Global Information Assurance Certification Paper

Introducing Viruses and Sophos Anti-Virus

Edward Josh (U.K.)
SANS GIAC GSEC Practical Assignment - Option 1
Version 1.4b
November 2002

Introduction

In this paper I will be focusing on the Sophos Anti-Virus desktop and server product and will be answering the questions raised in David Poston's GIAC GSEC practical paper; '*What to Look for in your Anti-Virus Solution?*'. David identifies some of the essential key questions you should ask yourself when considering an anti-virus (AV) product, such as, 'How easy is it to deploy?', 'Is it hard to update?', 'Does it catch viruses?', 'Once I find something, what can I do with it?' and 'How much does it cost?'.

Along with these questions I will also discuss the products main features, their advantages and disadvantages, as well as listing some best practice recommendations from my own experience that I hope will be of use to those in the process of scoping or reviewing their corporate anti-virus strategy.

Introducing Viruses and Sophos Anti -Virus

Speak to any I.T. administrator and ask them what security tools or systems they could not live without, it is an almost certainty that anti-virus would feature towards, if not at the top of their ten most wanted list. If you work in I.T. it is equally as likely that you have at sometime or another, seen or felt the effects of viruses, worms and trojans as well as other 'unwanted code' and programs.

Symantec, McAfee, Trend Micro, F-Secure, Kaspersky, Command and Computer Associates are just a small sample of software vendors who have anti-virus products on the market designed to fill this demanding requirement from industry, but with so many to choose from it can be quite daunting if you have been assigned the task of selecting your company's anti-virus solutions.

Sophos, with their product 'Sophos Anti-Virus' have rapidly become a major player in the world of AV. Their headquarters are based in the UK and they have subsidiaries and branch offices in the USA, Australia, France, Germany, Italy, Japan and Singapore.

Sophos Anti-Virus is currently on version 3.63 and is supported on the following extensive list of platforms:

AIX (PowerPC), Digital Unix (Alpha), DOS, FreeBSD (Intel), HP-UX (HP-PA), Linux (Alpha/Intel), Lotus Notes, Macintosh, Microsoft Exchange, Netware,

Open VMS (Alpha/VAX), OS/2, SCO OpenServer/UnixWare (Intel), Solaris (Intel/SPARC), Windows 3.1x, 95, 98, Me, Windows NT/2000 (Intel) and finally Windows NT (Alpha).

As of 1:18 p.m. on the 22nd November 2002 Sophos was capable of detecting all 78,389 *known* viruses in existence. With new viruses being released into the wild daily and the overall percentage increasing significantly each year, this worrying trend looks set to continue. The term virus is used very broadly in this paper and is used to describe many types of 'malware' (malicious software), including trojans, worms and the like.

A 'Virus', simply put, is a piece of software that can replicate and transfer itself from one computer to another, without the user being aware of it. Some are relatively harmless but many are extremely malicious and can damage and destroy data. Virus creators are continually adapting to anti-virus technology, designing increasingly complicated viruses that use different methods of infection and replication. With the advent of polymorphic, slow infector, macro, tunnelling, stealth, sparse infector, parasitic and worm type viruses, anti-virus defence is fast changing and becoming increasingly sophisticated.

Since the introduction of the *Computer Misuse* Act of 1990 (UK) it has become an offence to release a computer virus. Due to the way that viruses spread it is very difficult to identify the originating source and therefore prosecutions are few and far between. Also there are some countries where no specific legislation exists, so even when a source is identified, little or no action is taken.

Trojans or 'trojan horses', like viruses, come in many forms. Trojans do not replicate but often perform hidden and harmful functions. The infamous *SubSeven* 'backdoor' trojan is an excellent example. The *SubSeven* backdoor trojan can be merged with a legitimate application or file and when the intended target opens the infected file, the *SubSeven* trojan installs itself, hidden on the PC unknown to the user, it runs every time the system is turned on. It is then possible to upload, download, delete files and generally take control of the victim's computer remotely over the Internet.

