Global Information Assurance Certification Paper

STUDENT: Christopher Aiken 8/15/2000

SUBJECT: GIAC Advanced Incident Handling & Hacker Exploits Practicum

General.

I am the Director of Information Management for one of the states that make up the Army National Guard. The incident described in this paper was memorable in that like previous viruses that have affected our organization, it caused problems, but more so, it was the lynch pin for reviewing our security posture and incident handling measures.

This incident describes my staff's involvement with the Life Stages Worm, which is described by Symantec Corporation as **VBS.Stages.A.worm**. This incident started on 6/12/00 when our Help Desk was notified by a couple of personnel that received this virus in their email. Unfortunately, one of the individuals had already opened the email attachment and caused it to replicate itself to others.

We realized by that afternoon that this virus was quickly spreading and sent out a notice to everyone to not open any emails that contained the words: "Funny", "Life stages" or "Jokes". We also notified our higher headquarters of the incident as well asked about any fixes. While they were aware of the incident, they did not have fixes for it at the time. As a matter of fact, most of the tainted mail was coming from them to us.

We were able to manually fix this problem by a two-fold approach: 1) engaging a rule (see later in this paper) within individual email program (Microsoft Outlook 97/98), and 2) maximizing the filtering capability of our Microsoft Exchange Anti-Virus Program, Symantec Version 2.0. On 6/19/00, Symantec released their latest definition file that would clean this particular virus. On 6/21/00, we were "officially" advised by our CERT system about the virus. Luckily, we had already resolved the situation.

The management of this incident by my staff led me to the realization that better incident handling was required. Since, some of my staff have taken the Army National Guard web-based version of Incident Response Handling which is modeled after the SANS Advanced Incident Handling. This has heightened our awareness and desire to become better educated in various components of computer security.

Executive Summary, including diagrams.

Symantec identified this virus as a worm named **VBS.Stages.A.worm** and is classified as a Bloodhound.VBS.Worm. This worm appears as an attachment titled LIFE_STAGES.TXT.SHS. According to Symantec, execution of this attachment opens a text file into Notepad or email reader and displays the male and female stages of life. While the user reads the text file, the script starts executing in the background. The worm spreads itself using Outlook, mIRC and PIRCH. Symantec recommends corporate customers configure their email filtering systems to filter out or stop all incoming emails that have attachments with .SHS extensions.

A description of each of the six stages of incident handling

As previously mentioned, this incident opened our eyes on what needs to be established for responding to computer incidents.

Preparation

We have already established a standard procedure in response to any incident. Users have been instructed by both training and policy to immediately contact our Help Desk upon encountering an incident.

Incidents are recorded on a help desk ticket and are tracked by ticket number. We input ticket information into a database so as to record particular details concerning an incident as well as record resources rendered, i.e. equipment repairs, personnel hours expended, and knowledge notes for future reference. While documentation is sometimes lacking, it is an area we constantly emphasize due to the importance of good documentation in resolving future occurrences.

Incidents such as this particular one are telephonically relayed to our Network Operations Center (NOC) so that the System Administrator is advised of the situation. In turn the supervisor and then myself are notified. Upon confirmation of the situation, the supervisor or myself will contact the National Guard Bureau (NGB) CERT.

Identification

We advised NGB on 6/12/00 on this situation. They were already aware of this virus and were busily trying to eradicate it from their systems and staffs at the time.

We also sent out an email to all personnel to warn them of opening any emails that contained the words "Funny", "Life stages" or "Jokes" in the subject block. They were instructed to immediately delete the email without opening it. We also verbally advised personnel at various staff meetings and while conducting our daily activities.

Since the virus had spread quickly, we established a "tiger" team comprised of Help Desk members to go around and ensure that everyone's workstation had the Norton Anti-Virus (NAV) and that it was properly set up to be "managed" by the corporate version we ran in our NOC. Each workstation reviewed was to be reported to our NOC for confirmation that it was "picked up" by the NAV corporate edition software.

