Global Information Assurance Certification Paper

Nancy Roberts-GCIH (roberts005)
Mary Washington College/JMC
25 February, 2001

Exploit Details.

Name: W32.Hybris Worm
Aliases: Win32.Hybris, IWorm_Hybris, I-Worm.Hybris, W32/Hybris.gen@M, Troj_Hybris, W32.Hybris.gen, W32.Hybris.22528.dr, Troj_Hybris.A, Troj_Hybris.B, Troj_Hybris.C, Troj_Hybris.D, Troj_Hybris.E, Troj_Hybris.DLL, Troj_Hybris.PX, W32/Hybris.dll@MM, W32/Hybris.dr, W32/Hybris.exe, W32/Hybris.gen.dll@M, W32/Hybris.gen@M, W32/Hybris.gen@MM , W32/Hybris.ini, W32/Hybris.plugin@M, W32/Hybris.plugin@MM , W32/Hybris@M, W32/Hybris@MM , W95/Hybris@M
Variants: W32/Hybris-Drop
Operating System: Win 32 systems (Win95, Win98, Win NT, 2000, ME)
Protocol or Services: WSOCK32.DLL and WININIT.INI

Brief Description: The W32.Hybris worm infects the WSOCK32.DLL to allow it to intercept “Connect”, “Recv” and “Send” commands by appending itself to the end of file. The worm propagates by sending non-host initiated email to addresses intercepted from WSOCK32.DLL, can have any of 32 plug-ins for extended functionality and is self-updating through newgroup communications.

Protocol Description:

WSOCK32.DLL:

“Windows Sockets is an interface between applications and the transport protocol and works as a bi-directional pipe for incoming and outgoing application data.” (1) Each TCP/IP vendor supplies a Interprocess Communications (IPC) protocol to support distributed processing. This provides the capability to “share” tasks across the network providing accessibility for clients with minimal computing power while the majority of the work is being accomplished on a more powerful server.

Windows Sockets is the most common implementation of IPC in use today based on its wide availability and high levels of support. It is provided with Microsoft operating systems.

The Windows Sockets implementation that is exploited by this worm is WSOCK32.DLL (Windows Socket 32 Bit Dynamic Link Library). All applications link to WSOCK32.DLL implicitly to provide the necessary network connectivity, dial-up or LAN, providing the worm access to all the processes active on the infected host. WinSock is written in a C-like manner, however since the API is compiled into a DLL, programs written in any language can use it.

The below Registry Services subkey will contain the registry entries related to TCP/IP. The current control set is the process used to boot the system for the current session. Since the Registry Key defines Microsoft TCP (MSTCP) protocol as being used it would follow that WSOCK32.DLL would be the Windows Sockets used.

Nancy Roberts-GCIH (roberts005)
Mary Washington College/JMC
25 February, 2001

Hkey_Local_Machine\System\CurrentControlSet\Services\VxD\MSTCP\ Service Provider

The name and location of the Windows Socket DLL file is specified in ProviderPath subkey value. The default location of the WSOCK32.DLL is in the Windows/System folder. Easy for programs (malicious or not) to find.

WININIT.INI:

WININIT.EXE and WININIT.INI are not Microsoft Windows applications, but are provided with Windows to provide a critical function supporting Windows operating systems. When installing applications or modifying properties in Windows the install process needs to modify several system files. However, Windows system files that are in use or memory resident are locked and can not be modified.

WININIT.EXE provides auto-installation processes to support Windows. During an installation process, the install routine will make copies of systems files with the modification necessary to support the new application being installed. These modifications will not take effect until the system is booted and must be implemented prior to the Windows Protected Mode being loaded. (System files will be locked after the Windows Protected Mode is loaded).

WININIT.INI is used to facilitate the installation process and can rename, copy and delete files prior to the Windows protected mode load.

WININIT.EXE looks for and if found, runs the WININIT.INI as part of the boot process. The WININIT.EXE does not require any operator/user intervention to run and activate the WININIT.INI. WININIT.INI will rename the system files to be replaced, change extensions to provide a recovery process, delete old copies, or copy files as required.

