Global Information Assurance Certification Paper

LevelOne Security Essentials GSEC Practical Assignment
Version 1.2, current as of December, 2000

Submitted by: James Galvin

The Anna Kournikova Virus: Tennis Anyone? Everyone?
James Galvin
February 17, 2001

I'm working at my home computer, taking quizzes on the SANS GIAC Website in preparation for a certification exam. My wife is working on her office laptop preparing for a meeting when she suddenly exclaims, "I think I just received a virus!!"

I look over at her laptop screen and she has several e-mails with the same subject line "Here you have, ;o)" and a message body of "Hi: Check This!" with a an e-mail attachment titled "AnnaKournikova.jpg.vbs." The e-mail's attachment certainly had an unusual file extension, and there were several e-mails from unrelated people (many of which my wife did not know).

My first reaction is: don't open the e-mail!! My second reaction is: isn't this interesting, I have a research paper to write for my GIAC practical and I haven't selected a subject.

Unfortunately, we did not have updated anti-virus software to scan the attachment for malware, so my wife quickly deleted the suspect e-mails from her laptop. She did not want to take the chance of losing any of the information that she had been preparing for her business meeting in the morning. She also notified the senders of the suspect e-mail that their systems might be infected with a virus.

Later that evening, the TV News broadcasts are warning of the latest virus that is infecting computer systems. There is no information about what the virus does, other than to say that the virus is activated when a user opens the "Anna Kournikova" file attachment. The attachment appears to be a harmless picture of Anna Kournikova (a jpg graphics file), but upon closer examination of the file extension (.jpg.vbs), it is actually a Visual Basic script. When executed, it sends itself to everyone in the user's Microsoft Outlook address book.

In the morning, at work, there are discussions of the Anna Kournikova virus and several e-mail notifications are distributed to warn people not to open the e-mail attachment. Some people are saying the virus appears to be non-destructive, and others are stating that the facts are not in yet.

I began to research the virus for my LevelOne Security Essentials GSEC Practical

Assignment. The Internet is a wonderful source of information, even with all of its vulnerabilities. From the information I've been studying in the SANS GIAC course, I knew to watch for the effects of the virus on Confidentiality, Integrity, and Availability.

At this point, no one in our company knew exactly how the virus worked. If the virus extracted information from infected computers and sent the information across the Internet then our Confidentiality of information would be affected. If the virus altered information on infected systems then the Integrity of our information would be affected. What we did know was that the flurry of activity to protect our computer systems against the virus was affecting the Availability of our resources (both computer and human).

Generally, productivity was slowed as people carefully screened their e-mails for the Anna Kournikova virus, or one of several variants that were showing up (there were subtle changes in the words used in the subject of the virus e-mail– "Here You Go", or "Here You Are"). The virus also had several aliases: AnnaKournikova, Anna Kournikova, Calamar, I-Worm, I-Worm.Lee, Kalamar.A, Lee-0, Onthefly, Pica, Tennis, VBS/Anna, VBS_Kalamar.A, VBS/SST.A, VBS/SST-A, VBS/VBSWG.J.

People that would have been working on other projects were now sidetracked, protecting our systems against the spread of the Anna Kournikova virus.

As I surfed the Internet in search of information, I was struck by the opportunities made available by the virus. News Groups and Bulletin Boards were full of postings from people that wanted to point fingers and lay blame. Software manufacturers, especially anti-virus distributors, were advertising their latest versions to help save your computer systems from disaster.

Occasionally, mixed between the personal opinions and the business opportunities, were several helpful recommendations for preventing the infection of a virus, detecting a virus if you are infected, and fixing problems caused by a virus. Examples included blocking certain attachments (such as .scr, .vbs, .shs, .bat, .com, .exe, .pif), using updated anti-virus scanners to scan e-mails for virus-infected attachments at all times (any e-mail attachment can be a hiding place for malware), and applying current patches to E-mail servers to help protect them against attack.

Within a week, the alleged author of the Anna Kournikova worm admitted to writing and distributing the e-mail that infected thousands of computers. The virus had the potential to overload and crash e-mail servers, thereby causing an Availability attack. The virus also modified the Windows Registry with it's own record, thereby causing an Integrity attack. Lastly, the virus was not a virus but a worm that was created from a Visual Basic Worm Generating toolkit.

There are many suggestions for preventing the spread of malware. Defense-in-depth, using network and host based intrusion detection mechanisms will protect information systems against many attacks. The Anna Kournikova worm, however, used encryption to slip undetected through many intrusion detectors to get onto Outlook mail servers. With so much malware exploiting executable attachments, which are not required for e-mail applications to function properly, there is reasonable justification to filter them out of e-mail altogether.

Ultimately, the computer user has the final decision on whether to click on a suspect e-mail attachment that has evaded detection. The user is the last line of defense in the defense-in-depth concept. Computer users should be trained in intrusion detection techniques, with policies and procedures to react appropriately when required.

The following detailed information about the Anna Kournikova worm was taken from a posting by Ken Dunham on the SecurityPortal Web Site: http://www.securityportal.com.