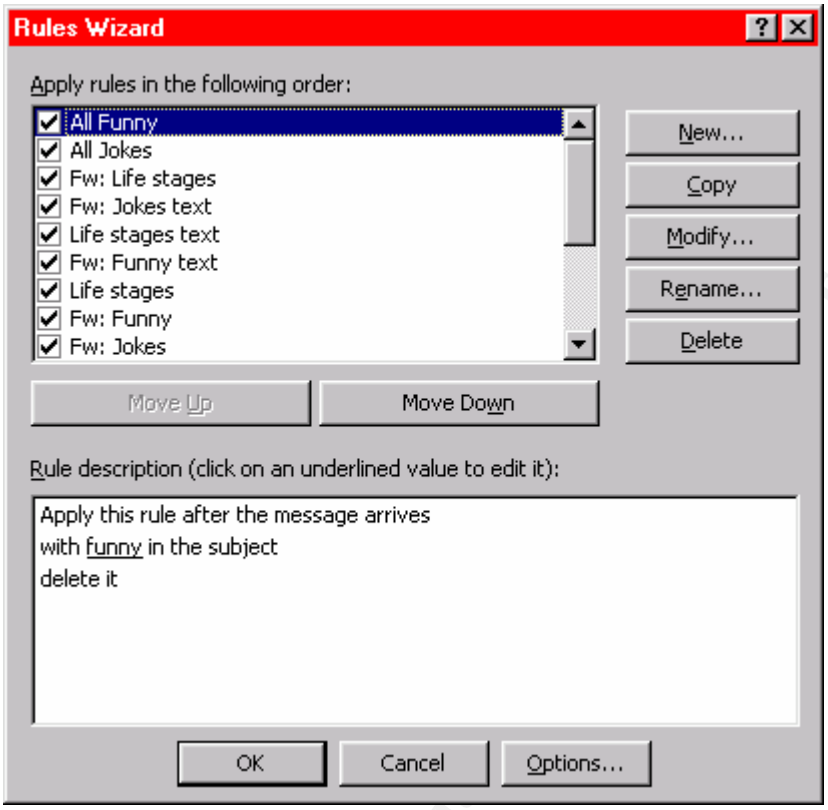
The Help Desk supervisor prepared an instruction letter that identified exactly the steps for reviewing, setting up and confirming the NAV client software on the workstation.

Containment

The virus was difficult to contain in that we did not have a fix to stop its propagation throughout our domain. We could tell by looking at the NAV for Exchange reports that it was coming at a

very fast rate. At this time, we did not have a new 'DAT' file available from Symantec to install. We only had two recourses available to us at this time. First was to constantly advise everyone to be vigilant for emails with the virus and to delete it immediately.

The second course of action was to engage the rules of Microsoft Outlook to delete emails with the words in the subject header.



Eradication

On 6/19/00, NAV released new virus definitions that would detect the VBS.Stages.A.worm. This allowed the NAV for Exchange to catch all incoming infected emails and either clean or delete them. Initially, the fix did not clean the files; therefore, we opted to 'quarantine' them. However, this proved to be wasteful for system resources and was quickly filling up our reports logs on NAV for Exchange. On 6/22/00, we changed the options to automatically delete the files upon identification by NAV for Exchange.

Within a few days, the virus appeared under control. Individuals were aware to delete any infected emails received (which were almost none). The Outlook rules caught any that passed through the NAV for Exchange which may have been none. The NAV for Exchange was reporting deletion of a high number of the virus upon entry into the organization.

NAV FOR EXCHANGE STATISTICS

Norton AntiVirus started on: **6/21/00 8:48 PM**
Number virus definitions: **47423**
Virus definitions date: **6/21/00 12:00 AM**
Action on detection: **Repair**
Number of emails processed: **5795**
Attachments processed: **2791**
Average scan time (ms): **795**
Total KBytes processed: **116678**
Infected attachments found: **2712**
Logged only: **0**
Quarantined: **2712**
Deleted: **2712**
Repaired: **0**
----------NAV Statistics----------

The analysis of this virus as determined by both Symantec and the Army CERT disclosed the following characteristics about this virus.

