GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Security Essentials (Security 401)"
at http://www.giac.org/registration/gsec

How to stay virus, worm and trojan free - without anti-virus software.
David Banes
Assignment v1.2d

Introduction.

There's no doubt that anti-virus software is here to stay but there are many things that can be done to prevent or reduce the risk of virus infection and the subsequent effects of such an infection. There are a host of working procedures and policies and some software alternatives that have the potential to greatly reduce your risk levels.

Preventative Measures.

The following items can help to prevent or reduce the risk virus infection in the first place, in no particular order;

- **Turn off automatic opening of email attachments, never open attachments from unknown sources or attachments you are not expecting.**

Don't be fooled into thinking you know what the attachment is, even though it may appear to have a .jpg extension Windows allows multiple extensions and many email programs will only show the first. For example you may see a file called **wow.jpg** when in fact it's full name is **wow.jpg.vbs**, launching this attachment may run a malicious VBScript not launch your .jpg viewer.

- **Use alternative document formats such as .rtf(Rich Text Format) and .pdf (Portable Document Format).**

The most common type of macro viruses use Microsoft Office applications to spread limiting the use of these document types will limit your risk, evaluate your users needs. For example whilst the accounts department needs to use MS Excel for spreadsheet work your sales team probably does not need to send out the actual spreadsheet, a pdf rendering will be adequate and is a lot safer.

Try to get people to save files as Rich Text, this doesn't mean just saving them with a .rtf extension but actually selecting the Rich Text file type in the MS Word 'Save As' dialogue box. Whilst Rich Text format can still contain embedded objects it does not natively support Visual Basic Macros or Jscript.

- **Ensure all current software security updates are applied to all client and server applications.**

This is essential to not only prevent possible denial of service (DoS) attacks (on serve software) but also to avoid buffer overflow[1, 3] vulnerabilities should some malicious code find it's way onto a client machine and be executed. Many viruses and worms exploit known vulnerabilities in common software programs which have been patched

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

by the vendors. Your software version control database must include patch level information.

- **Always scan floppy disks, CD's and any other removable media before using them on their computer.**

It used to be common that boot sector viruses arrived via hardware driver disks, or even the occasional file virus. The risk today is more likely to come from restoring some archived data from removable media. This can be a cause of confusion, you wouldn't normally associate becoming infected with a virus with a restoration of a backup.

- **Scan All files as opposed to program or selected file only.**

Anti-virus vendors have now defaulted to setting it's products to scan all files when they are installed. Limiting virus scanning to files with certain extensions is no longer an acceptable risk. This is because the authors of viruses and worms have learned to rename executable code and Windows itself now allows multiple periods (.) in filenames which often leads to confusion as to the real file type.

- **Do not share diskettes for installing software or even worse copies of software.**

This is one mechanism that allows Viruses to move from machine to machine. It is also possibly illegal if the license is not taken into account. It's a reasonable assumption to make that if the individuals copying illegal software are not concerned about the copyright laws and legal implications then they may also not be bothered about installing and maintaining adequate virus protection. Pirated software is a major source of virus infection

- **Do not download software from non-trusted sources.**

This is a difficult one, what is a trusted source, we all download software from web sites but do we bother to scan it before installing it? It's reasonable to assume that software downloaded from known reputable online software libraries is not infected but there are many other sites that offer software downloads and how can you be sure they have adequate anti-virus measures in place? Even software stored on your companies network should be treated with suspicion. If your network has areas (directories) setup for read and write access then a PC infected with Zmist or FunLove for example will quickly infect any files on those drives.

- **All computers should be configured to boot from drive C first, then drive A.**

Most computers allow this setting to be changed in the “CMOS configuration” during boot-up. This will eliminate all boot virus infections that arise when you leave an infected floppy disk in the A: drive and restart the PC. One of the main culprits here is that old floppy disk you have in your top draw with your resume on it.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- **Do not install any unapproved software on your computer**

You should not install software without the prior consent of your system administrator or manager. This goes with the above section on downloading software. Not only does using approved software mean you run a safer computing environment but it make troubleshooting when things go wrong and upgrading a lot easier.

