Global Information Assurance Certification Paper

Managing Sophos Anti-Virus on a College Network

Steven Blanc
April 30, 2004

GSEC Version 1.4b, Option 2

Abstract

Anti-virus software has become more important than ever with viruses rapidly spreading. Management of this software on a college campus can be complex due to the multitude of operating systems and possibility of numerous configurations. This paper provides techniques to manage anti-virus software for desktop and laptop workstations more easily on a college network using automation and scripting with Sophos Anti-virus.

Introduction

The threat of virus outbreaks looms over every system administrator on a daily basis. Anti-virus software is designed to reduce the risk of this threat, but only if it is functioning correctly. Anti-virus software is only as good as its last update, so to maintain an automated and reliable update and tracking system to ensure protection from viruses is important.

This paper expands upon the paper *Introducing Viruses and Sophos Anti-Virus*[1] written by Edward Josh. With the focus on Sophos, a leading anti-virus company, this paper describes using and expanding on their enterprise management products to provide reliable, low maintenance and automated anti-virus solution to a wide variety of operating systems.

This paper focuses on providing anti-virus software to desktop and laptop computers. While many of the techniques described will work in other situations, desktop anti-virus software should only be considered as part of an overall anti-virus and security plan.

Before Snapshot

The College has been using Sophos Anti-virus for approximately two years, directly supporting approximately 800 faculty and staff computers and 250 lab and kiosk computers. These computers are approximately 60% Windows, 35% Macintosh and 5% other operating systems. The greater part of the computers is managed and authenticated from a central authority.

The College supports a student body of approximately 1,600 students that are strongly encouraged to use this anti-virus solution, but are not required. The majority of these computers are suspected to be Windows 2000/XP, but the student Help Desk reports that they have seen many of the commonly available operating systems. According to the student Help Desk many students do not use Sophos due to the complexity of the installation.

Setup

At the beginning of this project, Sophos Anti-virus (SAV) was installed from CD-ROM to a network share that was located on one of the Windows 2000 print servers. Access to the share was provided using domain authentication, and

Appletalk services were handled by a product called ExtremeZ-IP. The share was used as a central installation directory (CID) for Windows and Macintosh clients.

Two types of updates were performed on the CID. The first was an update of the virus identification files (IDEs). This was accomplished by a script that was scheduled to run every eight hours. The script downloaded a zip file of IDEs from Sophos, unzipped it and performed an update of the CID. This procedure was completed whether or not new IDEs existed.

The second type of update was an engine update. Engine updates were made available monthly by CD. After the CD was received, a system administrator used it to manually update the SAV engine on the CID.

Clients were set up manually by running the setup program located on the CID. The technician running the installation needed to step through a wizard to install the standard configuration. The configuration would cause SAV to check for updates and automatically install them from the CID every 240 minutes. On Windows 2000/XP the install needed an account to run the auto update service. Computers located in the domain used a domain account which was granted "logon as service" rights. Non-domain computers needed to create an update account on the computer and give it logon as service rights before running the installation. SAV could only check for and perform updates while the computers were connected to the local campus network because the system used file sharing.

Problems

This system was far better than the one it replaced, which was virtually non-existent; but several problems were identified with the way Sophos was configured. As the system was analyzed, the problems could be broken into three major categories: updates, central monitoring and configuration, and reports.

Updates

Anti-virus software is only as good as its definitions. New viruses are found in the wild daily and the recent rapid releases of Netsky and Bagel virus variants has pushed the speed limitations of definition updates.[2] It is critical that the updating of any anti-virus software be quick and dependable. Examination of the current Sophos system revealed that it was slow, unreliable and often required manual intervention from an administrator.

The CID on the server was updated by a script scheduled to run every eight hours. SAV clients were installed and configured to check for updates every four hours. This left a window of up to twelve hours in which a new virus could attack without being detected. Increasing the update frequency produced a disruption to the user while it updated because every update that the CID performed

caused the SAV to run a complete update process, even when nothing new was updated. Additionally, the script which performed the IDE updates was prone to failing and would leave a hung process on the server. No updates would happen until the hung process was found and killed. Several weeks would often pass before this was discovered.

Macintosh updates had to be manually performed on the CID, and the CID was made available using ExtremeZ-IP which provided Appletalk services. SAV updates were more complicated, requiring the user to create a connection to the server and then open Sophos. The process of opening Sophos would cause it to check for updates and install any that were found.

Since our primary concern was protection from Windows viruses, this might have been workable except it only worked while computers were connected to the local network. Many professors use laptops on which they do research work, and they often travel off campus for extended periods of time. While these laptops were not connected to the local network, SAV would not update and the computer would not be protected from any new viruses.

Central Monitoring and Configuration

SAV installations which had stopped updating or suffered from a scanning engine that was inactive were often found by chance. Sometimes, the CID would stop updating and not be noticed for several weeks. No system was in place to monitor the status of the anti-virus system regularly with no way to know for sure how well the system was functioning.

In addition, after SAV was installed on a computer, there was no process to change the settings from a central location. For example, to change the way that a virus was handled when found, a technician would have to visit each desktop and change the setting. Due to the complexity and cost of making such a change, they generally were not made.