Most of us have been guilty of trying to rush the install process at some time or other and waiting to perform the Restart after an installation until we do a few more things on the workstation. When the Restart is postponed the new version system files or installation of the application is not activated. You may experience problems with the install until the boot process has been accomplished.

Since the WININIT.EXE runs prior to the Windows Protected Mode being loaded it can not recognize long file names. Therefore modifications initiated by the WININIT.EXE and WININIT.INI must conform to the short name (8.3) file naming structure.

How the exploit works:

In this exploit the WININIT.EXE and WININIT.INI applications are used against the host system to modify or infect WSOCK32.DLL without user interaction.

Nancy Roberts-GCIH (roberts005)
Mary Washington College/JMC
25 February, 2001

The worm takes advantage of the prevalence of TCP/IP and Windows Sockets for distributed processing across the network as well as the auto-installation capabilities of WININIT.EXE.

Win32.Hybris is an internet worm that infects the WSOCK32.DLL. When activated the worm performs the processes of a normal application installation using the functionality provided by Windows. It tries to write to the WSOCK32.DLL. If the file is busy or resident in memory the worm creates an infected copy of the WSOCK32.DLL by appending itself to the end of the file. This increases the WSOCK32.DLL file size between 21kb and 28kb depending on the plugins incorporated in that version of the worm.

The infected file is named using the short naming convention (8.3) required by WININIT.EXE. The file name is randomly generated by selecting letters between "a" and "p" (abcdefgh.ijk). The worm then creates or modifies the WININIT.INI ASCII file to request renaming of the existing WSOCK32.DLL and making the infected copy (abcdefgh.ijk) the new WSOCK32.DLL at the next system boot.

As a fail-safe the worm also copies the infected file (abcdefgh.ijk) to the Windows\System folder and edits the Registry to add a "Run Once" call to activate the worm program. The plugins are also written to the Windows/System folder using the same random short naming convention.

Upon successful boot, the worm is now ready to intercept "Connect", "Recv" and "Send" calls looking for email addresses to facilitate its propagation through email. When the user sends a clean email the worm intercepts the email address and without the host user being aware, sends a second email to the same addressee.

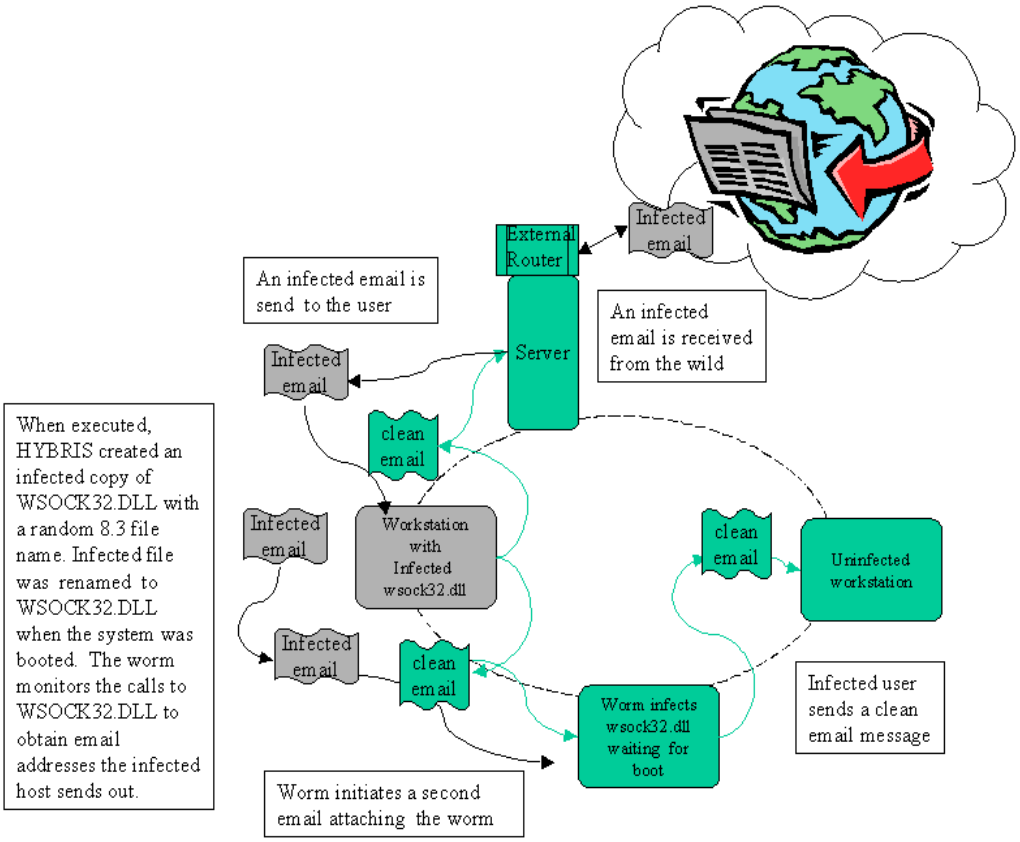
Win95 and Win98 are very susceptible to this type of exploit because the processes used are authorized within the operating system and considered normal functions. Additionally, Win95 and Win98 were not designed with security as a major focus, so the operating system is unprotected. System Administrator privileges are not required to modify system files or to perform applications installations.

