infected data of ever reaching the end-users. The next layer where an anti-virus solution can be implemented is at the Internet-gateway level, the entry point through which ALL Internet traffic passes through, using a variety of protocols—Simple Mail Transport Protocol (SMTP)/Post Office Protocol (POP3) for email, Hyper Text

Transfer Protocol (HTTP) for web content delivery, File Transfer Protocol (FTP) for file transfers, etc.

Any well-configured large-scale network has a least one firewall that stands between it and the Internet. This firewall monitors and controls all network incoming and outgoing traffic and can be configured to allow or deny access based on several criteria, such as IP address and destination ports. This can prove useful in helping protect against viruses. For example, it might be advantageous to consider configuring a firewall to block access to the popular commercial Internet-based email providers, such as Hotmail and Yahoo. Allowing access to these Internet-based email providers allows users to bypass the email server and its respective anti-virus scanning and attachment blocking functions completely, rendering any anti-virus measures put into place at the email server level useless. It is important to keep in mind that this will not eliminate the use of Internet-based email access completely, however. New Internet email providers arrive on the scene every day, creating an administrative nightmare of tracking and blocking each one. However, blocking the well-known providers will reduce the risk significantly.

Another configuration that may be made at the firewall/gateway level is the blocking of the well-known ports used for "instant messaging". Instant messaging is, by nature, an insecure method of communication and a recently evolved method of transmitting viruses. Although not currently widespread, based on the advances in the virus-development realm and the rapidly increasing popularity of instant messaging, it is only a matter of time before instant messaging become a leading venue for virus transmission:

Most instant messaging services use one particular port for inbound and outbound traffic that can be blocked at the firewall. For example, the following illustration created by Curtis Dalton and William Kannengeisser offers some basic instant message blocking options[9]:

TABLE 1: **Popular IM Services & Countermeasures**

IM SOLUTION	SERVICES	TO BLOCK
AOL Instant Messenger	Instant messaging, voice/video chat, file transfers and file sharing	By default uses TCP port 5190, but cannot be blocked since the app can use any open port
	Sending/receiving images	Block in- and outbound TCP port 4443
	*ALL	Block all access to **login.oscar.aol.com** on all ports
Microsoft .NET Messenger	File transfers and file sharing	Block in- and outbound TCP port 6891
	Instant messaging, voice/video chats	Block UDP ports 13324 and 13325
	Application sharing	Block TCP port 1503
	*ALL	Block all TCP port 1863 access to hosts within the **msgr.hotmail.com** subdomain
Yahoo! Messenger	Instant messaging, voice/video chat	Block in- and outbound TCP port 5010 file transfers and file sharing
	*ALL	Block all access to hosts within the ***.msg.*yahoo.com** sub-domain
AOL ICQ IM	Instant messaging	Block in- and outbound TCP ports 5190 (and UDP 4000 and TCP 4001 for earlier revisions)
	File transfers	Block TCP port 3574
	File sharing	Block TCP port 7320
	*ALL	Block all TCP port 5190 (and UDP 4000 and TCP 4001 for earlier ICQ versions) to **login.icq.com**

*ALL refers to blocking all IM services for this application.

Along with this precaution, however, it is recommended to lock down Internet browser settings at the desktop level to prevent users from selecting alternate ports for their instant messaging.

The solution for instant messaging illustrated above, however, may not be totally realistic for a large enterprise. Instant messaging is becoming more and more popular, and the demand for its use in the corporate realm is going to be something that cannot be ignored for long. Many companies today are feeling the pressure to allow instant messaging, and this demand is likely to increase, leaving network administrators no choice but to allow it and make it as safe as possible from viruses and other malicious code.

If you are left no choice but to allow the use of instant messaging, there are a few options to reduce the risk of virus transmitted via this medium. The major commercial vendors are developing anti-virus protection for instant messaging, usually involving the blocking of file attachments. (For example, Symantec's Norton Anti-Virus 2003 offers this new technology.[10]) Also, as an added layer of protection, it is recommended to implement an Intrusion Detection System (IDS), to monitor instant messaging activity.