Installing, Managing and Updati ng Sophos Anti-Virus

Installation

Sophos Anti-Virus is available on CD-ROM and can also be downloaded from their web site. Two types of installation for their desktop/server product are available; an installation for stand alone systems that will not be connected to the main network and a 'CID' installation which stands for Central Installation Directory. A CID is usually created on a deployment server which is used as a central point for network installations, configuration and updates.

The downloadable Windows NT/2000/XP Sophos Anti-Virus self-extracting zip file is approximately 8MB's in size. Installation of SAV is very straight forward.

Once the self-extracting zip file has been downloaded and run the following installation screens and options are followed:

- Selection of Local or Central Installation/Update
- Easy closing of Active Applications (If already installed)
- Selection of New installation or Update of existing installation (If already installed)
- Selection of Installation Path
- Auto-Update Options such as Auto-Update check frequency (CID Install)
- Selection of components to install - InterCheck Client/Server

A local installation could be successfully installed by a novice user purely by selecting 'next' on every screen.

Once you have created your Central Installation Directory it is necessary to share the application folder to make it accessible to all the machines on the network. Also you will need to make sure that an account with administrative rights over all machines on your network is available. This will be used when auto-updating machines. Furthermore, if you are running Windows 2000, you must also have the 'remote registry service' running on all machines, otherwise you will not be able view or paste Sophos down to them. This may well be disabled as part of you standard build configuration and therefore would need to be reviewed and changed if deploying Sophos.

Management

'SAVAdmin' is the application used to manage your deployment of Sophos on your networked (Windows) machines. Fortunately Sophos have decided not to utilise Microsoft's Management Console (MMC) when developing this tool and have created a stand alone product which can be installed and used on any administrators desktop. SAVAdmin, like Sophos Anti-Virus comes on CD-ROM, can be downloaded from their web site and is approximately 1MB in size.

SAVAdmin displays domains in a pane on the left and the workstations and servers are listed on the right in a network neighbourhood fashion (incidentally this is where SAVAdmin gets this information). SAVAdmin displays *every* conceivable piece of information about each machine's installation of Sophos that you would ever need for its administration:

The machines NetBIOS name, it's operating system, it's operating system's version, if you have administrative access to the machine, if SAV is installed, if SAV is active, what version of SAV is installed, what rollout it is on, what IDE's are installed, the total number of IDE's, if InterCheck Client is installed/active, if InterCheck Server is installed/active, it's Central Installation Directory path, it's auto-upgrade account, it's configuration name, if Sophos is up to date, it's local installation path and lastly, even which windows service pack and CPU type it has.

Fortunately you can select what columns are displayed in SAVAdmin's preferences. Once you have configured a machine on your network to your exact specification it is possible to copy and save the machines configuration. This can then be used to paste down to machines without Sophos installed. Installing Sophos remotely is really as easy as highlighting the machine and clicking paste configuration.

Updating

Each month Sophos releases an updated version of Sophos Anti-Virus which offers protection against the new viruses that have been released into the wild. Sophos's version number changes incrementally each month and is currently on 3.63. Between updates Sophos releases virus 'IDE' files, short for identity, to enable users to protect themselves against the threat that each new virus brings.

If you are manually updating Sophos each time a new virus IDE is released, they can be downloaded from Sophos's web site (each IDE is only a few kilobytes in size). The IDE can then be copied into the Central Installation Directory and will be pulled down by the clients each time they are set to update.

Enterprise Manager is a relatively new addition to Sophos's suite of products which automates the process of updating Sophos and IDE's. Once the Enterprise Manager has been installed and configured it will connect to the 'Sophos Databank' to look for product and IDE updates and automatically push them down to your Central Installation Directory. This process is administered by the 'Sophos Console' which is a snap in for the MMC. Thanks to the introduction of the Enterprise Manager, updating of Sophos (which can be configured to look for updates 24 times a day) has become truly automated.

Does it catch viruses?