The process is more complicated in WinNT because administrative access is required to modify system files. If the user does not have administrative privilege then the malicious code has to escalate the user's privilege or it has to add a process/service to the computer with system administrative rights. This could be done by granting specific "Rights" to the system user and then using the CreateProcessAsUser function.

Administrative rights can be gained through such methods as: IP Spoofing, Sniffing Usernames and Passwords from the host workstation or LAN, or Session Hijacking, to name but a few. The malicious code could then use the CreateProcessAsUser to grant full access to the windowstation or desktop where the process executing the worm will run. Additional complexity is added by the various operating system configurations, and service pack or patches that can be loaded on the system.

Nancy Roberts-GCIH (roberts005)
Mary Washington College/JMC
25 February, 2001

Diagram of W32.Hybris exploit process:



How the W32.Hybris worm exploits WSOCK32.DLL and WININIT.INI:

Win32.Hybris was discovered in September 2000 and is believed to have been created in South America. Distribution is considered high, and risk is considered medium. It has similar functionality to Happy99 worm of January 1999. The worm author used great care in developing survivability and adaptability into the worm. The author played on humanities dark side and sexual nature.

The plugins provided infinite modifications to the Subject line, message text, and attachment names which are randomly selected from the plugins in the body of the worm code.

The infected email has a From line of:

Hahaha <hahaha@sexyfun.net>

Nancy Roberts-GCIH (roberts005)
Mary Washington College/JMC
25 February, 2001

(Siting have claimed that some variants do not have a From: indicated, but this has not been verified by the major Anti-Virus Vendors.)

Earlier versions of the worm had the subject line of:

"Snowhite and the Seven Dwarfs – The REAL story!"

The text would be set to (misspellings as annotated):

"Today, Snowhite was turning 18. The 7 Dwarfs always where very educated and polite with Snowhite. When they go out work at mornign, the promissed a "huge" surprise. Snowhite was anxious. Suddlently, the door open, and the Seven Dwarfs enter…"

The plugins also provided for text in Spanish, French and Portuguese.

French:
From: Hahaha [hahaha@sexyfun.net]
*Subject: Les 7 coquir nains *or* Blanche neige et ...les sexe nains*
*Body: C'etait un jour avant son dix huitieme anniversaire. Les 7 nains, qui avaient aidé 'blanche neige' toutes ces années après qu'elle se soit enfuit de chez sa belle mère, lui avaient promis une *grosse* surprise. A 5 heures comme toujours, ils sont rentrés du travail. Mais cette fois ils avaient un air coquin...*
Attachment: blancheneige.exe or sexynain.scr or blanche.scr or nains.exe