Reports

After installing and configuring SAV, no mechanism was in place to monitor the effectiveness or efficiency of the system. No means was available to determine the number of viruses that Sophos was intercepting except for the number of phone calls the Help Desk received during a virus outbreak. Likewise, it was difficult to determine which computers were infected with viruses so they could be removed from the network if Sophos were unable to remove the virus automatically.

During Snapshot

After identifying problems with the current anti-virus system and deciding how the system should work, a careful analysis of Sophos and several other products was performed. During the analysis it found that the other products did not offer any significant differences that could not be obtained from Sophos by better

utilization of the product. Combined with the fact that the College was in the middle of a multiyear contract with Sophos, the decision was made to make Sophos work better.

Updates

Updates were the first set of problems that were approached. Using several products in the Sophos Enterprise Manager suite, combined with changes in the way SAV was installed, the concerns of automation, speed and reliability were addressed.

EM Library

The first major change to the anti-virus system was made to the process that managed the CIDs. Part of the Enterprise Manager suite, EM Library is used to create, update and manage CIDs for Sophos anti-virus clients. With EM Library, updates are available automatically, or on demand, from a special, dedicated website. After the Library receives the updates, the CID is automatically updated. Without manual intervention, both virus identification files and the scanning engine can be updated. Emergency updates may be forced with a manual update.

EM Library was installed and the CIDs were moved to a new server to be shared with Microsoft Software Updates Services. A Windows 2000 server operating system has been installed and secured with assistance from Bryce Thompson's paper *Securing Windows 2000 with Security Templates.*[3] Two special configurations to the server have been made: Microsoft Appletalk services have been installed to allow the Macintosh clients to connect to the file shares and update, and guest access has been made available for both the Macintosh and Windows file shares.

After setting up the server, EM Library was installed using the startup guide from Sophos.[4] After installation, a Library was created, packages were selected, a download schedule was set, and the CIDs were created. The latest versions of the Windows 9x, NT/2000 and Macintosh packages were selected to allow the engine updates to be automatically deployed each month. The Library was set to check for updates every hour to minimize the length of time between the release of virus identities and the update.

A file share for the CID has been created on the server and shared as "\\server\interchk." The share was set up to allow connections from Windows and Macintosh computers. On this share, multiple CIDs were configured with customized settings for faculty and staff computers, lab computers and student computers.

Finally, EM Library was configured to send notifications of problems with updates to an email account. If EM Library encounters any errors while trying to

download updates from Sophos or while trying to update the CIDs, an administrator is emailed and paged.

Sophos Anti-virus

Sophos Anti-virus (SAV) is the scanning engine that is installed on each client to provide protection from viruses that attack through email, CD, floppy, network shares, instant messaging or web pages. The client consists of two parts: SAV which provides on-demand and scheduled scanning of files and Intercheck, which provides on-access scanning of a file before it is allowed to be opened or run.

Sophos provides installation and user manuals for each platform that it supports. Manuals for Windows 9x[5], Windows NT/2000[6] and Macintosh[7,8] were downloaded from their website and used. The manuals are well written; but much of the information in the next section is undocumented and has been discovered, created or provided by Sophos technical support. SAV installs have been broken down into the four major types of computers that are encountered: Windows computers in and out of a domain; and Macintosh OS 9 and OS X.

Windows - Domain

Sophos is easiest to use when all the client computers are Windows based and they all belong to a domain. The faculty, staff and lab computers that are supported on campus are all Windows XP computers that are members of the Windows 2000 domain. While this is the simplest of the installs, several undocumented command line options exist.

Windows NT based computers require an update account be established on the domain to be used to start the network update service. Sophos recommends this account be named "sweepupd," and the account requires "logon as service" rights on each computer that it updates. Using Active Directory and group policy, this was easily established.

To maintain a standard install of SAV, a command line configuration has been placed in a script that is run to finish setting up a computer after it is imaged. The command line syntax for Windows 9x and NT is:[9]

```
\\<servername>\Interchk\W95Inst\setup -inl -a

\\<servername>\Interchk\NTInst\i386\setup -a -in -inl -config=1 ➲
      –Updaccount=Domain\Username\password
```

The command line shown non-interactively installs SAV from a network CID on the local machine with Intercheck client enabled. On NT based computers it requires administrative privileges. The –a switch causes the setup to run in a non-interactive mode while the –in switch runs the install without a progress indicator, and –inl prevents the display of the Sophos logo. The –config=1 switch

is used to install Sophos with Intercheck client and auto-updating enabled. This switch must precede the –Updaccount switch which is used to pass the credentials of the network update account to the installer.

In addition to scripting the install of SAV, scripting uninstalls was also useful. The command line syntax for uninstalls is:

```
\\<servername>\Interchk\pathtoCID\setup -remove -ni -force
```

The –remove switch indicates the setup program should use its uninstall mode. Using –ni tells the setup programs to operate in a non-interactive mode. The –force switch tells the setup to force any open Sophos programs to close so the uninstall process can be finished.

Windows - Non-Domain

Sophos Anti-virus will work in a non-domain, or workgroup, environment; however, it becomes more difficult to manage in an automated fashion and from a central point. All of the students on campus with Windows computers fit into this category, making it a significant portion of the clients to manage. This type of install presents interesting challenges, including providing an auto-update account and access to the CIDs.

