Global Information Assurance Certification Paper

SANS-GIAC Practical Assignment for Security Essential Certification

Title : *What is VBS.SST@mm worm?*
Author : *Eka Hartono*
Date : *February 2001*

Introduction

On February 12, 2001, the world is once again awakened by a new worm attack. The worm was called VBS.SST@mm, was also known as the VBS.Lee-o, VBS. OnTheFly, VBS. Vbswg.gen, Anna Kournikova, and VBS/VBSWG.J@mm.[i] The worm circulated rapidly hiding itself as an electronic picture of the famous Russian tennis star Anna Kournikova.[ii,iii,iv]

What is VBS.SST@mm?

VBS.SST@mm is a VBS email worm that was being coded using a virus creation tool.[v] The worm arrives as an email attachment called AnnaKournikova.jpg.vbs. Upon execution, the .VBS worm automatically email itself to the email address list in Microsoft Outlook. In addition, the worm comes with a message: "Hi: Check This!" and at least three subject lines were identified: "Here you are", "Here you have", and "Here you go" followed by a smiley face.[vi] There is no damaging payload of the worm, except for automatically directing the infected user's web browser an Internet address in Netherlands (http://www.dynabyte.nl). The Internet address is apparently a Dutch's shop website.[vii] According to Symantec AntiVirus Research Center, the worm is considered highly in the Wild and has high distribution capability.[viii] However, since the worm will just tied up the mail server with its' action of sending mass mailing, the worm is considered at a low damage level.

How does it work technically and how to get rid of it?[ix]

When the user clicks on the attachment, the worm will run and create the registry key:
HKEY_CURRENT_USER\Software\OnTheFly

Once January 26 of each year hits, the work will attempt to direct the user's web browser to http://www.dynabyte.nl.

In the mean time, the worm will check if mass mailing to all the email address in Microsoft Outlook has been sent. If such an action is not yet executed, it will send the mass mailing and set the registry key:
HKEY_CURRENT_USER\Software\OnTheFly\mailed ; to "1" (value one), to prevent the mailing routine to execute again.

Within a period of time after the first attack of this worm, major anti-virus vendors managed to provide solution to prevent and remove the worm. One of the major Internet security vendors, Symantec Corporation, recommends its' customers to download the latest virus definition to detect the worm and do the following action to remove the worm from their systems:

1. Run Live Update to make sure the system has the most recent virus definitions.
2. Start Norton AntiVirus (NAV), and run a full system scan, making sure that NAV is set to scan all files.
3. If any files are detected as infected by VBS.SST@mm, click Delete
4. (Optional) Delete the following registry key:

   HKEY_CURRENT_USER\Software\OnTheFly

In fact, users who are fairly educated on the fact that that .EXE and .VBS files are executable and worm/virus prone, would have already deleted the attachment. Thus, prevent them from being infected. However, as mentioned by Vincent Weafer and Stephen Trilling of Symantec, "Close to Valentine's Day, anything novel or different like this will get people's attention more than normal"[x] and since the .VBS extension may be hidden and people are attracted to the .JPG attachment of the tennis star, it increases the likelihood of a user "clicking" on the attachment.[xi] Unlike .EXE and .VBS, .JPG is not typically viral.

In addition, since the removal of the worm is considered easy, IT personals can now better filter these types of scripts worms and users now know not to click on AnnaKournikova.jpg.vbs, the worm should start dying out quickly.

Who wrote the VBS.SST@mm worm and why?[xii, xiii]

According publications referred in this paper, the worm was written by a young Dutch man who claimed to have no intention on creating such havoc and was apparently surprised with the damage it potentially created. Even more interesting, the writer claimed to have no programming skill and used a "virus toolkit" known as a Visual Basic Worm Generator to create the worm.

In addition, he claimed to be a big fan of Anna Kournikova, thus the Anna Kournikova photo masquerade, and simply needed an internet site to be attached to the program, thus www.dynabyte.com was chosen.

Conclusion

Asserting my own opinion to this recent outbreak, you do not have anti-virus software in your system or have not recently up-date your anti-virus software,

please do so immediately. This latest news definitely creates an alarming awareness of the potential of major virus/worm outbreaks, simply because of the wide spread availability of virus/worm generator toll kits.