Names: IRC/Stages.worm, Life_Stages Worm, VBS_Stages.A
Category: Worm
Size: 39,936 bytes
Virus definition: June 16, 2000
Threat assessment: Wild: High
Damage: Low
Distribution: High
Number of infections: 50-999
Number of sites: More than 10
Geographic distribution: High
Threat containment: Easy
Removal: Difficult
Payload trigger: Execution of the LIFE_STAGES.TXT.SHS attachment
Payload:
Large scale emailing: Sends mail to as many as 100 randomly selected addresses from your MS Outlook address book
Modifies files: System registry, Regedit.exe, Mirc.ini
Causes system instability: Could overload mail servers

Distribution:
Subject of email: There are 12 possibilities for the subject of the email
Name of attachment: LIFE_STAGES.TXT.SHS
Size of attachment: 39,936 bytes
Shared drives: Copies itself to mapped drives
Reference: http://www.symantec.com/

Symantec described this file as an SHS file, which is a Microsoft Scrap Object file. These types of files are executable and can contain a wide variety of objects. The scrap object (SHS) extension does not appear in Windows Explorer. These files are the most unpredictable file types of all, since they can be anything from an authentic file to a Trojan application. In this case, the file cannot be trusted.

This virus does contain content that is displayed while it installing itself into the local host. The following contents of the file is shown:

----------Copy of displayed text----------
-The male stages of life:

Age. Seduction lines.
17 My parents are away for the weekend.
25 My girlfriend is away for the weekend.
35 My fiancee is away for the weekend.
48 My wife is away for the weekend.
66 My second wife is dead.

Age. Favorite sport.
17 Sex.
25 Sex.
35 Sex.
48 Sex.
66 Napping.

Age. Definiton of a successful date.
17 Tongue.
25 Breakfast.
35 She didn't set back my therapy.
48 I didn't have to meet her kids.
66 Got home alive.

- The female stages of life:

Age. Favourite fantasy.
17 Tall, dark and hansome.
25 Tall, dark and hansome with money.
35 Tall, dark and hansome with money and a brain.
48 A man with hair.
66 A man.

Age. Ideal date.
17 He offers to pay.
25 He pays.
35 He cooks breakfast next morning.

48 He cooks breakfast next morning for the kids.
66 He can chew his breakfast.
----------End of displayed text----------

Symantec states that the worm sends an email to all contacts in the user's Microsoft Outlook Address book if there are less than 101 addresses. If the number of addresses exceeds 100, the worm will randomly select 100 addresses as recipients. The email contains the LIFE_STAGES.TXT.SHS attachment. The subject of the email is randomly generated and can be one of twelve strings. It may or may not begin with "Fw:". It will contain "Life stages", "Funny" or "Jokes" and may or may not be followed by "text". Examples would be "Fw: Life stages", "Jokes text" or "Fw: Funny text". The worm deletes copies of the emails after they have been sent to insure there is no record of its presence.

An unusual aspect of the SHS file is that the extension remains hidden, even though the operating system is set to show file extensions. In this case, this helps to confuse the user into believing the file is really a '.TXT' file type. Double clicking on the file installs the worm in the following manner.
----------System Changes----------

Moves REGEDIT.EXE from the Windows folder to the recycle bin as "RECYCLED.VXD" and modifies the registry to use this relocated file when importing or using registry type files

Creates files of random names throughout the local system and all available drives. Fixed names include the following:

c:\WINDOWS\[machine name].acl
c:\WINDOWS\SYSTEM\MSINFO16.TLB
c:\WINDOWS\SYSTEM\SCANREG.VBS
c:\WINDOWS\SYSTEM\VBASET.OLB
c:\RECYCLED\DBINDEX.VBS
c:\RECYCLED\MSRCYCLD.DAT
c:\RECYCLED\RCYCLDBN.DAT
c:\RECYCLED\RECYCLED.VXD (really REGEDIT.EXE)

The following are examples of random names generated:

c:\report.txt.shs
c:\My Documents\IMPORTANT.TXT.SHS
c:\WINDOWS\LIFE_STAGES.TXT.SHS
c:\WINDOWS\Start Menu\Programs\unknown_805.txt.shs In the creation of random named SHS files, this worm uses the following algorithm to determine a name: ([Random1]+[Random2]+[Random3])+TXT+SHS.