Without a domain, an account needs to be created on the computer and given the appropriate rights to "logon as a service" to allow SAV to update correctly. In addition, the CID from which it is updating must be accessible to this account. Initially, a set of instructions were developed to walk students through the process. Most students found the five pages of instructions too daunting to bother with, resulting in poor compliance.

Next, the process was automated with a script. The script, which generated the update user and granted it the special rights it required, was distributed to the students. Guest access was granted to the share on the server that stored the CIDs. The script determined which version of Windows was running and would install the correct version of Sophos.

The script reduced the complexity of installing SAV but it still did not resolve other issues, such as off-campus students that used an ISP or students that took their computers home for break. Updates still did not work if the computer was not connected to the campus network. The script was abandoned in favor of using Remote Update which uses a web connection to update and does not rely on special update account or a connection to the local network. A copy of the script is in Appendix A.

Macintosh

The install and update process for SAV on the Macintosh platform is quite different from Windows version. Automation of the installer has not been

attainable; however, the installation process is simpler, making the directions easier to write and follow.

The most significant difference with the Macintosh version of SAV is that it does not require a special account to perform updates. However, the installation and update procedure does require a CID that can provide Apple File Protocol (AFP) connections. To provide this, Microsoft Apple Services have been installed on the server, and a Macintosh share of the CID was created.

OS 9

To install SAV on OS 9 a connection is made to the CID on the server. This is achieved by opening the chooser, selecting Server IP and entering the DNS name or IP for the server containing the CID. When prompted for credentials, guest access is chosen and CID share is selected. To mount the CID as a network drive every time the computer starts, the box next to the share name should be checked.

The installer is started by opening the network drive that is mounted on the desktop and selecting the Sophos Installer. The wizard is short, and all of the defaults settings may be chosen. Updates for SAV are initiated by opening the SAV interface while the CID is mounted rather than on a schedule.

OS X

Except for the process used to create the mount point to the server, the process of installing and updating SAV for OS X are the same as OS 9. A dynamic AFP mount point for the CID is created by making the appropriate entries into the local NetInfo database. With assistance of a colleague, Mike Bowden, a script was written to automate the creation of the mount point:

```
!#/bin/bash
niutil -create . /mounts/<server>
niutil -createprop . /mounts/<server> "opts"
niutil -createprop . /mounts/<server> "vfstype" "url"
niutil -insertval . /mounts/<server> "opts" "net" 0
niutil -insertval . /mounts/<server> "opts" ➲
      "url==afp://;AUTH=NO%20USER%20AUTHENT@<server>/Interchk" 1
niutil -createprop . /mounts/<server> dir "/Network/Servers"
niutil -createprop . /mounts/<server> name "<server>:/Interchk"
```

The shell script uses the command line utility “niutil” to create a dynamic AFP connection to the CID using guest access. SAV still needs to be opened to trigger an update, but the connection to the CID happens automatically and is invisible to the user. It is important to note that SAV requires an AFP connection to the server – SMB connections do not work.

Remote Update for Windows

Remote Update is part of the Enterprise Manager suite providing an easy way to keep remote clients up-to-date. It is targeted at computers that are not always connected to the campus network, but are frequently connected to the Internet. Remote Update utilizes a special agent on the client computer to check for and download SAV updates over a web connection to the CID. Instructions for installing and using Remote Update can be found on the Sophos website.[10]

The first step to configure Remote Update is to reconfigure the server. IIS was installed, configured and secured with help from Michael Wherley's paper *Security Procedures for a new IIS Server.*[11] EM Library was used to create a custom CID which was secured and made accessible with IIS. Finally, a domain account was created to be built into the installer and used to connect to the website.

After establishing Remote Update on the server, the installation of Remote Update was organized to make it as automated as possible. The installer was configured to include the default settings for the DNS name of primary CID and the account and credentials to be used to access the Remote Update website. The agent has been configured to check for updates every 120 minutes.

Winzip Self-Extractor was used to provide a single executable file that automatically launches the setup program for Remote Update. This installed Remote Update, but did not install SAV. To rectify this a script has been created to wrap the Remote Update installer. The script was included in the self-extracting archive to install Remote Update and automatically download and install SAV.[12]

```
IF EXIST "%ProgramFiles%\Sophos\Remote Update\iupdate.exe" GOTO ➲
        UPDATESAV

IF NOT EXIST %temp%\_ISTMP1.DIR GOTO INSTALLREMOTEUPDATE
del %temp%\_ISTMP1.DIR\*.* /q
rmdir %temp%\_ISTMP1.DIR

:INSTALLREMOTEUPDATE
ECHO Installing Remote Update ...
start /wait "Remote Update setup" "C:\Program Files\Sophos\Remote ➲
        Update\servinst\remupd\setup.exe" -nirestart

:BUSYLOOP
IF EXIST %temp%\_ISTMP1.DIR\_INS5576._MP GOTO BUSYLOOP

:UPDATESAV
"%ProgramFiles%\Sophos\Remote update\iupdate.exe" savnt
```

The script checks for an install of Remote Update and if it is not found, it starts the install process. The setup program uses the –nirestart switch to perform a non-interactive install. A temp file is used to figure out when the install has

completed and loops until the installation is completed. On the last line Remote Update starts the install and update process for SAV for NT/2000. The "savnt" option should be substituted with "sav95" to install SAV on a Windows 9x system.