In any case, further demonstrating the benefits of a "layered approach", anti-virus protection at the desktop will still be in the "fallback" position, catching any viruses and other malicious code that makes its way past the Internet gateway. Major anti-virus vendors have recently taken the existing functionality of the firewall and created products to enhance its usefulness. Most now offer products that act as, or in tandem with, firewalls to scan for viruses in real time at the Internet gateway. This solution is becoming extremely popular due to the broader range of protocols that can be scanned at this level. Instead of simply

scanning SMTP traffic, as the email store solution does, gateway anti-virus protection can also scan HTTP traffic. This is becoming more and more critical, as it enables the scanning of HTML (Hyper Text Markup Language) code, which is delivered to the user via HTTP. HTML provides the ability to embed scripts and commands, allowing malicious code writers to transparently place harmful scripts (written in, for example, Java or ActiveX) into an HTML-formatted email or a web page. These scripts will automatically run when a user simply browses to a web page or opens an HTML-formatted email message, as the code is executed instantly to display the content, eliminating the need to provide an infected file attachment that may be end up stripped at the email store or left unopened by the end user. In the case of email, even if the user does not choose to open an HTML-formatted message, simply "previewing" it (as some email client software applications allow) will execute the code and launch the virus. Traditional anti-virus scanning tools will NOT detect this type of attack. A gateway anti-virus solution can monitor network traffic for the malicious Java, ActiveX, etc., scripts, protecting the end users as they are reading their email or using their Internet browser.

Incidentally, there is yet another benefit to scanning traffic at the Internet gateway, not related to viruses, but more as a value-added service. Since all traffic is being actively broken down and scanned as it is entering the network, it also provides the ability to perform services that are currently growing in demand—email/browsing content monitoring and even spam filtering. In fact, according to a recent survey, spam is growing at an alarming rate, and is rapidly developing the same traits and delivery methods as viruses. As Mark Sunner, Chief Technology Officer of MessageLabs, stated:

> The lines between virus and spam are becoming increasingly blurred. In the past virus writing was just about malicious intent, but the new breed of virus writers clearly have monetary objectives as well.[1]

Putting it all together

> Because viruses are becoming multi-tiered and more sophisticated, businesses must deploy equally multi-tiered and comprehensive email security solutions. –Karl-Heinz Dahley, Vice President, GROUP Technologies.[11]

The combination of gateway, email store and desktop anti-virus protection provides an aggressive, highly effective means of preventing infection, eliminating a "single point of failure". It is almost certain that viruses will stopped somewhere along its path from the Internet or another internal device, reducing the burden of desktop anti-virus protection alone. After all, one desktop that is vulnerable puts the entire network at risk.

There are some other things to consider when using the layering approach to anti-virus protection. They are as follows:

Forget "Brand Loyalty"

Not only is it wise to arrange anti-virus protection on a variety of layers in your network, it is also beneficial to consider using more than one anti-virus vendor. This will ensure that in the event of a new virus outbreak, you will have the best chance of receiving the earliest signature from the vendor.

The disadvantage to this is that mixing vendors is not always a cost-effective, however. Many vendors provide discounts for using their "suite" of anti-virus products. Maintaining two or three separate products may be more expensive, and the need for additional administrative support may be necessary, but the added peace of mind may be worth it. Whether you choose one or several vendors, however, choose one that is widely known and ISCA certified[12].

"The Weakest Link"

Wrapped around this layered approach is a basic, yet commonly overlooked line of defense. It doesn't require special hardware or software, or advanced technical knowledge to implement. It is employee awareness. Employee awareness goes a long way in preventing virus outbreaks in that it strengthens what is commonly known as the "weakest link" of the information security chain—the end user. The untrained end-user is a ripe target for "social engineering"—the practice of building a trusted relationship and then exploiting that trust in order to get the unsuspecting "victim" to reveal information or perform a certain task. Social engineering provides the easiest way to inject a virus into a system. After all, if you are the creator of a virus, what better way to spread it than to simply entice a user to install it themselves? A classic example of this is the Anna Kournikova[13] virus—unsuspecting computer users were asked to open an attachment that they believed to be a photo of a famous female tennis star, when, instead it was a virus that replicated itself quite rapidly around the globe via email once the attachment was opened.

So how does one begin to fight against social engineering and its use to spread viruses? One may think that with all the layers of protection that have been discussed thus far, users are sufficiently protected, and, to an extent, they are. But, what about the user who has disabled his/her anti-virus protection at the desktop, either intentionally or unintentionally, and downloads a virus-infected file, or opens an infected email obtained from one of the Internet-based email providers discussed earlier, or brings in a virus from an infected floppy disk? It must be accepted that there will always be new ways that end-users can inadvertently bring a virus into the network, and the best defense is education. If all other layers of virus protection fail, an educated user may mean the difference

between safety and disaster. Most users are not aware of the methods viruses are spread, or even what a virus is, for that matter. Therefore, it is important to educate all users of the network how to reduce the chance of virus infection.