[Random1] is a selection of one of five choices:

"IMPORTANT"

"INFO"
"REPORT"
"SECRET"
"UNKNOWN"

[Random2] is a selection of one of two choices:

"-"
" "
"_"

[Random3] is a randomly generated number between 0 and 999. The combination of these three randomizations results in 10,000 possible different names.

Modifies the registry to run SCANREG.VBS at Windows startup.

Modifies the registry to run DBINDEX.VBS when loading ICQ.

Modifies the registry to run RECYCLED.VXD when calls are made to run REGEDIT type files.

Modifies MIRC.INI to load an auxiliary script file for PIRCH/mIRC installations.

Creates SOUND32B.DLL whenever Windows restarts in the Windows folder via SCANREG.VBS. SOUND32B.DLL is an auxiliary script file called by MIRC.INI. SOUND32B.DLL contains instructions to send the file LIFE_STAGES.TXT.SHS when connecting to IRC channels.

Modifies the following registry settings (to recover, modify these to original "from" settings):

HKLM\Software\CLASSES\regfile\DefaultIcon
Value "@":
from "C:\WINDOWS\regedit.exe,1"
to "C:\RECYCLED\RECYCLED.VXD,1"

HKLM\Software\CLASSES\regfile\shell\open\command
Value "@":
from "regedit.exe "%1""
to "C:\RECYCLED\RECYCLED.VXD "%1""

Creates the following registry settings (to recover, delete these keys):

HKU\.DEFAULT\Software\Mirabilis\ICQ\Agent\Apps\ICQ\
Parameters="C:\RECYCLED\DBINDEX.VBS"
HKU\.DEFAULT\Software\Mirabilis\ICQ\Agent\Apps\ICQ\
Path="C:\WINDOWS\WSCRIPT.EXE"
HKU\.DEFAULT\Software\Mirabilis\ICQ\Agent\Apps\ICQ\
Startup="C:\WINDOWS"

HKLM\Software\CLASSES\txtfile\
AlwaysShowExt=""

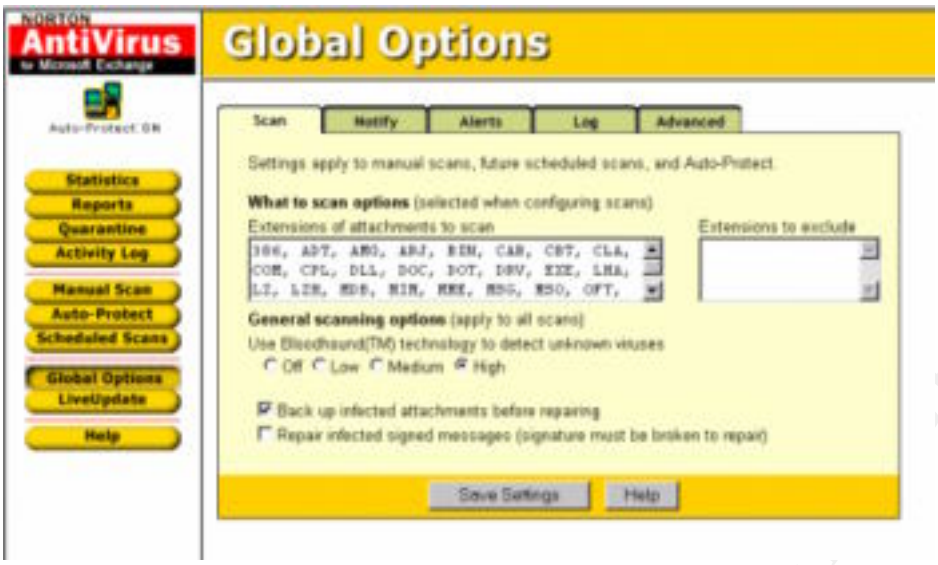
HKLM\Software\Microsoft\Windows\CurrentVersion\
OSName="Microsoft Windows"
HKLM\Software\Microsoft\Windows\CurrentVersion\RunServices\
ScanReg="C:\WINDOWS\WSCRIPT.EXE C:\WINDOWS\SYSTEM\SCANREG.VBS"
----------End of System Changes----------