The final product is a single executable that is downloaded and run by the user. The executable installs Remote Update and SAV and the user is left with a system that automatically updates from anywhere on the Internet.

Central Configuration and Monitoring

Configuration with SAVAdmin

SAVAdmin provides real-time monitoring and control of SAV for Windows, enabling administrators to set immediate and scheduled tasks to install, update, change CIDs and reconfigure Windows clients over the network. SAVAdmin has proven itself most useful for pushing emergency updates to all the clients that are currently connected to the network.

The SAVAdmin manual may be found online[13] and includes instructions for performing most tasks. SAVAdmin tasks work well to change and troubleshoot settings on small groups of computers that are known to be online. It also works well to reinstall SAV on individual computers. It was less useful when changing the configuration of a large number of computers, especially if it is not known when they will be online. The scripts in the next section have proven more useful.

Configuration with Scripts

Using an undocumented feature called an "Afterscript"[14], a standard configuration for SAV can be set on the CID and changed as needed. Computers which install or update from this CID use the specified configuration.

First, SAV is installed on a test computer and configure it with desired settings for Intercheck actions, scheduled scans and excluded drives. After SAV is configured, the "Sophos Anti-virus" service (sweepsrv.sys) is stopped, which forces the settings to be written back to the registry. Next, the registry editor is opened and the "HKLM\Software\Sophos" and "HKU\.Default\Software\Sophos" registry branches are exported to a text file named "sophos.reg". In the export file, the entries for "RollOutSerialNumber" and "Version" must be removed to prevent the computers from thinking they have suddenly become out of date after the settings are applied.

Next, a script is created that stops the SAV service, installs the registry settings from the registry export file created and then restarts the SAV service. The script should be named "sophos.cmd":

```
net stop sweepsrv.sys
regedit /s sophos.reg
net start sweepsrv.sys
```

After creating sophos.reg and sophos.cmd they should be copied to the CID that the configuration applies to. The next step is to open the "sav.cfg" file located on the CID and add the following section to the end of the file:

```
[Scripts]
  ScriptFiles=sophos.reg, sophos.cmd
  AfterScript=[RunAlways]%ScriptPath%\sophos.cmd
```

Changing the "sav.cfg" file causes the files listed on the line beginning "ScriptFiles," to be downloaded from the CID and the script specified on the "AfterScript" line to be executed after the installer finishes. "AfterScript" also has the option "Show" which can be specified after "RunAlways". "Show" will force the script being run to display. This script runs under the security context of the System account.

With the configuration described, SAV applies the settings in the script every time an update is performed, thereby wasting network resources and extending the length of the update process. If the configuration is not changed very often, logic should be added to the "sophos.cmd" script to determine if the settings have been applied previously. A script with this logic is available in Appendix B.

Status Monitoring

Status monitoring is used to ensure that SAV is up-to-date and active on all desktop computers. Manual spot inspections have revealed that some SAV installations stopped updating or became inactive. By using SAVAdmin tasks combined with a script, SAV installs that were not functioning correctly are found.

SAVAdmin was installed on a server with two permanent tasks: the first checks the network for computers which are currently connected and the second checks each of the computers for the status of SAV and generates a report. These two tasks are scheduled to run twice a day. A SAVAdmin task is run as a scheduled job by using the command line syntax where <number> is the permanent task number in SAVAdmin you want to run:

```
SAVADMIN.EXE" -TASK=<number>
```

Following the completion of the SAVAdmin tasks, a script is scheduled to run that parses out information about SAV installs that are not updating or are inactive from the report that was generated by SAVAdmin. The information is compiled and sent as an email to an administrator. This script is listed in Appendix C.

Each time the script is run, administrators are automatically notified with a list of computers on which SAV is not correctly running. Armed with this information the administrator uses SAVAdmin to force a reinstall or update of SAV.

Reporting

A reporting mechanism has been added to the anti-virus system to track the effectiveness of the system and allow technicians to identify and fix compromised computers on the network. Another component of the Enterprise Manager suite, EM Reporter, is used to collect alerts generated by SAV and produce a range of reports. Documentation on installing and using EM Reporter may be found on the Sophos website.[15]

Configuration

EM Reporter has been installed on a server which hosts various IT maintenance tools. It consists of two components; the first is an Microsoft Management Console (MMC) used to view canned Crystal Reports and the second is a SQL database used to download and store the data.

A special email account has been established to which SAV sends virus alerts. EM Reporter has been configured to pick up email from this account and insert the information into the SQL database. Additionally, SAV has been reconfigured to send virus alerts to the special email account.

Monitoring

After the reporting system was in place, access was granted to the Help Desk and administrators which need to view reports. The MMC for EM Reporter has also been installed on their desktop computers. This provides the Help Desk and administrators with the ability to check important information such as hosts that are infected with viruses, how SAV reacted to the virus and the most prevalent viruses on the network.

After Snapshot

Risk of infection by a virus to the desktop computers has decreased with the implementation of the anti-virus system. However, the vulnerability has not been eliminated, and because of the reactive methods used to fight viruses it may never be, but the situation is now under control. When a virus outbreak happens, the reaction is a systematic process. Data collected from each incident allows the system to be reevaluated to make it more effective.