At the minimum, network users should be taught the following:

- Do not open file attachments from people you do not know.
- Turn off the "preview" option in your email application.
- Do not download programs from untrusted web sites
- Call your help desk/technical support if you notice any of the following:
    - Unusual icons residing in the system tray
    - Unusually slow system response
    - Frequent hard drive activity

Empowering the end-users with knowledge and providing friendly, helpful assistance, as opposed to a "heavy-handed", disciplinarian approach, will ensure that the end user will be comfortable pointing out unusual activity on his/her pc or suspicious emails, which not only creates a "team approach" to spotting viruses, but may provide the first "heads-up" during the beginning of a new virus epidemic, before virus signatures are available.

There may be a downside to this, however, and that is the tendency for users to become overly vigilant. I am referring to the spreading of virus "hoax" warnings. Users should be educated on how to identify a virus hoax and be discouraged from spreading them. Users should be taught to look for the following signs within an email warning to determine its validity:

- Excessive use of capital letters and/or explanation points
- Urgent tone
- Information allegedly received from a "friend" or "friend of a friend", or confirmed by a well-known technical organization
- Indication that there is no "cure" available

Summary

The information herein is meant to be a general set of guidelines to follow when developing and implementing a large-scale anti-virus solution. The ideal scheme would be to implement all of the suggestions mentioned here. However, in today's economic environment, that may not always be possible. When choosing anti-virus solution, there will always be the challenge of attempting to maximize security while minimizing costs.

At a minimum, anti-virus protection should ALWAYS be implemented at the desktop level. Any additional layers further incorporated will be more expensive,

obviously, but the additional peace of mind may be worth it. After all, it only takes one virus outbreak to spell disaster for your network, and the damage isn't only done to your hardware and sensitive information—it's also done to the reputation of you and your company.

References:

[1]MessageLabs. "Email Virus Growth Continues; Spam Has Grown 38.5% In 2003 According To MessageLabs". URL: http://www.messagelabs.com/news/virusnews/detail/default.asp?contentItemId=481&region=america

[2]Kapersky, Eugene. "The History of Computer Viruses – From the Ancient Days to Present Time – Journey's Start". 27 July 2003. URL: http://www.viruslist.com/eng/viruslistbooks.html?id=11

[3]Danyliw, Roman; Dougherty, Chad; Householder, Allen; Ruefle, Robin. CERT Coordination Center, "CERT® Advisory CA-2001-26 Nimda Worm" 25 September 2001. URL: http://www.cert.org/advisories/CA-2001-26.html (27 July 2003).

[4]Hallawell, Annabella. "Viruses A Weak Threat? Think Again". IT Management. 4 June 2001. URL: http://itmanagement.earthweb.com/secu/article.php/778051. (13 July 2003).

[5]Theriault, Caroloe. "An Introduction to Computer Viruses". Sophos White Paper. 1999 October. URL: http://www.sophos.com/virusinfo/whitepapers/videmys.html. (25 July 2003).

[6]Elnitiarta, Raul K. "W97.Melissa.A". Symantec Security Updates. 29 March 1999. URL: http://www.symantec.com/avcenter/venc/data/mailissa.html. (28 July 2003).

[7]Armstrong, Andrew. "Viruses—Know Your Enemy". 22 January 2003. URL: http://www.vnunet.com/Features/1138188. (20 July 2003).

[8]Avolio, Fred. "Gateway Guardians". Information Security Magazine. February 2003.

[9]Dalton, Curtis E. & Kannengeisser, William. "Instant Headache". Information Security Magazine. (August 2002). URL: http://infosecuritymag.techtarget.com/2002/aug/cover.shtml. (27 July 2003).

[10]"Symantec Corporation. "The Potential Dangers of Instant Messaging". (2003). URL: http://www.symantec.com.au/region/au_nz/homecomputing/library/i_message.html. (29 July 2003)

[11]Armstrong, Illena. "Virus Advancements". SC Magazine. May 2002. URL: http://www.scmagazine.com/scmagazine/2002_05/feature.html. (29 July 2003)

[12]ICSALabs. "Certified Anti-Virus Products". URL: http://www.icsalabs.com/html/communities/antivirus/index.shtml. (29 July 2003)

[13]Cohen, Cory; Danyliw, Roman; Finlay, Ian; Shaffer, John; Hernan, Shawn; Houle, Kevin; King, Brian B.; Van Ittersum, Shawn. "FedCIRC Advisory FA-2001-03 VBS/OnTheFly (Anna Kournikova) Malicious Code". 13 February 2001. URL: http://www2.fedcirc.gov/advisories/FA-2001-03.html. (30 July 2003)