Spanish:
From: Hahaha [hahaha@sexyfun.net]
Subject: Enanito si, pero con que pedazo!
*Body: Faltaba apenas un dia para su aniversario de de 18 años. Blanca de Nieve fuera siempre muy bien cuidada por los enanitos. Ellos le prometieron una *grande* sorpresa para su fiesta de compleaños. Al entardecer, llegaron. Tenian un brillo incomun en los ojos...*
Attachment: enano.exe or enano porno.exe or blanca de nieve.scr or enanito fisgon.exe

Portuguese:
From: Hahaha [hahaha@sexyfun.net]
Subject: Branca de Neve pornô!
Body: Faltava apenas um dia para o seu aniversario de 18 anos. Branca de Neve estava muito feliz e ansiosa,

Nancy Roberts-GCIH (roberts005)
Mary Washington College/JMC
25 February, 2001

*porque os 7 anões prometeram uma *grande* surpresa.*
As cinco horas, os anõezinhos voltaram do trabalho.
Mas algo nao estava bem... Os sete anõezinhos tinham
um estranho brilho no olhar...
Attachment: branca de neve.scr or atchim.exe or
dunga.scr or anão pornô.scr

The attachment filename is randomly chosen from the following list*: "sexy virgin.scr", "joke.exe", "midgets.scr", dwarf4you.exe*" (2)

Additional plugins provided new subject lines and attachment file names adding:

"sexy", "horny" and "pleasure" (2). Possible attachment names:
*Anna.exe, Raquel Darian.exe, Xena.exe, Xuxa.exe, Suzete.exe, famous.exe, celebrity rape.exe, leather.exe, sex.exe, sexy.exe, hot.exe, hottest.exe, cum.exe, cumshot.exe, horny.exe, anal.exe, gay.exe, oral.exe, pleasure.exe, asian.exe, lesbians.exe, teens.exe, virgins.exe, boys.exe, girls.exe, SM.exe, sado.exe, cheerleader.exe, orgy.exe, black.exe, blonde.exe, sodomized.exe, hardcore.exe, slut.exe, doggy.exe, suck.exe, messy.exe, kinky.exe, anpo porn(.scr, atchim.exe, branca de neve.scr, dunga.scr, enano porno.exe, sexy virgin.scr, joke.exe, midgets.scr, dwarf4you.exe, fist-f*cking.exe, or amateurs.exe*.(3)

The list is almost endless in the worm authors attempt to grab the curiosity of the recipient of the infected email.

The worm's functionality is expanded by any one of 32 plugins that can be installed in the worm. The plugins greatly expanded the actions that the worm could take and were encrypted with 128 bit encryption to enhance the worms survivability. The NEWS plugin provided for a "call home" capability and is set to "call" on the full moon, computed off the host internal clock. The worm would use the "Connect" function and log on to contact alt.comp.virus newsgroup to provide communication to the author and to self-update with new plugins. The HTTP plugin allow for updates from a web site. To hide its location, it uses fake email addresses to send plugins to root@microsoft.com through the anon.lcs.mit.edu gateway.

"The format of the newsgroup-posted message is as follows:
anon.lcs.mit.edu!nym.alias.net!mail2news
Message-ID: 20001113080521.28781.qmail@nym.alias.net
From: [USE-AUTHOR-ADDRESS-HEADER@[127.1]]
Author-Address: anonymous [AT]anon [DOT]lcs [DOT]mit [DOT] edu
Subject: http [code containing upper- and lower-case letters]
Mail-To-News-Contact: postmaster@nym.alias.net
Organization: mail2news@nym.alias.net
Newsgroups: alt.comp.virus
Lines: 46

KUWJGJWCVICGIWIWCZIWHCFXCHB [continues]....

Nancy Roberts-GCIH (roberts005)
Mary Washington College/JMC
25 February, 2001

[more coded lines]
[terminated by four asterisks]
**** "(4)

A preservation technique is provided by the AVIP or AVINET.DAT plugin. It blocked connectivity to the most popular anti-virus sites to prevent inoculation of the host system.