Problems Solved

Three primary goals were identified during this project: to increase the reliability, automation and tracking of anti-virus protection for desktop computers. Through the course of this project, these goals have been met.

The reliability of SAV has been dramatically improved in several ways. First, changing from manually updated CIDs to EM Library has eliminated problems with the CID update process hanging. If a problem does occur, an administrator is promptly notified so the situation can be resolved. Next, the implementation of SAVAdmin and scripts has allowed the status of Windows clients to be

monitored. If SAV is found in an inactive state or it is not updating, an administrator is notified so it can be fixed.

Several improvements have made the anti-virus system more automated. In addition to automatic status monitoring and notification, the speed of automatic updates was reduced to less than two hours from the time the IDE is released from Sophos. In an emergency, manual intervention reduces this time to about 20 minutes for desktops actively connected to the network. Scripts have provided a central, standard configuration for SAV that can be changed across the network with very little effort.

EM Reporter has provided a method to measure the effect of a virus outbreak on the desktop computers and how effective the resulting response. Previously this data could only be estimated from the number of calls the Help Desk received. Data reported by SAV allows the number of affected computers to be measured and allows technicians to find and follow up with the computers that were unable to clean the infection automatically.

Problems Remaining

Despite the success of the project, some areas of concern remain. Most of the concerns stem from the fact that most of the automated systems put in place do not work for Macintosh. Specifically, no mechanisms to make central changes to the configuration or monitor the status of the SAV are available. Sophos has indicated that they are working on a product to address these issues.

Another concern is the limitations of the canned reports in EM Reporter. EM Reporter currently requires the use of a special MMC console that needs to be installed for each person who would like to view the reports. The canned reports allow for minor customizations, but do not allow for major changes. Reports pulled from the database and displayed in a web browser would be more helpful.

Conclusion

The results of this project have been very positive, providing much better anti-virus protection for the College's desktop computers. During this project it has been important to identify goals to accomplish and then mold the vendor-supplied solution to fit the goals.

Persistence and creativity have been very helpful. During communication with technical support, the same question often needed to be asked in different ways before enough information was put together to produce a solution. By thinking outside of the box, this information often was used in ways that it was not necessarily intended.

In the end, a reliable and automated desktop anti-virus system with a good tracking system was produced. As with any system it will require constant evaluation and improvement.

References

[1] Josh, Edward. *Introducing Viruses and Sophos Anti-Virus*. November 2002. <http://www.giac.org/practical/GSEC/Edward_Josh_GSEC.pdf>

[2] "'War of the worms' erupts on the net"**.** March 4, 2004. <http://cooltech.iafrica.com/technews/307317.htm>

[3] Thompson, Bryce. *Securing Windows 2000 with Security Templates*. April 2003. <http://www.giac.org/practical/GCWN/Bryce_Thompson_GCWN.pdf>

[4] Sophos. *EM Library Startup Guide*. January 2004. <http://www.sophos.com/sophos/docs/eng/instguid/eml_ien.pdf>

[5] Sophos. *Windows 95/98/Me peer-to-peer network Installation guide*. February 2004. <http://www.sophos.com/sophos/docs/eng/instguid/95_ien.pdf>

[6] Sophos. *Windows NT/2000/XP peer-to-peer network Installation guide*. January 2004. <http://www.sophos.com/sophos/docs/eng/instguid/ntp_ien.pdf>

[7] Sophos. *Mac OS 8 or 9 on a network Installation guide*. February 2004. <http://www.sophos.com/sophos/docs/eng/instguid/mac_ien.pdf>

[8] Sophos. *Mac OS X on a network Installation guide*. February 2004. <http://www.sophos.com/sophos/docs/eng/instguid/mcx_ien.pdf>

[9] Sophos Technical Support. E-mail to the author. December 2003.

[10] Sophos. *Remote Update Administrator guide*. February 2003. <http://www.sophos.com/sophos/docs/eng/instguid/rupa_ien.pdf>

[11] Wherley, Michael. *Security Procedures for a new IIS Server*. May 13. 2003. <http://www.giac.org/practical/GSEC/Michael_Wherley_GSEC.pdf>

[12] Sophos Technical Support. E-mail to author. March 2004.

[13] Sophos. *SAVAdmin User manual*. July 2002. <http://www.sophos.com/sophos/docs/eng/manuals/sadm_men.pdf>

[14] Sophos Technical Support. E-mail to author. February 2004.