- **Disable the Windows Scripting Host**

The Windows Scripting Host(WSH) (4) runs scripts, these can be of various types but are usually VBScript or Jscript. Windows Scripting is as near as we are going to get to the return of the batch file. Scripts run in a DOS prompt using cscript.exe, or within Windows with wscript.exe doing the hosting. Simply put, the Windows Scripting Host acts as an interpreter between a scripting language that supports the ActiveX Scripting interface such as VBScript, JScript or Perl, plus all the Windows features, including access to folders, file shortcut's, dial-up networking and the Windows registry

The first viruses/worms to use the WSH where VBSy and VBSv777 (5). It's quite simple to disable the WSH and as it's an optional component completley safe, you can always re-install it. There are fiull instructions and a tool available online.(6)

Will the Operating System help?

Add to these measures a certain amount of thought from Microsoft and the news that Whistler will be able to block unsigned code (2) and there is another layer of security for free. The plan appears to be that Windows will block the execution of any code that does not have a valid digital signature. This of course makes the assumptions that digital signatures are in fact legitimate and can be trusted themselves, which we've seen is not always the case with some certificate authorities (CA's) unwittingly giving out certificates to un-authorised people!

I suspect that an effective way of enforcing this technique is a long way off however. Even if Microsoft get to a point in Windows development where they are signing all executable code many independent software vendors (ISV's) will be slow on the uptake and Microsoft will be forced to make code signing an option. As we know, options in code and be turned on and off and not always the way we expect them to be.

Users will then be faced with a difficult choice, turn off the signature checking feature or stop using un-signed code/applications, a choice similar to that which we where all forced to make prior to Y2k. Make sure the application is Y2k compliant, fix it or stop using it.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

In house software developers will also have to be persuaded to sign their code. The idea is a good one, only allow signed code to run, but the reality is that applying a code signing model to an operating system is always going to bring that old trade off back, security vs usability.

Server based Firewalls and filtering.

If you work in a company environment, or are an IT Administrator then there are other things we can do to reduce the risk of virus infection. Firewalls are traditionally used to block or control access to computers by allowing a higher level of control over IP addressing and port access.

Many worms and trojans, specifically back door trojans access resources, perhaps plugins or updates on specific port numbers. Here are a few examples for you to ponder;

Backdoor.Acropolis(7) uses Port number 32791 and 45673. A remote operator of this Trojan can then use the 'infected' PC to send messages using mIRC, these messages could have file attachments.

W32.Semisoft.59904 (8) uses port 531 to ping 4 different IP addresses thereby passing the infected machines IP address to the recipient of the pings.

However, W95.Hybris and W95.USSRHYMN piggy back existing email ports (well that is they watch communications) and use this transport mechanism for their own use so blocking those will block email as well, this will soon have a helpdesk fending off irate users.

As you can see, simply having a tight control over which ports are open and which internal IP addresses are visible externally you can control the level of damage or infection within your organisation.

There are several high quality email and html filtering products available that can be setup to examine files attachments and html pages. Various objects like executable files or code can be stripped out before passing them on or quarantine them for later inspection. Many of these product vendors have developed alternative detection techniques to those more commonly used by anti-virus companies.

There is an 'unofficial' list of port numbers used by malicious code in Appendix A, this is made up from list (9) found on a hackers web site, NiteRyders reference Desk(10) and the addition of other known port usage by viruses, trojans and worms researched by Symantec.

The list is probably not complete and may even have errors in it but it's a strong argument for turning OFF all ports and only enabling the ones you really need to have open. Credible products will take this approach anyway.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Client based firewalls and filtering

As well as blocking server based virus transport mechanisms there are fire walling and filtering options available for clients, more commonly for Windows PC's. The last year has seen a rash or personal firewall type of products from freeware, shareware and commercial vendors.

Many of these are now in their second or third iteration and are very effective at blocking both incoming and outgoing traffic. There is also at least one solution, ZoneAlarm Pro that blocks VBScripts as well. This makes it a very effective product against the many VBS worms that we are seeing a rapid growth in this type of threat.

Some email programs have filtering options. Setting up a filter or rule to move all incoming email to a separate folder if it has an attachment will at least prevent you from accidentally running an attachment. Once a day you can review the folders contents and delete the mails you think are suspect.

Of course this approach only works if the email client you are using does not suffer from any unpatched exploits that may cause the attachment to be run automatically.

Home office and general consumer type users are now moving over to broadband internet connections, these bring the usual threats associated with 'always on' connections. At a minimum a personal firewall should be installed and email filters setup along the lines proposed earlier.