Glossary

Worm - Is an independent program that replicates itself, crawling from machine to machine across network connections. It often clogs networks as it spreads -- often via e-mail.[xiv]

Virus - A program that can "infect" or "contaminate" other programs by modifying them to include a copy of itself. Viral code is typically malicious and detrimental to data or system integrity. [xv]

Wild – The extent to which a virus is already spreading among computer users. This includes number of independent sites infected, the number of computers infected, the geographic distribution of infection, the ability of current technology to combat the threat, and the complexity of the virus.[xvi]

Payload – This is the malicious activity that the virus performs. Not all viruses have payload, but there are some that perform destructive actions.[xvii]

Related Readings

McCargo, Bernard. How Viruses Attached. 8 December 2000. URL: http://www.sans.org/infosecFAQ/malicious/attach.htm (19 February 2001)

Whalen, Tracey. "I Love You" Worm. 9 September 2000. URL: http://www.sans.org/infosecFAQ/malicious/iloveyou_worm2.htm (19 February 2001)

Dooley, Patricia. What is the VBS.Stages.A Worm? 28 November 2000. URL: http://www.sans.org/infosecFAQ/malicious/VBS_stages.htm (19 February 2001)

Williams, Gary. VBS_NEWLOVE.A Worm. 1 December 2000. URL: http://www.sans.org/infosecFAQ/malicious/VBS_NEWLOVE.htm (19 February 2001)

References

[i] Chien, Eric and Hindocha, Neal. SARC Write-up – VBS.SST@mm. 15 February 2001. URL: http://service1.symantec.com/sarc/sarc.nsf/html/pf/VBS.SST@mm.html (19 February 2001).

[ii] E-mail Virus Circulating Rapidly. Associated Press. 12 February 2001. URL: http://espn.go.com/tennis/news/2001/0212/1079565.html (16 February 2001)

[iii] Lemos, Robert. From Russia with Love? Koumikova Virus Smashes Net. ZDNet News. 12 February 2001. URL:http://dailynews .yahoo.com/h/zd/20010212/tc/from_Russia_with_love_koumikova_virus_smash (16 February 2001)

[iv] Sieberg, Daniel. New Email Virus Preys on Anna Koumikova fans. 12 February 2001. http://www.cnn.com/2001/TECH/internet/01/12/anna.worm/index.html (16 February 2001)

[v] Chien, Eric and Hindocha, Neal. SARC Write-up – VBS.SST@mm. 15 February 2001. URL: http://service1.symantec.com/sarc/sarc.nsf/html/pf/VBS.SST@mm.html (19 February 2001).

[vi] E-mail Virus Circulating Rapidly. Associated Press. 12 February 2001. URL: http://espn.go.com/tennis/news/2001/0212/1079565.html (16 February 2001)

[vii] Delio, Michelle. Anna Worm Write Tells All. 13 February 2001. URL:http://www.wired.com/news/technology/0,1282,41782,00.html (17 February 2001)

[viii] Chien, Eric and Hindocha, Neal. SARC Write-up – VBS.SST@mm. 15 February 2001. URL: http://service1.symantec.com/sarc/sarc.nsf/html/pf/VBS.SST@mm.html (19 February 2001).

[ix] Chien, Eric and Hindocha, Neal. SARC Write-up – VBS.SST@mm. 15 February 2001. URL: http://service1.symantec.com/sarc/sarc.nsf/html/pf/VBS.SST@mm.html (19 February 2001).

[x] E-mail Virus Circulating Rapidly. Associated Press. 12 February 2001. URL: http://espn.go.com/tennis/news/2001/0212/1079565.html (16 February 2001)

[xi] Head of Research at Symantec's Anti-Virus Research Center discussed about Anna Koumikova Virus. 12 February 2001. URL: http://www.usnewscast.com/messageboard/NASDAQstocks/symc/index.html)19 February 2001)

[xii] Delio, Michelle. Anna Worm Write Tells All. 13 February 2001. URL:http://www.wired.com/news/technology/0,1282,41782,00.html (17 February 2001)

[xiii] Koumikova Virus Suspect Arrested. !4 February 2001. URL: http://www.cnn.com/2001/TECH/internet/02/14/knournikova.virus/index.html (17 February 2001)

[xiv] Symantec Anti-Virus Research Center. URL: http://www.sarc.com (19 February 2001)

[xv] Symantec Anti-Virus Research Center. URL: http://www.sarc.com (19 February 2001)

[xvi] Symantec Reference Area – Glossary of Terms. URL: http://www.symantec.com/avcenter/erfa.html (19 February 2001).

[xvii] Symantec Reference Area – Glossary of Terms. URL: http://www.symantec.com/avcenter/erfa.html (19 February 2001).