The VB100% is an award given to vendors for products, that during extensive tests, have shown to detect 100 percent of all 'in the wild' viruses with no false positives. 'Virus Bulletin' (www.virusbtn.com) provide independent anti-virus advice and testing of anti-virus products. Virus Bulletin has tested 28 different vendors products and Sophos Anti-Virus has a very good overall track record and detection rate. Here are the results of the latest Virus Bulletin testing on SAV:

Windows ME – February 2002 - Pass

SuSe Linux – April 2002 – Fail (incidentally no other products received a VB 100% award in these tests for that month)

Windows XP – June 2002 - Pass

Netware – August 2000 - Pass

Windows 2000 – November 2002 - Pass

Laptop Tip

A simple change in a configuration file will ensure that laptops that had SAV pasted down to them from a CID, will update themselves automatically upon connection to your network. The default auto-check for updates frequency is set to 240 minutes (this can be changed when installing the CID) and therefore laptops may be disconnected from your network before they check for an update. A quick and simple tip is to edit the *WSWEEPNT.CFG* file found in the default install folder C*:\Program Files\Sophos SWEEP for NT* on the laptop. At the very end of the configuration file the following settings can be found:

```
[%APPNAME\Current Version\RunTimeInfo\SweepNT Specific]
Show Uninstall Info=1
Immediate Sweep On Startup=0
Service As System=1
Upgrade SweepNT=1
Upgrade DOSSweep=1
Upgrade InterCheck=1
Install InterCheck Server=0
Install InterCheck Client=1
InteractiveUpgrade=0
AllowUserToPostponeUpgardes=0
AllowUserToPostponeAttempts=1
AllowUserToPostponeLifeDays=0
UpgradeMinuteFreqency=1
UpgradeDailyFrequency=0
UpgradeMinuteFrequency Number=240
UpgradeWeeklyFrequency=0
UpgradePostponeLifeDaysNumber=14
UpgradePostponeNumber=5
HardShutDownAfter=9000
ShutDownWarnUserAfter=5000
ShutDownAfterWarnUser=8000
```

Amend the line *UpgradeMinuteFrequencyNumber=240* to the desired auto-update check time required.

Configuring Sophos

Not everyone will want their AV to automatically delete files that have been found to be infected. Sophos Anti-Virus is an extremely configurable application, letting you tune it to function and react exactly how you want. Figure 1 shows the Sophos Anti-Virus main interface.