[15] Sophos. *EM Reporter Installation guide*. April 2003. <http://www.sophos.com/sophos/docs/eng/instguid/emrep_ien.pdf>

Appendix A

VBScript to create and configure a Sophos update user and install SAV on non-domain Windows computers.

```
Option Explicit
On Error Resume Next

'=========================================================================
' DECLARE VARIABLES
'=========================================================================
Const SOPHOS_ACCT = "sweepupd"
Const SOPHOS_FULLNAME = "Sophos Update"
Const SOPHOS_PWORD = "Sweep1t"
Const SOPHOS_DESC = "DO NOT REMOVE -- Sophos Antivirus Update User"
Const NT_PATH = "\\server\Interchk\NTInst\i386"
Const PATH_9X = "\\server\95Inst"
Const SAV_AGENT = "\\server\95Inst\savagent.exe"
Const SAV_LOC = "c:\windows"
Dim MSG_CONTINUE: MSG_CONTINUE = "You are about to install Sophos ➲
      Anti-Virus on your computer.  This requires" & vbcrlf & "a ➲
      valid network connection.  If you have other anti-virus ➲
      software " & vbcrlf & "on your computer, click 'Cancel' and ➲
      remove it before continuing.  Please call" & vbcrlf & "The ➲
      student Helpdesk if you need assistance."

Dim objNetwork, objShell, objFSO, objFile

'=========================================================================
' MAIN SCRIPT
'=========================================================================
Set objShell = CreateObject("wscript.Shell")
Set objNetwork = CreateObject("wscript.Network")
Set objFSO = CreateObject("Scripting.FileSystemObject")

If MsgBox(MSG_CONTINUE,vbokcancel + vbquestion,"Install Sophos ➲
      Anti-Virus") = vbCancel Then
      WScript.Quit
End If

If GetOS() = "NT" Then

      FindAndDeleteUser SOPHOS_ACCT

      CreateLocalUser SOPHOS_ACCT,SOPHOS_FULLNAME,SOPHOS_PWORD, ➲
            SOPHOS_DESC,True,True

      'grant sophos user log on as service rights
      objShell.Run NT_PATH & "\ntrights.exe +r SEServiceLogonRight ➲
             -u " & SOPHOS_ACCT,0,True

      If CheckForProcess("SWEEPSRV.SYS",False) Then
            'remove old sophos install
            objShell.Run NT_PATH & "\setup.exe -Remove -Force ➲
                  -ni",0,True
```

```
	End If

	If CheckForProcess("setup.exe",False) Then
		'make sure uninstall is done
		WScript.Sleep 5000
	End If

	'run sophos install
	objShell.Run NT_PATH & "\setup.exe -a -IN -INL -Config=1 ➲
		-Updaccount=" & objNetwork.ComputerName & "\" & ➲
		SOPHOS_ACCT & "\" & SOPHOS_PWORD,0,True

	Do while CheckForProcess("setup.exe",False)
		'setup still running
		WScript.Sleep 2000
		If CheckForProcess("swupdate.exe",False) Then
			WScript.Sleep 2000
			Exit Do
		End If
	Loop
Else '9x computer
	'copy savagent to local computer and set regkey to auto run
	objFSO.CopyFile SAV_AGENT, SAV_LOC & "\savagent.exe"
	objShell.RegWrite "HKLM\Software\Microsoft\Windows\ ➲
		CurrentVersion\Run\SophosAgent",SAV_LOC & "\savagent.exe"
	'install sophos
	objShell.Run PATH_9X & "\setup.exe -inl -a",0,True

End If

'=========================================================================
' FUNCTIONS
'=========================================================================
Function FindAndDeleteUser(strUser)
	Dim objDomain, objUser

	Set objDomain = GetObject("WinNT://.")

	objDomain.Filter = Array("user")
	For Each objUser In objDomain
		If objUser.name = strUser Then
			objDomain.Delete "User", strUser
			FindAndDeleteUser = True
		Else
			FindAndDeleteUser = False
		End If
	Next
End Function

Function CreateLocalUser(strUser, strFullName, strPassword, strDesc, ➲
bPasswordExpire, bPasswordCantChange)
	Const UF_ACCOUNTDISABLE       = 2
	Const UF_LOCKOUT              = 16
	Const UF_PASSWD_NOTREQD       = 32
	Const UF_PASSWD_CANT_CHANGE = 64
	Const UF_DONTEXPIRE_PASSWD    = 65536
```

```
	Dim objLocalPC, objUser

	Set objLocalPC = GetObject("WinNT://.")
	Set objUser = objLocalPC.Create("User", strUser)

	objUser.SetPassword strPassword
	objUser.FullName = strFullName
	objUser.Description = strDesc

	'Set user flags
	If bPasswordExpire Then 'Don't expire the password
		objUser.userFlags = objUser.userFlags Or ➲
			UF_DONTEXPIRE_PASSWD
	Else 'Set password to expire
		objUser.userFlags = objUser.userFlags And Not ➲
			UF_DONTEXPIRE_PASSWD
	End If
	If bPasswordCantChange Then 'The user can't change the password
		objUser.userFlags = objUser.userFlags Or ➲
			UF_PASSWD_CANT_CHANGE
	Else 'Allow user to change password
		objUser.userFlags = objUser.userFlags And Not ➲
			UF_PASSWD_CANT_CHANGE
	End If

	'Save it
	objUser.SetInfo

	CreateLocalUser = 1

End Function

Function GetOS()'Returns the Operating system version
	On Error Resume Next
	Dim strVersion, oShell

	Set oShell = CreateObject("WScript.Shell")
	strVersion = oShell.RegRead("HKLM\SOFTWARE\Microsoft\Windows ➲
		NT\CurrentVersion\CurrentVersion")
	If strVersion = "5.0" Or strVersion = "5.1" Then '2k or XP
		GetOS="NT"
	Else
		GetOS="9x"
	End If
End Function

Function RegkeyExist(strKey)
	'Checks for the existance of specified registry key
	On Error Resume Next
	Dim strTest
	Err.Clear
	strTest = objShell.RegRead(strKey)
	If Err.Number <> 0 Then 'it doesn't exist
		RegkeyExist = False
	Else
```

```
            RegkeyExist = True
      End If
      Err.Clear
End Function

Function CheckForProcess(strProcess, bTerminate)
      'Checks for running processes and terminiates if asked
      'Returns TRUE if found

      Dim bFound, objWMIService, colProcessList, objProcess

      bFound = FALSE

      Set objWMIService = GetObject("winmgmts:{impersonationLevel= ➲
            impersonate}!\\.\root\cimv2")
      Set colProcessList = objWMIService.ExecQuery("Select * from ➲
            Win32_Process Where Name = '" & strProcess & "'")
      For Each objProcess in colProcessList
          bFound = TRUE
          If bTerminate = TRUE Then
                objProcess.Terminate()
            End If
      Next

      CheckForProcess = bFound

End Function
```

