Interested in learning more about security?

SANS Institute
InfoSec Reading Room

This paper is from the SANS Institute Reading Room site. Reposting is not permitted without express written permission.

A Practical Guide to Enterprise Antivirus and Malware Prevention

What can an IT person working on a private, but interconnected, network do to prevent against an influx of "malcontented software" which causes most other IT work to come to a halt while each new outbreak is contained and eradicated? The answer lies in "defense in depth", a military term that means you deploy your defenses in a pattern so you have more than one chance to stop the enemy. This paper describes several common practices which, when implemented together, will greatly decrease, and perhaps almost stop, this u...

Copyright SANS Institute
Author Retains Full Rights

AD

A Practical Guide to Enterprise Antivirus and Malware Prevention

Jay Martin
August 17, 2001
Version 1.1

Introduction

Viruses, worms, and Trojans, each of which has some unique characteristics, are starting to blend together in people's perceptions as well as the way they behave. A virus can use worm-like logic to spread and also install a Trojan horse type program. The distinctions are also mostly lost on the IT professional trying hard to keep this software from impacting their network and end nodes. For the purposes of this paper, I'll put them all together with the term malware. Malware has been getting much more prevalent and virulent, despite the fact that programs that counteract these undesirable applications have been getting better and better.

The problem is several fold; the tools to write malware are getting more sophisticated, more powerful, and easier to use, the ongoing expansion of the internet keeps on giving malware more (and more inexperienced) targets, mail systems, in becoming more feature rich, are becoming unwitting accomplices in the spread of malware, and some malware authors are getting better at the social engineering aspect of spreading their code.

The question is, what can a IT person working on a private, but interconnected, network do to prevent this influx of "malcontented software" which causes most other IT work to come to a halt while each new outbreak is contained and eradicated? The answer lies in "defense in depth", a military term that means you deploy your defenses in a pattern so you have more than one chance to stop the enemy.

I'll step through several common practices which, when implemented together, will greatly decrease, and perhaps almost stop, this undesirable traffic.

A. Company Policies:

While few IT staff enjoy writing and updating policies and accepted procedures, they are an absolute necessity when the time comes for enforcing the security practices that you wish to implement. There are many resources on the Internet, some free and some fee-based services, that can help you write and communicate IT policies to your user community. All IT policies must include upper management "buy-in", an enforcement mechanism, and a method of informing and educating the users to be effective. Your malware policy should be included with the other policies, with each element addressed clearly.

Much has been written elsewhere about writing, publishing, and enforcing IT policies; suffice it to say that this should be a first step, not last, and no malware prevention campaign will be complete or as effective without it.

B. Desktop Malware Protection:

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

The next best thing is to have an installed, running, real-time, and up-to-date antiviral product on your desktops. When the primary threat vector for malware was diskettes, as it was at one time, this action alone would almost stop it completely. There are several components to getting this accomplished.

1. **Installed and Running:** Make sure that every desktop and laptop has the company-supported anti-virus software installed and set to auto-run on OS boot. The people putting new PCs on desktops should be charged with installing your AV application right after the OS is installed. Put wording in the company IT policy that makes it an offense to de-install or disable the antiviral real-time scanning. While some anti-virus products might conflict with your chosen productivity applications and / or your in-house applications, most anti-virus programs have settings that enable you to customize the program to not scan certain files or applications. You have to balance speed and performance with the amount of security that you need from scanning.

2. **Real Time:** Anti-virus programs have two basic modes, real-time "dynamic" scanning and "static" file scanning. "Static" file scanning is useful for when you have to scan a file or a volume to check to see if any of the files are currently infected with malware, but real-time scanning is really what is needed to prevent the computer from getting infected in the first place. In this mode, all files that the operating system opens or uses are scanned first before they are fully opened. Any files that are reported infected are treated according to certain rules that can be set up in the application. Most often, the anti-virus program will try to first repair / disinfect the file, but, barring that, they will either "quarantine" the file by putting it in a hidden or inaccessible directory for later treatment or simply delete the file. These actions can be customized to the needs of the company or individual user. Be aware that some "savvy" users will sometimes disable real-time protection for whatever reason, and then forget to re-enable this later, leaving them completely vulnerable to the next malware component to hit them.