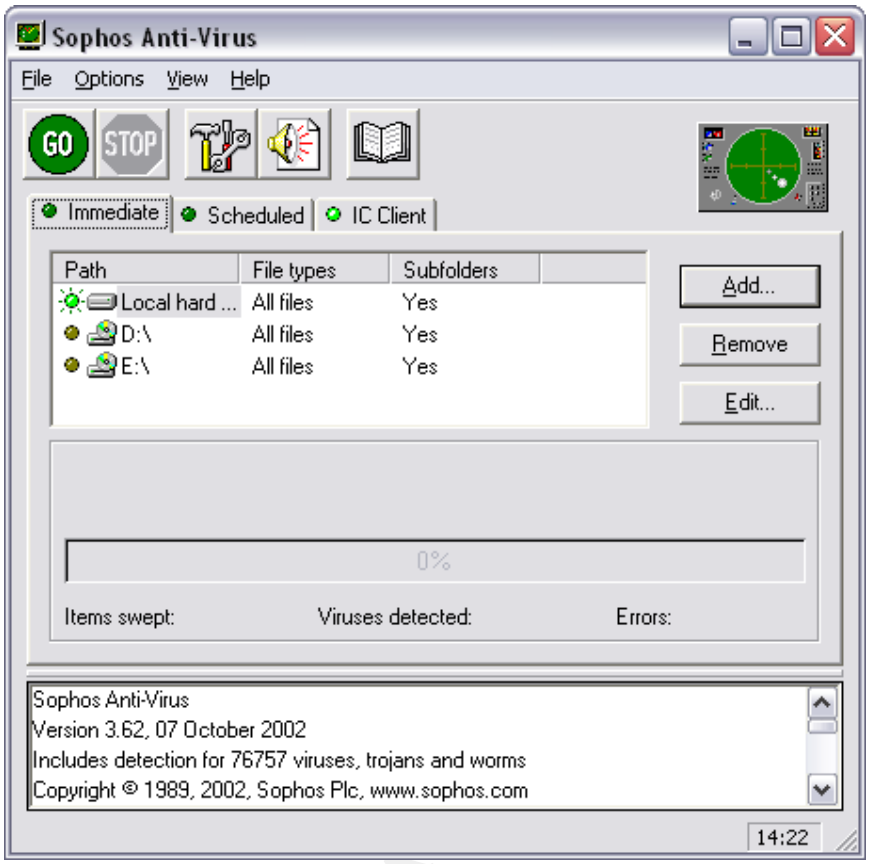

Figure 1

Immediate scans on floppies and CD's can be initiated through the first tab on the main interface. Local drives can be added and removed as required and it is also possible to add network drives so scans can be performed remotely across a network, without the need to go to a machine to perform an immediate scan. The ability to select whether Sophos scans 'All Files' or just 'Executables' as well as 'Subfolders' can be quickly and easily changed individually for each drive or folder.

Opening the *Immediate Mode Configuration* screen presents you with the *Mode*, *Action* and *Report* tabs. In *Mode* you can choose your Sweeping Level. *Quick* will only scan parts of files that are most likely to contain viruses and *Full* scans the complete contents of files (needed to detect some viruses) but this can affect overall performance and is slower than *Quick*.

Mode also lets you set Sophos's priority level to *Normal* or *Low*. *Low* will mean less impact on your systems but will increase the overall time it takes Sophos to perform a scan. Other options such as whether to *Scan inside archive files*, *Add scan results to central checksum file* and *Include Macintosh viruses* can be selected. Depending on your hardware or even by the way in which you use your systems, by correctly configuring these options you can greatly influence the way in which Sophos runs and/or affects your systems performance as well as overall virus detection. Figure 2 shows the *Immediate Mode Configuration* screen on the *Action* tab.

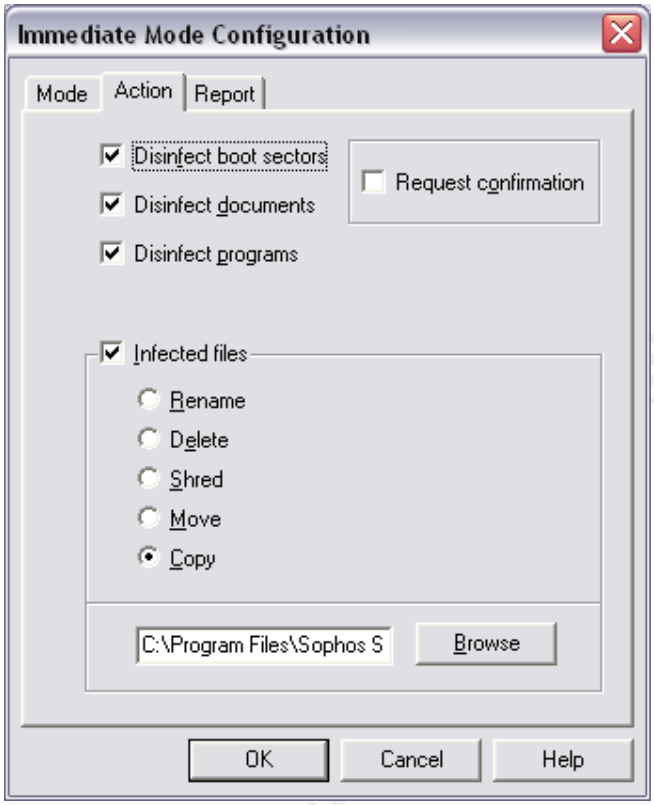

Figure 2

As I mentioned earlier, not everyone will want to automatically delete viruses that have been detected. The *Action* tab allows you define exactly whether boot sectors, documents and programs will be disinfected upon detection as well as what action to take with infected files.

From my experience it is not a good idea to set *delete* infected files and *request confirmation* for users desktop configurations; as quite often the prompt '*the file you have spent hours creating is infected with a virus! Are you sure you want to delete it?*' will generally mean a click in the direction of the no button and the infection remains.

Finally the *Report* tab allows you to set the reporting mode and the scan report file output path.

Moving back to the main interface the *Scheduled* and *IC Client* tabs are very similar to *Immediate* and also have their own individual configuration screens.