Appendix B

NT Command script to apply Sophos Anti-virus settings with logic to keep track of which configuration it has applied:

```
SET rollout=1

IF EXIST "%windir%\sophossettings.lok" GOTO CHKVER
GOTO SETREG

:CHKVER
FOR /f %%v IN (%windir%\sophossettings.lok) DO SET value=%%v
IF NOT %value% LSS %rollout% GOTO END

:SETREG
REM Apply Registry Settings
NET STOP SWEEPSRV.SYS
REGEDIT /S SOPHOS.REG
NET START SWEEPSRV.SYS

ECHO %rollout% > %WINDIR%\SOPHOSSETTINGS.LOK

GOTO END

:END
```

Appendix C

VBScript to parse report from SAVAdmin, checking for inactive or out of date SAV installations:

```
Option Explicit
On Error Resume Next

'=====================================================================
' DECLARE VARIABLES
'=====================================================================
Const FROM = "email@domain.edu"
Const FILE = "d:\path\to\report.csv"

Dim strNotInstalled, strOutOfDate, strICInactive, strDate
Dim strFullReport
Dim aKeys, aDate, aEmails, aData
Dim dicData, i, k
Dim objFSO, objTextFile

'List of email addresses to send the report To
'To send report to more addresses, add them to the array below.
aEmails = Array("email@domain.edu")

'=====================================================================
' MAIN SCRIPT
'=====================================================================
Set objFSO = CreateObject("Scripting.FileSystemObject")
Set objTextFile = objFSO.OpenTextFile(FILE)
Set dicData = CreateObject("Scripting.Dictionary")

'Start processing file - first 5 lines can be skipped
objTextFile.SkipLine
objTextFile.SkipLine
objTextFile.SkipLine
objTextFile.SkipLine
objTextFile.SkipLine

'Get Report Date
aDate = Split(objTextFile.readline,",")
strDate = aDate(0) & "at" & aDate(1)

'Skip another blank line
objTextFile.SkipLine

'Get column Keys
aKeys = Split(objTextFile.readline,",")
For i = 1 To UBound(aKeys)
      dicData.add aKeys(i),Null
Next

'Skip another blank line
objTextFile.SkipLine

'Process the bulk of the data
```

```
Do While Not objTextFile.AtEndOfStream
      aData = Split(objTextFile.readline,",")
      For i = 1 To UBound(aKeys)
            dicData.Item(aKeys(i)) = (aData(i))
      Next
      ProcessData
Loop

'Send emails to the list above
strFullReport = DisplayReport()
For k = 0 To UBound(aEmails)
      SendMailNotification strFullReport, "Sophos Report for " & ➲
            Now, aEmails(k), FROM
Next

'=====================================================================
' FUNCTIONS
'=====================================================================
Function ProcessData()
      'Report not installed/not active computers
      If dicData.item("Access") = "Full" and dicData.item("SAV ➲
            Installed") <> "Installed" Then
            strNotInstalled = strNotInstalled & dicData.item ➲
                  ("Computer") & vbtab & dicData.item("SAV Version")➲
                   & vbtab & dicData.item("Rollout") & vbtab & ➲
                  dicData.item("SAV Active") & vbcrlf
      elseIf dicData.item("IC Client") = "Inactive" Then
            strICInactive = strICInactive & dicData.item("Computer") ➲
                  & vbtab & dicData.item("SAV Version") & vbtab & ➲
                  dicData.item("Rollout") & vbtab & dicData.item("SAV ➲
                  Active") & vbcrlf
      elseIf dicData.item("Up to Date") = "Out of date" Then
            strOutOfDate = strOutOfDate& dicData.item("Computer") & ➲
                  vbtab & dicData.item("SAV Version") & vbtab & ➲
                  dicData.item("Rollout") & vbtab & dicData.item("SAV ➲
                  Active") & vbcrlf
      End If

End Function

Function DisplayReport()
      Dim strReport, strHeader
      strHeader = vbcrlf & "PCName" & vbtab & "Version" & vbtab & ➲
            "Rollout" & vbtab & "Status" & vbcrlf

      If strNotInstalled = "" And strICInactive = "" And strOutOfDate➲
             = "" Then WScript.quit 'nothing to report

      strReport = strDate & vbcrlf & vbcrlf
      If strNotInstalled <> "" Then strReport = strReport & "SAV NOT ➲
            INSTALLED OR IS INACTIVE" & vbcrlf & strHeader & ➲
            strNotInstalled & vbcrlf
      If strICInactive <> "" Then strReport = strReport &  "INTERCHECK➲
            INACTIVE" & vbcrlf & strHeader & strICInactive & vbcrlf
      If strOutOfDate <> "" Then strReport = strReport &  "SAV OUT OF ➲
            DATE" & vbcrlf & strHeader & strOutOfDate & vbcrlf
```

```
      DisplayReport = strReport
End Function

Function SendMailNotification(strMessage, strSubject, strTo, strFrom)
      'REF:  MS KB Article Q286431
      Dim msg

      set msg = WScript.CreateObject("CDO.Message")

      msg.From = strFrom
      msg.To = strTo
      msg.Subject = strSubject
      msg.TextBody = strMessage

      msg.Configuration.Fields("http://schemas.microsoft.com/cdo/config
uration/smtpserver") = "mail.domain.edu"
      msg.Configuration.Fields("http://schemas.microsoft.com/cdo/config
uration/sendusing") = 2
      msg.Configuration.Fields.Update

      msg.Send

End Function
```