As mentioned, the user cannot see the SHS file extension with Explorer. The reason for this is due to a registry entry for Shell Scrap file types:

HKEY_CLASSES_ROOT\ShellScrap
"NeverShowExt"="0"

This can be corrected by renaming the entry above from "NeverShowExt" to "AlwaysShowExt" or by deleting the entry. Once it is modified, the system must be restarted for the change to take effect.

Symantec's recommendation for removal of the virus is to use the specified engine and DAT files on their anti-virus program for detection and removal. On 6/19/00, we were able to update our NAV for Exchange and handle the virus.



It should be noted that we elected to have our NAV for Exchange scan all attachments and all mailboxes. While this may be more resource intensive, we feel it is a more prudent and safer solution.

Symantec also developed a tool called 'fixlife.exe' that repairs the changes to a client or local computer system caused by the virus. The user can execute this file by clicking 'Start', 'Run' after typing the following in the Run dialogue box: 'C:\Windows\Desktop\fixlife.exe'. Clicking 'Enter' starts the automatic program.

Recovery

On 6/20/00, we declared ourselves as in control. We advised NGB that our NAV for Exchange was eliminating the virus from entering our domain and infesting our users. Over the next few days, we went to each staff and checked users and their systems. Users were well informed about immediately deleting infected files. Only one workstation was brought in to our Help Desk for deeper review. The Help Desk was unable to determine the cause of the system crash and suspected that it was due to a driver corruption. The Help Desk reformatted the hard disk and reinstalled our standard system software from a ghosted drive.

The following recommendations were identified from this situation.

1. Install new Microsoft update for Outlook that identifies email attachments. We decided to await NGB review and recommendation.

2. Ensure that macro protection is on within Office applications. This setting is set on in our ghost installs of software on our systems.

3. Ensure that everyone is using the anti-virus program. Confirm that it is updated and set up as managed by the corporate version administered by our staff. This is a standard operating procedure in place.

4. Establish procedures to maintain signature files and scanning engine up to date. The Network Administrator and System Administrator check weekly. Our NAV for Exchange and NAV Corporate Version each check the Symantec web site each night for updates.

5. Administer goodwill for those that report a suspected virus. The earlier we can catch it, the easier the work may be. User awareness and cooperation is key to minimizing damage.

6. Ensure that our systems, servers and firewalls are secure. Download the latest security patches and install them correctly. The Network Administrator and System Administrator check weekly. NOC supervisor, new CERT team and myself will review.

7. Know and understand our system's normal baseline operating parameters, so differences are quickly spotted and investigated. CERT team will review and validate baseline requirements.

8. Develop, prepare and implement contingency plans. After completing training, the staff along with our new CERT team will develop improved policies, training and inspection documents.

9. Train, develop and support our new CERT team. This team will provide much needed security support to our existing infrastructure and user training.

Follow up or lessons learned

The security measures taken in response to this incident opened our eyes and alerted the command on the potential seriousness and consequences of viruses and the like. This has fostered a climate for much needed training and development. All key members of our staff have completed a computer security awareness class and the Army Guard version of Incident Response Handling training. We plan to train all members of this staff on these facets of security and incident handling.

As mentioned, we have stood up a CERT team. While this team is made up of drilling reservists, it will add enhanced security to our operations as well as another perspective. At least two personnel on this team are full-time with our staff, which gives us an extra layer of protection that we did not have before.

For at least one operating system involved in the incident, show the process used to assess and contain, including screen shots and operating system commands. In this section, you should describe your jump kit, or all the tools that you used.

The operating system involved in this situation was NT 4.0, which is our primary operating system. All systems in the command are networked; therefore, they are inside our perimeter (which is pending a Firewall and an Intrusion Detection System). Effects on the operating system are noted under **Eradication**.