The *Scheduled* configuration screen has the additional tabs *File List* and *Time* to allow you to set exactly where and when (down to the time and day) you want your scheduled scans to take place. Scheduling Sophos to begin a full desktop system scan at 10.00 a.m. will not only affect your users systems performance at peak times but can also prove to be hazardous to your health. Configuring scheduling scans to take place out of ours at night or when

systems are least likely to be in use will ensure both scheduled scans and user's sanity will not be affected.

The *IC Client* configuration screen also has additional tabs in the form of *Check* and *Exclusions*. The *Check* tab allows you to set what file types and when, such as 'on read', 'on write' and 'on rename' to allow the InterCheck monitor to scan in real-time. Under *Exclusions* you can set what files and drives to ignore.

Properly configured Sophos should have little or virtually no impact on your systems day to day performance. Obviously the more of the functionality you have switched on, its detection rate increases but system performance decreases. Your exact configuration will need to be tailored to your systems and users to ensure an even balance.

If a virus is detected or there has been an error disinfecting or deleting a file you will definitely want to be made aware. Configuring alerts in the *Notification configuration* screen gives you a variety of alerting methods. Sophos will send an SMTP email alert to defined email addresses, can be set to send an SNMP trap and also utilise Network Messaging (if this hasn't been locked down). Where ever you are logged on you will receive an alert of the virus and where it was detected.

How much does it cost?

Cost is always the second biggest question after functionality. At present, based on five users SAV costs £54 per user (£63 inc. VAT) and £10 per user (£12 inc. VAT) based on a 1000 users. Of course these prices are subject to change but as with the economies of scale; the more you buy the cheaper it gets. I recommend you contact Sophos to get a quote that is tailored to your location, number of machines and length of maintenance updates.

Testing Sophos Using *eicar*

The European Institute for Computer Anti-Virus Research (eicar) have created anti-virus test files that you can use to test your AV and its configuration. At present there are four test eicar files available, all of which can be detected by Sophos Anti-Virus.

eicar.com, *eicar.com.txt*, *eicar_com.zip* and *eicarcom2.zip* are all available to be downloaded from www.eicar.org. The files allow you to test different scenarios such as double extensions and viruses in compressed zip files. If Sophos is not configured correctly it will fail to detect the later. Figure 3 shows the SAV alert message I received whilst attempting to download the eicar test file that had been zipped and then zipped again.

As you can see the file was copied to the default quarantine area and renamed as specified in my configuration.

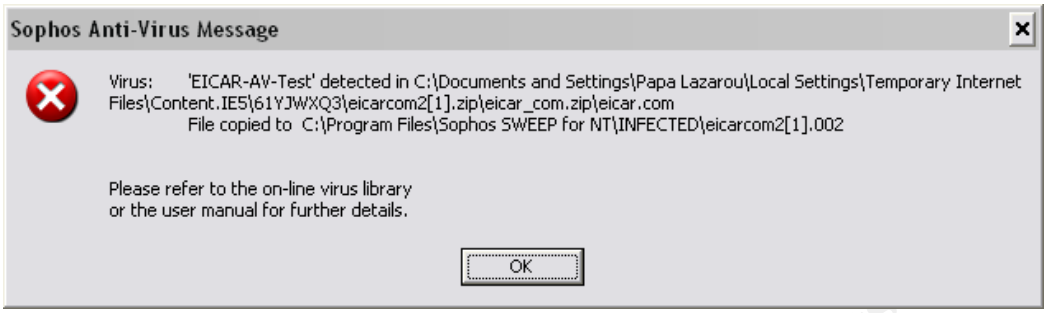

Figure 3

Anti-Virus Best Practise

If you have anti-virus on your desktops and servers, it is vital that you ensure that *every* single machine has it fully installed and configured. The one machine that doesn't will often be the first to get infected and become the source of a wider infection. It's not unusual to find a machine that was built 'years ago' and hasn't been touched as it has 'never gone wrong'. In combination with an insecure operating system such as Windows 95 or a poorly configured build that has never seen a security patch, these machines lurking in the corners of server rooms and under desks can hide viruses that have sat dormant for years.