Last Updated: June 26th, 2017

Upcoming Training

SANS London July 2017	London, United Kingdom	Jul 03, 2017 - Jul 08, 2017	Live Event
Cyber Defence Japan 2017	Tokyo, Japan	Jul 05, 2017 - Jul 15, 2017	Live Event
SANS Munich Summer 2017	Munich, Germany	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Cyber Defence Singapore 2017	Singapore, Singapore	Jul 10, 2017 - Jul 15, 2017	Live Event
SANS Los Angeles - Long Beach 2017	Long Beach, CA	Jul 10, 2017 - Jul 15, 2017	Live Event
Community SANS Phoenix SEC401	Phoenix, AZ	Jul 10, 2017 - Jul 15, 2017	Community SANS
Mentor Session - SEC401	Ventura, CA	Jul 12, 2017 - Sep 13, 2017	Mentor
Mentor Session - SEC401	Macon, GA	Jul 12, 2017 - Aug 23, 2017	Mentor
Community SANS Atlanta SEC401	Atlanta, GA	Jul 17, 2017 - Jul 22, 2017	Community SANS
SANSFIRE 2017	Washington, DC	Jul 22, 2017 - Jul 29, 2017	Live Event
SANSFIRE 2017 - SEC401: Security Essentials Bootcamp Style	Washington, DC	Jul 24, 2017 - Jul 29, 2017	vLive
Community SANS Fort Lauderdale SEC401	Fort Lauderdale, FL	Jul 31, 2017 - Aug 05, 2017	Community SANS
SANS San Antonio 2017	San Antonio, TX	Aug 06, 2017 - Aug 11, 2017	Live Event
SANS Boston 2017	Boston, MA	Aug 07, 2017 - Aug 12, 2017	Live Event
SANS Prague 2017	Prague, Czech Republic	Aug 07, 2017 - Aug 12, 2017	Live Event
Community SANS Omaha SEC401*	Omaha, NE	Aug 14, 2017 - Aug 19, 2017	Community SANS
SANS New York City 2017	New York City, NY	Aug 14, 2017 - Aug 19, 2017	Live Event
SANS Salt Lake City 2017	Salt Lake City, UT	Aug 14, 2017 - Aug 19, 2017	Live Event
Community SANS Trenton SEC401	Trenton, NJ	Aug 21, 2017 - Aug 26, 2017	Community SANS
Community SANS San Diego SEC401	San Diego, CA	Aug 21, 2017 - Aug 26, 2017	Community SANS
SANS Virginia Beach 2017	Virginia Beach, VA	Aug 21, 2017 - Sep 01, 2017	Live Event
Virginia Beach 2017 - SEC401: Security Essentials Bootcamp Style	Virginia Beach, VA	Aug 21, 2017 - Aug 26, 2017	vLive
SANS Adelaide 2017	Adelaide, Australia	Aug 21, 2017 - Aug 26, 2017	Live Event
SANS Chicago 2017	Chicago, IL	Aug 21, 2017 - Aug 26, 2017	Live Event
Mentor Session - SEC401	Minneapolis, MN	Aug 29, 2017 - Oct 10, 2017	Mentor
SANS Tampa - Clearwater 2017	Clearwater, FL	Sep 05, 2017 - Sep 10, 2017	Live Event
SANS San Francisco Fall 2017	San Francisco, CA	Sep 05, 2017 - Sep 10, 2017	Live Event
Mentor Session - SEC401	Edmonton, AB	Sep 06, 2017 - Oct 18, 2017	Mentor
SANS Network Security 2017	Las Vegas, NV	Sep 10, 2017 - Sep 17, 2017	Live Event
Community SANS Albany SEC401	Albany, NY	Sep 11, 2017 - Sep 16, 2017	Community SANS
Community SANS Dallas SEC401	Dallas, TX	Sep 18, 2017 - Sep 23, 2017	Community SANS