Description

SST was reportedly created by "OnTheFly" using VBS Worms Generator 1.5b authored by [K]alamar. The identity of OnTheFly has been concealed by authorities but has been speculated by InternetNews as Jan Dewit, a 20-year-old Dutch man from the town of Sneek. SST currently sends out malware email with the following data:

> Subject: Here you have, ;0)
> Body: Hi: Check This!
> Attachment: AnnaKournikova.jpg.vbs, AnnaKour.vbs

Because this malware uses a double extension, .JPB.VBS, users may not realize that the attachment is a VBS file. This Trojan aspect of SST is designed to deceive users into believing they have received a JPEG image of the famous Russian tennis player Anna Kournikova.
SST has been reported by multiple resources as spreading quickly in the wild, putting mail servers at risk for CPU/memory/bandwidth overload and possibly resulting in email server crashes.

Symptoms

Presence of an email with possible subject, body, and attachment as noted in the description above. Presence of a file on the local hard drive, C:\WINDOWS\AnnaKournikova.jpg.vbs.
Because the subject, body, and attachment names for this malware may change as the malware spreads in the wild, SecurityPortal recommends the following preventative measures:

1) Do not open VBS email attachments.

2) Save any other types of attachments to a local drive to scan with an updated antivirus scanner before executing them. Make sure your antivirus

product has been updated for this specific malware.

3) Save any questionable email attachments in a protected area for a few days until the outbreak of SST has been contained. Updates will be available for most vendors, which can then be used to scan questionable attachments at that time.

4) Configure servers to filter out the known "AnnaKournikova.jpb.vbs" attachment along with other VBS files and known malware attachments.

5) Download and install Outlook Security patches to protect against such malware. Patches are available for Microsoft Outlook! 98 E-mail Security Update and Microsoft Outlook! 2000 E-mail Security Update.

6) Remove Windows Scripting Host from your system. If you're not a programmer or using complex software, you can probably live without Windows Scripting Host. Use the Add/Remove Software control panel to remove it from your system.

7) Practice safe computing, such as not opening attachments. Read the recent SecurityPortal article, "Don't Be Bit by the Lovebug," for more details on safe computing.

Infection

Once the attachment "AnnaKournikova.jpg.vbs" has been executed, SST creates the following registry key:

HKEY_CURRENT_USER\software\OnTheFly

SST then uses this registry key to check the status of mass-mailing. If no mass-mailing has occurred, SST attempts to email itself to all users within the Microsoft Address Book on the infected machine. SST then modifies the registry key to:

HKEY_CURRENT_USER\software\OnTheFly\mailed

If it is the 26th of January, this malware attempts to connect to a Netherlands Website, http://www.dynabyte.nl/.
After execution, SST continues to run in memory. If it is deleted it attempts to recreate itself, but fails due to a bug in the code, resulting in a zero-byte file.

Payload

Modifies the HKEY_CURRENT_USER\software\OnTheFly registry and attempts to connect to http://www.dynabyte.nl/ on the 26th of January. Because it spreads so quickly, just as LoveLetter did in 2000, SST may also crash email servers due to CPU/memory/bandwidth overload.

Disinfection

Use updated antivirus software, making sure the most recent update detects and removes

this malware, and/or available fixes. One fix that is immediately available is from Central Command. Updates for various programs for SST will likely available at the following Internet sites within the next 48 hours:

AVG
AVP
AVX
Command Antivirus/F-Prot
Dr. Solomon Antivirus
InocuLAN
InoculateIT
McAfee
Norman
Norton Antivirus (or use LiveUpdate feature)
Panda
PC-Cillin
Sophos
Trend Micro
VET Antivirus

For manual removal delete the HKEY_CURRENT_USER\software\OnTheFly registry key, and all email, attachments and files (such as C:\WINDOWS\AnnaKournikova.jpg.vbs) associated with this malware.

References (for SANS GIAC Practical):

Delio, Michelle. "Anna Worm Writer Tells All". Posted on the SANS Institute Information Security Reading Room.13 Feb 2001. URL: http://www.wired.com/news/technology/0,1282,41782,00.html

Dunham, Ken. VBS.SST@mm . Posted on the Security Portal Web Site. 12 Feb 2001. URL: http://www.securityportal.com/research/virus/profiles/vbssst.html

Delio, Michelle. “The Internet: It’s Full of Holes”. Posted on the Wired.com Web Site. 6 Feb 2001. URL:
http://www.wired.com/news/technology/0,1282,41625,00.html

London, England (CNN). “Kournikova virus suspect arrested”. Posted on the CNN.com Web Site.14 Feb 2001. URL:
http://www.cnn.com/2001/TECH/internet/02/14/kournikova.virus/index.html

Palo Alto, California (CNN). “Kournikova virus slams U.S., Europe, misses Asia. Posted on the CNN.com Web Site. 13 Feb 2001. URL:
http://europe.cnn.com/2001/TECH/internet/02/13/anna.worm/index.html

(CNN). “New e-mail virus preys on Anna Kournikova fans”. Posted on the CNN.com Web Site. 13 Feb 2001. URL:
http://asia.cnn.com/2001/TECH/internet/02/12/anna.worm/

Dunham, Ken. “Don’t be Bit by the LoveBug”. Posted on the SecurityPortal Web Site. 09 Feb 2001. URL:
http://www.securityportal.com/articles/dontbebit20010209.html