3. **Up to Date**: The best anti-virus program in the world is largely useless without the up-to-date virus signatures it needs to identify new viruses. With a few exceptions, most of the malware you will see in your e-mail inbox will have been released in the last 12 months. Having old virus signatures leaves the user mostly exposed. While most antiviral solutions do have some heuristic scanning capabilities that look for "virus-like" behavior to catch new or unknown viruses, it would be very unadvisable to trust them to prevent infection. If you have ever tried to keep your user base current on virus pattern files by having them update themselves, you know it is an uphill battle. Compliance is spotty at best. You cannot keep up to date without an automated mechanism. All major AV vendors have options that allow you to set the client to periodically check for new AV strings and automatically

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

install them on the desktop. Most also allow you to set up an internal "master" AV server that gets the updated strings, then delivers them to each of the internal desktops at planned intervals, thereby saving bandwidth in your internet connection. One area to take special note in is with laptops. Since they are often booted up and used without being connected to the internal network, they can fall behind in updates quickly. User education has to come into play here so they know how to update their PCs on their own.

C. File Server Malware Protection:

It would be a mistake to think that if all of your end nodes are protected, your servers will be also. No matter what your policies state and how much you threaten; some users will not always be using AV protection. Sometimes it is knowingly, sometimes naively, and sometimes there are OS boot problems that will prevent the AV application from starting up. One unprotected node can rapidly infect lots of files on the network server if server-side malware protection isn't installed.

1. **Installed, Running, Real Time, and Up-to-Date**: The same conventions that are true for desktops and end nodes are also true for servers.

2. **Resource Utilization:** A real issue for server based AV is the amount of resources that is uses. You will need to test this to see what impact it has on your own file and print servers. If you have hundreds of users opening hundreds of files each minute, the overhead from checking every file can be significant. The best way to approach this is to first make sure you have enough RAM to allow the AV software to work efficiently, then fine-tune the scanning rules so that you scan only a subset of all the files that are being opened, just make sure you are still scanning the critical files and the ones that are more likely to be infected.

D. Gateway Malware Protection:

The best new tool that malware fighters have in their toolbox has matured a great deal and gained popularity in the past few years. Since e-mail has become the most prevalent vector for malware infections, adding another layer in your defense by implementing gateway, or network edge, protection can go a long way in preventing problems from cropping up. Gateway protection can come in several forms, AV software that is specifically made for running on your e-mail server, gateway SMTP systems that are dedicated to scanning before passing the messages to your e-mail servers, or AV and malware services that are provided by your e-mail provider outside of your internal network. Whatever form your edge protection takes, there are several issues to look at.

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

1. **MX Record**: If you have your own internal e-mail system, and implement a SMTP gateway system to scan e-mail, you will need to communicate with your ISP to change your DNS MX (Mail eXchange) record to point to the new server. This will force all e-mail destined for your domain from outside to first go through the gateway server. You can opt to have two MX records with your SMTP gateway server being a higher priority than your primary e-mail server, but while this will allow for an uninterrupted flow of e-mail if your gateway server goes down, it will also allow for unscanned e-mail to go directly to your end users while the system is down. A more cautious approach would be to only use one MX record and let the e-mail queue or bounce until the problem with the gateway SMTP server is resolved.

2. **Scanning Rules:** You will need to set up rules on your gateway SMTP system to optimize scanning of incoming e-mail. Be aware some systems may only scan attachments, while others scan attachments and e-mail text for malware. This is an important distinction since there are viruses, like "KakWorm" or "BubbleBoy" that can infect PCs without existing as an attachment. Using Norton AntiVirus for Gateways 2.5 as an example, there are several different options you can enable.
    a. You can scan all attachments regardless of extension name, all attachments except for certain ones you designate, or no attachments except for the ones you list. The best option is to simply scan all attachments.
    b. When a virus is detected in an attachment, you can either delete the attachment outright, attempt to repair the file, or simply log the event and pass it through. If an attempted repair fails, you then can delete the file, or log it and pass the e-mail on. (Not very advisable.)
    c. You can also opt to Quarantine files with viruses. This enables you to possibly repair the file at a later date if the AV info for a new virus wasn't released yet, or you can submit as yet unknown viruses to Symantec for inspection.