One technique I like is to put a router between the cable/ADSL modem and make sure it's configured correctly. A good router for home use is the Netgear RT311, or the RT314 which has a built in hub. These can be setup to block access to the PC('s) connected and have Network Address Translation (NAT), this means you computer(s) behind the router are own their own 'internal' IP address range and not visible to the outside world. (It's a good idea to make sure your ISP is happy with multiple computers hanging off one connection).

Conclusion

It is possible to develop a set of working practices and policies that minimise the risk of virus/worm/trojan infection without the use of anti-virus software. The reality is that it is extremely difficult to educate and train a large workforce and get them to conform to these guidelines, even more difficult to get your own family to follow them. ☺

This is why anti-virus software has become and will remain a necessity for any company and many home and home office computer users. People just can't be relied upon to follow complicated and unwieldy procedures and working practices unless there is a very strong incentive, for example, you work in defense or sensitive government areas.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The software is a viable alternative even with the continual upgrades, patches and weekly or even daily virus definition updates. It provides a level of security that computes users are comfortable with and is on the whole very effective.

Anyone responsible for an anti-virus implementation should however take this paper and use it as a guideline for a new anti-virus policy or as a reality check to make sure an existing policy is realistic and workable. There will be changes and additions to the above items to mould the policy to your own organisation and no doubt a few ideas that I haven't thought about.

The area of computer anti-virus research is always evolving to meet the challenges of new threats, never believe you have all the areas covered. Review your anti-virus software and policy implementations at least quarterly.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

References

(1) Coffee, Peter, "How 'buffer overflow' attacks work", July 20th 2000
http://www.zdnet.com/eweek/stories/general/0,11011,2605669,00.html

(2) Raikow, David, "Whistler to block unsigned code", November 20, 2000
http://www.zdnet.com/devhead/stories/articles/0,4413,2655786,00.html

(3) Walters, Ryan, "Lotus Domino Buffer Overflow', January 2001,
http://www.symantec.com/avcenter/sirc/lotus.dos.malformed.email.html

(4) Esposito, Dino, "Windows Scripting Host", June 1998
http://www.microsoft.com/mind/defaulttop.asp?page=/mind/0698/cutting0698.htm&nav=/mind/0698/inthisissuecolumns0698.htm

(5) Banes, David, "A new host emerges", December 1998
http://www.symantec.com/region/reg_ap/avcenter/news/9812.html

(6) Symantec, "Removing the WSH", 1998
http://service1.symantec.com/sarc/sarc.nsf/html/win.script.hosting.html

(7) Reyder, Dmitry, "Backdoor.Acropolis", February 2001
http://www.sarc.com/avcenter/venc/data/backdoor.acropolis.html

(8) Chien, Eric, "W32.Semisoft.59904", February 1998
http://www.sarc.com/avcenter/venc/data/w32.semisoft.59904.html

(9) [Withheld], "Ports used by Malicious Code", May 2001
http://www. *[domain removed]* . ru/main/hack/12.htm

(10) NiteRyder?, "NiteRyders refernce Desk", May 2001
http://www.nccn.net/~ncpcug/trojans.htm

© SANS Institute 2000 - 2002 Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Appendix A Ports used by Malicious Code (9)
(I apologise if you are in this listing and should not be, let me know and I'll remove the list item:)

Acid Battery 1.0	32418
Agent 31	31
AimSpy	777
Ajan	25
Ambush	10666
Antigen	25
AOLTrojan1.1	30029
Back Construction	21
Backdoor.Acropolis	32791, 45673
Backdoor.Asylum	Various
Backdoor.BrownOrifice	8080
Backdoor.G	1243, 6711, 6776
Backdoor.NTHack	29292
Backdoor.Rat	1-65525
Backdoor.Sadmind	600
Backdoor.SMBRelay	139
Backdoor.Smorph	23276, 23477
Backdoor, Transscout	1999
BackConstruction 1.2+1.5	5400
Back Orifice 2000	8787, 54320
Back Orifice DLL	1349
Back Orifice	31337
Back Orifice-DeepBO	31338
BigGluck, TN	34324
Bla 1.1	1042
Bla	20331
Blade Runner	5400, 5401, 5402
BO Jammerkillah	121
BOWhack	31666
Bugs	2115
Chupacabra, Logged!	20203
Coma Danny	10607
Deep Throat 1.0, The Invasor	3150
Deep Throat 1.0	2140
DeepThroat 2.0 & 3.0	60000, 6670, 6671
Delta	26274
Delta	47262
DeltaSourceDarkStar	6883
Der Spaeher 3	1000
Devil 1.03	65000
DMSetup	59
Doly Trojan	1012

