Global Information Assurance Certification Paper

VBS/VBSWG.j@MM

Jennifer L. Wheeler

Introduction

Being vulnerable to virus attacks means gambling the confidence and security of company data and value with complete strangers. That is, you can receive a damaging virus from a malicious user hundreds or thousands of miles away, who may not know it's recipients, or even care. The fact is that more and more companies, like the one I work for, store and process all critical company information on computers. Unlike technology companies where daily business actually comes to a stop when computers are offline, our company simply is unable to function normally without them. E-mail, planning, sales and marketing, development, and payroll all contain critical information that would seriously compromise the company if unrecoverable from destruction or spread via virus to competitors.

Overview

On February 12, 2001 I noticed a high volume of viruses being blocked by groupshield. ~~groupshield catching a virus~~ (see example in figure 1). ~~That virus~~ The virus in question was a worm called VBS/SST. A worm, as opposed to a virus, is a self-contained program with the ability to spread itself. This worm was originally discovered in August of 2000, but had no description associated with it until Feb 12, 2001. At that time it was named VBS/VBSWG.j@MM and was given a risk assessment of "High" by NAI.

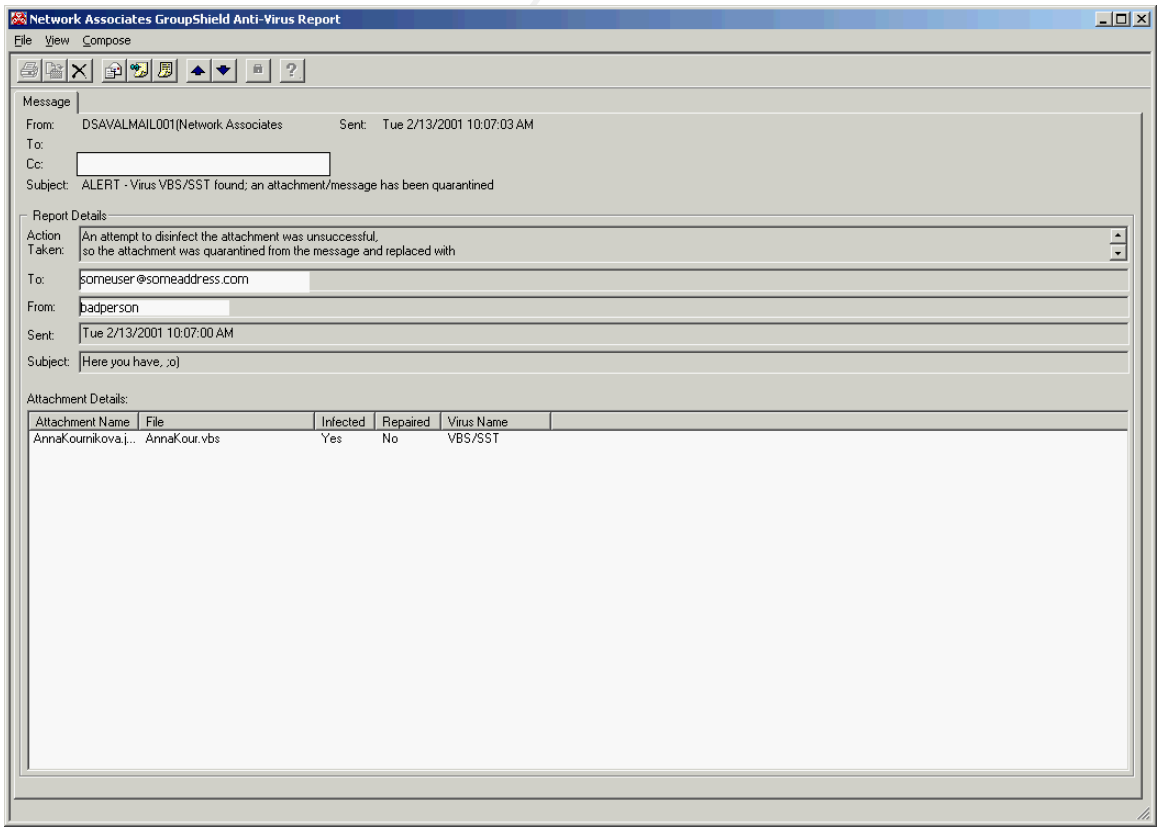

Figure 1

Specifics

AVERT ~~said~~ reported the worm was first discovered ~~they first discovered this worm~~ in August of 2000. Details from ZDNet reported ~~said that it had some of~~ the virus had the same characteristics as the ILOVEYOU worm~~,~~ and that it would use the Outlook address book to send copies of itself. One of its ~~most~~ distinctions is its capability to ~~destructive payloads is that it can~~ overload email servers with excess traffic~~,~~ although it is not ~~but is said not to be a~~ destructive ~~virus~~ otherwise. That is, it does not modify or delete files.

This worm ~~script~~ was created by VBS Worm Generator 1.50b. This is a toolkit that allows someone to fill in the spaces and create a virus. Basically, the creator was able to point and click and a virus was created. ~~Note: a worm is a self-contained program with the ability to spread itself.~~ To kill the worm, one just has to delete the program.

The email that comes to the user has the following characteristics:

Subject:
Here you have, ;o) OR
Here you are ;-) OR
Here you go ;-)

Body:
Hi:
Check This!