3. **Attachment Blocking Rules:** While your user community will probably be happy with the gateway malware protection I've described so far, they might not like the next option as much. This is the type of situation where written policies can help a great deal. These blocking rules are very important, though, because even if you have the best automated AV string update system on the market, there is <u>always</u> a lag between the time a rapidly spreading virus or worm hits the internet until you have the updated strings deployed at the gateway and the desktop. Good blocking rules greatly decrease this window of vulnerability. The best way to block potential problem attachments is by extension name. There are obvious ones that have caused a lot of problems in the past, like .EXE, .COM, .VBS, and .SCR, but there are other ones also that should be blocked. A partial list is .asd, .asf, .asx, .bas, .bat, .chm, cmd, .com, .dll, .exe, .hlp, .hta, .hto, .js, .jse, .link, .lnk, .pif, .reg, .scr, .vb, .vbe, .vbs, .wsf, .wsh, and .wsc. You can inform your users that if they are trying to receive

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

one of these types of files for a legitimate purpose, they can ask the senders to rename the extension when they send the attachment.

4. **Subject Line Blocking**: In addition to attachment blocking, you can also block e-mail based on the subject line. This is helpful when you receive news of spreading malware but don't have the updated AV strings yet. While some viruses and worms spread with changing subject names, others you can discard at the gateway by keying on the text in the subject line. This is also an important line of defense against a worm like "Sircam", which was hard for some scanners to detect since it used its own SMTP engine and non-standard encoding. Again, defense in depth dictates that you use the options at your disposal to stop these files from reaching your end users.

E. Malware Protection for other Vectors

There always seem to be other ways for malware to get into your internal network that are not as obvious. These are some of the other vectors that viruses can use to sneak through your defenses.

1. **Portable Media**: Floppies have long been a culprit for spreading malware, but in today's world where more and more of your users have access to CD-RW drives on their home computers, CD-ROM drives are rapidly becoming just as dangerous. While your policy should include prohibitions on user-installed software, they could be simply transferring files to work on at home. Tape drives, while less prevalent, should also be considered. Some IT departments make it a policy to disable floppy drives, CD drives, etc on some users desktops to prevent this from being an issue.

2. **POP3 / WebMail Sites**: No matter how much protection you put on incoming e-mail, a user with a Hotmail, Yahoo, or Juno account can circumvent several levels of protection by browsing to a web-based e-mail server or pointing their e-mail client to the ip number of their favorite ISP's POP3 server. Some options to combat this vector would be to have a policy against external e-mail systems and back it up with a HTTP content filtering server and use a firewall to block POP3/SMTP traffic to and from everything except approved servers and sources. Another option would be to use a proxy server to block any e-mail connections other than approved ones.

3. **Remote Access Users**: The number of users working remotely or from home is climbing rapidly. The PCs they use to access your network may not be owned by your company and certainly are harder to control even if they are. If they have VPN access to your network, be aware that VPNs do not protect your network from viruses; it only means that they have an encrypted pipeline for malware to come across. Remote access software such as Metaframe makes it easier to do work from other locations, but a policy is needed to ensure that remote users have up to date AV software running on their

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

desktops also. It is a good idea and in the company's best interest to give any remote user a license for the selected AV program to enable them to run it on their end nodes, whether or not the company owns those nodes.

F. User Education:

While stories abound about end users compromising and circumventing security measures that where put in place for their own protection, it is important to include those same users in your malware prevention plan. If your users understand why procedures and policies are implemented, and what can happen if they are not followed, you will get a much higher level of compliance and understanding. When they understand the implications of turning off automatic update or real time protection, they will be much less likely to do so. Explain smart e-mail use to them; tell them why they should not open every attachment that shows up in their in-box. A concise e-mail to your user base and a short explanation when they initially receive their PCs can go a long way to preventing problems in the future. Also, the more educated they are on malware the more likely that they are going to react to real threats and be able to identify the hoaxes that are always part of the Internet landscape.

In short, any information that you can give them to get them to understand what you're trying to accomplish and how it benefits them also will make them more a part of the solution instead of being part of the problem.