While the Army CERT and Symantec performed the actual effects upon the operating system, the information was shared and reviewed among the technical members of the staff for their own knowledge and understanding of virus attacks.

Since completing this class, we have established a core team that consists of the following members:

Director – Team Chief provides direction and coordinates with staff and external organizations.

Chief of Help Desk – with four (4) additional members from his staff (also is the CERT Team Leader on drills). Members provide technical and mechanical support on client systems.

Chief of NOC – with two (2) additional members from her staff provides network and system administration support of network resources.

Physical Security Officer – administers physical security requirements and coordinates with our plans and operations directorate.

Staff Judge Advocate – on call to provide legal assistance.

CERT Team – can be mobilized during an emergency.

We are in the process of ordering laptops for each member, reviewing and cataloging software tools for use in various situations, establishing a test lab for training and development, and working with another established CERT for training. While we are still in the embryonic stage, we have taken the necessary steps to immeasurably improving our security posture.

For at least one operating system involved in the incident, describe in detail the process used to back up the system. This write-up should include descriptions of the hardware, commands, and any problems that you ran into.

Our Exchange server has a RAID 5 assembly to protect our data. Additionally, we use NT back up for our Exchange server, which is backed up weekly. We are implementing a data backup service that will place the information stores on another array of drives that are both RAID 5 and backed up on the fly by a daily scheduler. The backups are on tape, which a weekly version is picked up by a commercial backup file company.

The following sequence is used for backing up our Exchange server.

Start>Settings>Control Panel>Services
Goto Microsoft Exchange Message Transfer
Stop>OK
Microsoft Exchange System Attendant
Stop>OK
Microsoft Exchange Event Service

Stop>OK

This turns off the Exchange services and locks the private and public information stores, which prevents corruption of the data files.

Now we follow the Stac Replica procedures for backing up the server.

Log in with Administrator privileges.
Mount tape in tape drive.
Start>Programs>Stac Replica for Windows NT>Replica
OK – Stac Replica Single Server Edition Screen appears
Click maximize on window
Click Operation>Replicate
Click Source tab – Partitions show up on the left-hand screen. Ensure that each has a red check next to them.
Click Schedule tab – you're prompted for when to run schedule
Click on Immediate tab
Click Options tab – make sure Overwrite radio button is marked. All others blank.
Click Start – Start/Submit screen appears. Enter job (server) and description (type backup).
Click OK
Click History tab – shows all events associated with this job. Be sure to press F5 to refresh.
When job is completed, click File>Exit
Remove tape from drive
Store tape in tape room.

Describe in detail the chain of custody procedures used, any affirmations, and a listing of all evidence.

This incident did not involve chain of custody or evidence collection requirements. Nevertheless, we were cognizant of the requirement for possible legal action concerning the initiation of the virus. It was for this reason we elected to retain all the viruses in quarantine until NGB advised us that this was not necessary. Although, we have changed the options on our server to delete this virus, we still have copies on hand should the need arise for someone to conduct further analysis. This evidence is on a floppy disk and has been placed in our commercial backup file facility.

Conclusion

This was a tremendous learning experience for our staff and organization. With the advent of Y2K followed by the numerous episodes of web page hacks, computer intrusions and virus attacks, our command (along with many in the area) have become acutely aware of the potential danger to our systems and most importantly, to our users. Today, many of our users are totally dependent upon unencumbered access to their data and assurance that it is current, accurate and

valid. The security of the infrastructure, our systems and continual support to our users has become extremely important and imperative to mission accomplishment.

References

Symantec Corporation, 20330 Stevens Creek Boulevard, Cupertino, CA 95014 USA http://www.symantec.com/

Army Computer Emergency Response Team (ACERT), Suite B211, 8825 Beulah Street, Fort Belvoir, VA 22060-5246 acert@liwa.belvoir.army.mil

Advanced Incident Handling and Hacker Exploits Course, SANS Institute, 5401 Westbard Ave. Suite 1501, Bethesda, MD 20816 sans@sans.org