Restrict access to floppy and CD-ROM drives to essential system administrators or personnel. Employees bringing disks containing data from their unprotected home PC's is another very common source of infection. CD writer and rewriter drives are now almost as widespread as the humble floppy drive and these disks are equally as likely to get or be infected. CD's have the habit of giving people a false sense of security and should also be scanned prior to use. Those with access to these drives should be trained to effectively utilise your AV software to scan their media prior to use and should be taught other 'best practices' such as write protecting floppy disks. Purchasing terminals with no CD-ROM or floppy drives or even removing them from existing machines is another, more direct approach, to controlling what enters and leaves your systems.

In the past few years I have witnessed two popular personal computer magazines distribute cover CD's infected with viruses. If your company distributes disks to clients it is advisable to scan every disk with a fully updated AV scanner. Distributing disks with an infection can damage your reputation severely as well as the potential for legal action and financial loss.

Just installing anti-virus isn't the end of the battle. If you're AV doesn't have the ability to automatically update and requires manual intervention, this should be done each and every time that updated protection for a new virus becomes available. If your anti-virus is only updated ad-hoc, the viruses that you are most likely to be affected by are the ones you have no protection against.

The SANS Institute is a great advocate of 'Defence in Depth'. Having multiple layers in your security systems ensures that one system will prevail where another falls down. Your AV architecture should also incorporate this practise to ensure you never place all your eggs in one basket. Using the same vendor to protect your desktops, servers, Internet and mail gateways is not an ideal approach. If the product scanning your Internet traffic does not detect an infected file that is being downloaded, the second layer, an alternative product on your desktop, hopefully would.

Other common sources of infection are newsgroups, web-mail and chat applications. If you are unable to physically prevent access you should consider restricted their use through your Internet acceptable use security policy. Configure your operating systems to display file extensions as default. This will make it easy to spot any files with 'double extensions' that are used to fool you into believing they are legitimate files or documents such as open_me i'm_not_a_virus_honestly.doc.exe.

Careful attention should be given to disabling unused ports such as USB in the machines BIOS if possible. With removable USB storage media such as key fobs and Windows 2000's Plug and Play functionality; this is yet another possible source of infection or a security loophole that savvy employees can use to get data on and off your network.

Creation of an anti-virus policy is essential to ensure that anti-virus isn't an afterthought and that it is company policy to have AV installed on all machines, preferably before a new system is attached to the network and also to set requirements for minimum update periods.

Summary

With anti-virus being such an important part of security strategy, I hope that this introduction to viruses and Sophos Anti-Virus has given you insight into the threats that viruses pose and introduced you to just one of the many anti-virus solutions that are available on the market today, along with the more practical ideas and advice that you can use to help protect yourself.

References

1. Sophos Anti-Virus
   www.sophos.co.uk

2. Poston, David. "What to Look for in your Anti-Virus Solution?"
   www.giac.org/practical/David_Poston_GSEC.doc

3. European Institute for Computer Anti-Virus Research
   www.eicar.org
   www.eicar.org/anti_virus_test_file.htm (Anti-Virus Test Files)

4. Virus Bulletin
www.virusbtn.com

5. Her Majesty's Stationary Office. "Computer Misuse Act 1990 (c. 18)"
Copyright © 1990 Crown
www.legislation.hmso.gov.uk/acts/acts1990/Ukpga_19900018_en_1.htm

6. SubSeven Trojan Official Site
www.subseven.ws

7. Oldfield, Paul. "Computer viruses demystified"
Copyright © 2001 Sophos Plc
ISBN 0-9538336-0-7

8. Hruska, Jan. "Computer virus prevention: a primer"
www.sophos.com/virusinfo/whitepapers/prevention.html
First published: August 2000
Revised: February 2002

9. Carr, Katherine. "Sophos Anti-Virus detection: a technical overview"
www.sophos.com/virusinfo/whitepapers/savdetection.html
October 2002

10. "The Hutchinson Dictionary of Computing, Multimedia, and the Internet"
Copyright © 1997 Helicon Publishing Ltd
ISBN 1-85986-159-8