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Doly Trojan 1.1	21
Doly Trojan 1.1+1.2	1011
Doly Trojan 1.35	1010
Doly Trojan 1.5	1015
Doly Trojan 1.6	1016
DonaldD.Trojan	23476, 23477 (SPX: 0x9014, 0x9015)
DRAT	48, 50
Eclipse2000	12701
Evil FTP-Ugly FTP	23456
Executor	80
FileNail Danny	4567
Firehotcker	5321
Fore	50766
FTP99CMP	1492
GabanBus,NetBus	12345
GabanBus,NetBus	12346
Gatecrasher	6969, 6970
GirlFriend	21544, 21554
Gjamer	12076
Hack?99 KeyLogger	12223
Hack'a'tack	31787, 31785
Hack City Ripper Pro	2023
Hack Office Armageddon	8879
Hackers Paradise, Masters Paradise	31
Hackers Paradise	456
Happy99	119
Hidden port V2.0	99
HVL Rat5	2283
ICKiller	7789
IcqTrojan	4590, 4950
Illusion Mailer	5521
InCommand 1.0	9400
Indoctrination	6939
Infector 1.3	146
Ini-Killer, Phase Zero, Stealth Spy	555
InI Killer	9989
Invisible FTP	21
Kazimas	113
Kuang	30999
Kuang2 The Virus	13700
Larva	21
Linux.Ramen.Worm	27374
Masters Paradise	3129, 40421, 40422, 40423, 40426
Maverick's Matrix	1269

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Millenium	20000, 20001
NetMetropolitan 1.0 & 1.04	5031
NetMetropolitan 1.04	5032
NetMonitor	7300, 7301, 7306, 7307, 7308
NetSphere	30100, 30101, 30102
Netsphere Final	30133
NetSpy	1033
NetSpy DK	31339
Online Keylogger	49301
OOTLT	5011
Pass Ripper	2023
Phineas Phucker	2801
Portal of Doom	3700, 9872, 9873, 9874, 9875, 10067, 10167
Priority	16969
Progenic trojan	11223
Prosiak 0.47	22222
Prosiak	33333
Psyber Streaming Server	1170, 1509, 4000, 1024
Rasmin	531
Remote Grab	7000
Remote WindowShutdown	53001
RingZero	80
Robo Hack	5569
Satanz Backdoor, Peur de Rien FTP	666
Schwindler 1.82	21544
Schoolbus 1.0	4321
Schoolbus 1.6 & 2.0	43210, 54321
Senna Spy	11000
Shiva Burka	1600
ShockRave	1981
Shitheep	6912
Shitheep Danny	69123
Shtrilitz	25
Silencer, WebEx	1001
Sockets de Troie	5000 , 5001, 50505
Socket 25	30303
SoftWar	1207
Spy Sender	1807
Stealth Spy	555
Streaming Audio Trojan	1170
Striker	2565
SubSeven	1243, 6711, 6712, 6713, 6776
SubSeven 2.1	27374
Tapiras	25
Telecommando	61466

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

The Invasor	2140, 3150
The Spy	40412
The tHing	6400
The tHing 1.6	6000
The Unexplained	29891
Tiny Telnet Server	34324
Total Eclypse 1.0	3791
Transscout	2000
TrojanCow	2001
Trojan Spirit 2001a	30133
Trojan Spirit 2001a	33911
Ugly Ftp	23456
Ultors Trojan	1234
Voodoo Doll	1245
Vampire	6669
Voice	1170
W32.DoS.Trinoo	27665
W32.Gnuman.Worm	99
W32.NewApt.Worm	80
W32.Semisoft.59904	531
W32.Sonic.Worm	1973,19703
W32.HLLW.Qaz.A	7597
WebEx	21
Whack-a-mole	12361
Whack-a-mole	12362
WinCrash	3024, 5714, 5741, 5742,
Wincrash 2	2583
Xtcp	5550

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.