Attachment: AnnaKournikova.jpg.vbs

It also creates a registry key and key values. The script refers to these values to check if the mailing routine has already taken place:
HKEY_CURRENT_USERS\.DEFAULT\Software\OnTheFly
HKEY_CURRENT_USERS\.DEFAULT\Software\OnTheFly\mailed=(1 for yes)

On January 26th, the script attempts to connect to a Dutch shopping web site http://www.dynabyte.nl

Symptoms

- Presence of the file "c:\WINDOWS\AnnaKournikova.jpg.vbs"
- Presence of the registry key:
  HKEY_CURRENT_USERS\.DEFAULT\Software\OnTheFly

Method of Infection

This script arrives as an email attachment. Once infected, the script attempts to mail itself to everyone in the Outlook address book.

Removal
Update your anti-virus software with the most current virus definitions and do a full scan of the hard drive to include .vbs files. Delete all infected files. Optionally, you can remove the registry key:
HKEY_CURRENT_USER\DEFAULTS\Software\OnTheFly

Protection

1. Remove Windows Scripting Host. This is installed on Windows 98 and Windows 2000 machines and allows VBScript and JavaScript to execute. Removing this will stop the script from executing.

2. Run the scriptlet.typelib/Eyedog patch. Scriptlet.typelib allows local files to be created or modified. Eyedog allows "registry information to be queried and machine characteristics to be gathered."[7] This patch disables both of these features and should be done as a preventive measure.

3. Install the Outlook 98/2000 security patch. This patch prevents a program from accessing your address book or contacts, thus rendering the worm unable to self-propagate.

4. Keep anti-virus up-to-date. This should be as fundamental as daily hygiene ~~brushing your teeth everyday~~. Viruses are continually evolving and the protection ~~you~~ installed two days ago will not protect ~~you~~ r PC from the new virus that was created two hours ago.

5. Have anti-virus software scan for "all files". It is not enough to just accept the default installation, but users need to verify that their virus protection will check all files.

Aliases
Anna Koumikova
AnnaKoumikova
VBS.VBSWG.J (CA)
VBS/Anna
VBS/OnTheFly@mm (F-Secure)
VBS/SST (Virus Scan)
VBS/SST-A (Sophos)
VBS/SST.A (Panda)
VBS/SST.Worm (CAI)
VBS/SST@MM (Virus Scan)
VBS_Kalamar.a (Trend)

Lessons Learned

I was able to ~~find~~become aware -and contain this virus though keeping our virus scan software current. I was fortunate enough to have virus definitions for this virus installed and thus, ~~I was~~ able to detect and stop this virus before it spread throughout the company. During the onset of this virus, the anti-virus software blocked approximately 39 worms from entering our company. This is approximately 8% of our employees whom would have propagated the virus to the remaining employees. It also reinforces to users to keep their anti-virus software current and not to open up emails from unknown users (however, most that came through the users knew). Even though this virus was not destructive to the users in that it did not destroy or modify files, it ~~utilized the~~ placed a fair amount of load on our email ~~server~~ server, and the load, both email and network would have been much greater if the anti-virus software was not current.

Proactive Lessons Learned

As with any virus, we have to quickly assess and react to protect company data from getting destroyed or spread. In this case, it first seemed obvious that the emails going through the exchange server was being protected by groupshield. Further investigation proved that those people using unsanctioned email accounts, such as free internet email accounts, were only protected by our "pushing" anti-virus dat file updates to those PC's.

Being proactive to protect the company and serve users resulted in many changes. They are technological, procedural and policy changes.

Technological changes include

- using anti-virus software
- using server-based groupshield
- forcing updates to user's PC's.

Procedural changes include

- watching groupshield
- keeping abreast of the news
- having preplanned actions detailed so action may be taken immediately upon hearing of a virus in the wild
- posting signs on entrance way doors for employee awareness
- disconnection of network access to protect network data during dangerous virus outbreaks (before updates to groupshield are made) until every employee is checked
- manually updating those who do not have the anti-virus update "pushed" to them
- 19-point FAQ distributed to everyone and presented in the companies corporate orientation.

Policy changes include

- Company internet and computer usage policy.
- Employees must agree to internet and computer usage policy which makes them aware and responsible to update or ensure their anti-virus software is updated
- Using personal computer equipment on the companies internal network is forbidden

~~'s processor space and hard drive space.~~

References:

1. Vamosi, Robert. "How the Anna Virus was created." February 12, 2001. URL: http://www.zdnet.com/zdhelp/stories/main/0,5594,2684736,00.html

2. Vamosi, Robert. "Anna virus spreading fast." February 12, 2001. URL: http://www.zdnet.com/zdhelp/stories/main/0,5594,2684479-1,00.html

3. Lemos, Robert. ZDNet News "From Russia with love? Koumikova virus smashes net." February 12, 2001. URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2684605,00.html

4. NAI "VBS/VBSWG.j@MM." February 12, 2001. URL: http://vil.nai.com/vil/virusSummary.asp?virus_k=99011

5. Trend Micro "VBS_KALAMAR.A" URL: http://www.antivirus.com/vinfo/virusencyclo/default5.asp?VName=VBS_KALAMAR.A

6. Symantec. VBS.SST@mm. February 15, 2001. URL: http://service1.symantec.com/sarc/sarc.nsf/html/VBS.SST@mm.html

7. Microsoft. "Microsoft Security Program: Microsoft Security Bulletin (MS99-032)." October 12, 1999. URL: http://www.microsoft.com/technet/security/bulletin/ms99-032.asp