Conclusion

Malware in the form of viruses, worms, and Trojan horses is with us to stay for the foreseeable future. While malware keeps on getting more sophisticated and more prevalent, the tools and methods to deal with it keep on advancing also. It is incumbent on the security administrator to keep on getting the education that they need to stay abreast of the current technologies at their disposal. While we know from experience that the next big outbreak of malware might use a method and vector that hasn't even been realized yet, there are many actions that can be taken that can lessen the ongoing background "noise" of known viruses and vectors.

There is no foolproof way of stopping all malware from getting to your network, but deploying "defense in depth" practices by using company policies, server and client side AV protection, gateway protection at the edge of your network, watching alternative e-mail sources, and educating your users, you can make your network a much safer place.

Armstrong, Illena "Viruses: Preparing for the Onslaught." SC Magazine May 2001: 24 - 30

© SANS Institute 2001, As part of the Information Security Reading Room. Author retains full rights.

Harley, David & Burrell, Bruce, et.al. "alt.comp.virus FAQ" April 23, 2000
http://www.bocklabs.wisc.edu/~janda/acv_faq.html (August 17, 2001)

Julio Cella, "Antivirus at SMTP Gateways Level" April 9, 2001
http://www.sans.org/infosecFAQ/malicious/gateway.htm (August 17, 2001)

Symantec AntiVirus Research Center "Security Updates" August 14, 2001
URL: http://www.symantec.com/avcenter/vinfodb.html (August 17, 2001)

Ankdom "poisoned.txt" Distrusted e-mail attachments
URL:http://www.geocities.com/ankdom/poisoned.txt (August 17, 2001)

© SANS Institute 2001, Author retains full rights

Last Updated: May 22nd, 2013

Upcoming SANS Training

Click Here for a full list of all Upcoming SANS Events by Location

SANS Malaysia @ MCMC 2013	**Cyberjaya, MY**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
SANS Pen Test Berlin 2013	**Berlin, DE**	**Jun 03, 2013 - Jun 08, 2013**	**Live Event**
Industial Control Systems Security Training - Houston	**Houston, TXUS**	**Jun 10, 2013 - Jun 15, 2013**	**Live Event**
Security Impact of IPv6 Summit 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 16, 2013**	**Live Event**
SANSFIRE 2013	**Washington, DCUS**	**Jun 14, 2013 - Jun 22, 2013**	**Live Event**
SANS Canberra 2013	**Canberra, AU**	**Jul 01, 2013 - Jul 13, 2013**	**Live Event**
Digital Forensics & Incident Response Summit 2013	**Austin, TXUS**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS London Summer 2013	**London, GB**	**Jul 09, 2013 - Jul 16, 2013**	**Live Event**
SANS Rocky Mountain 2013	**Denver, COUS**	**Jul 14, 2013 - Jul 20, 2013**	**Live Event**
SANS Mumbai 2013	**Mumbai, IN**	**Jul 22, 2013 - Jul 27, 2013**	**Live Event**
SEC528 SANS Training Program for the CompTIA® New Advanced Security Practitioner (CASP) Certification	**Washington, DCUS**	**Jul 22, 2013 - Jul 26, 2013**	**Live Event**
SANS San Francisco 2013	**San Francisco, CAUS**	**Jul 29, 2013 - Aug 03, 2013**	**Live Event**
SANS SEC 560: Network Penetration Testing @ Bangalore 2013	**Bangalore, IN**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
SANS Boston 2013	**Boston, MAUS**	**Aug 05, 2013 - Aug 10, 2013**	**Live Event**
Critical Security Controls Summit	**Washington, DCUS**	**Aug 12, 2013 - Aug 18, 2013**	**Live Event**
Industrial Control Systems Security Training - DC	**Washington, DCUS**	**Aug 12, 2013 - Aug 16, 2013**	**Live Event**
SANS Thailand 2013	**Bangkok, TH**	**Aug 19, 2013 - Aug 31, 2013**	**Live Event**
SANS Virginia Beach 2013	**Virginia Beach, VAUS**	**Aug 19, 2013 - Aug 30, 2013**	**Live Event**
Mobile Device Security Summit 2013	**OnlineCAUS**	**May 30, 2013 - Jun 06, 2013**	**Live Event**
SANS OnDemand	**Books & MP3s OnlyUS**	**Anytime**	**Self Paced**