The SPIRALE or @@@@ plugin created an animated black and white spiral or a black sphere and displayed it on the screen as a service to prevent the user from being able to close the process. This plugin activates if the date is the 16th, or 24th of September or on the 59th minute of any hour in the year 2001, providing ample opportunity to disrupt your day of computing.

(2)

Various plugins infected Windows PE files appending to the end of the file and then recalculating the CRC values to hide its existence.

The worm targets executable files, appending itself to the end of files. The I_RZ plugin uses the companion method to infect ZIP and RAR files on drives C: through Z:. It changes the name of the .exe to .ex$ and copies it self in to the archive with a .exe extension. Sub7 plugin locates SubSeven Trojans and uses SubSeven commands to copy the worm unsuspecting systems. The ENCR or POLY plugin uses a polymorphic program to encrypt the worm.

Nancy Roberts-GCIH (roberts005)
Mary Washington College/JMC
25 February, 2001

As an added safety feature the author coded a PGP public key into the body of the worm to ensure that it would only accept authorized updated plugins containing the correct private key.

W32/Hybris-Drop provides a dropper for the W32.Hybris worm. The files carrying the dropper are created by worm using the exploit of the WSOCK32.DLL and the WININIT.INI.

Signature of the W32.HYBRIS Worm:

Each version of the infected email has a From line of: hahaha@ sexyfun.net even though they are being sent from the users domain. Symptoms of infection would arise as email correspondents began stating that they received email from you that you had not sent. If an Intrusion Detection System is in place it will alert to a possible worm email, or if monitoring had been turned on the router/Firewall/ISP connection would be registering the increased activity and the email sender.

There is also commonality in that each of the plugins for the W32.HYBRIS worm is the text related to “Snowhite” and the “7 Dwarfs” these character strings could be used to identify the worm in each of the 4 lauguages used. The worm also contains the text:

HYBRIS
c) Vecna

which can be used in a file scan or filtering routine.

Since the size of the W32SOCK.DLL increases in size between 21-28kb, checks on file size and dates updated would provide evidence that something was awry.

Given these symptom, a browse through the Windows/System folder would show files with randomly selected letters between “a” – “p”.

How to Protect Against the W32.HYBRIS Worm:

Most popular anti-viral software companies such as Kaspersky Labs, SecurityPortal, NAI, Norman, Sophos, Symantec, now have signatures for the W32.HYBRIS family of malicious code. The terminology is somewhat different from vendor to vendor. Some classify the W32.HYBRIS as a virus, others as a worm, some yet as a Trojan. The anti-virus protection has been effective in protecting systems.

In the SMTP connector (Internet Mail Connector) you can block either hahaha@sexyfun.net or the entire sexyfun.net domain (unless of course you do regular business with the sexyfun.net domain).

Additionally, with Internet Gateway or a Firewall installed, rejecting emails from a specific addressee and file restrictions on file types .exe and .scr can

either block and hold for inspection or automatically delete these files. Blocking executable file types is effective as preventative controls for this worm as well as virus, worms, or Trojans not yet defined in anti-viral software. Additional file extensions can be blocked to increase your level of protection (.vbs, .hlp, etc).

One of the problems with trying to block this specific worm by email address and attachment name is that some variants may not display any From address and with the myriad of plugins the attachments are always changing. Blocking is not a perfect cure but when used in conjunction with other safety measures greatly enhances uninterrupted mail services.

In the end secure computing and email practice and security education can provide a good foundation to prevent malicious code infections. Outlook can be set to restrict access to questionable sites and programming applets:

In Outlook select “Tools” menu.
Select “Security” tab.
Under “Secure Content” set the Zone to “Restricted Sites”
Under “Zone Settings” select “Custom Level”
Under “ActiveX Controls and Plugins” set to disable.
Under “Scripting” set to disable.

Although W32.Hybris does not use Virtual Basic Scripting (.vbs) to spread several noteworthy malicious codes have popularized this approach to propagation. WSH is required for and is installed on the host if Internet Explorer 5 is installed, or if it was download from microsoft.com. This can be prevented by:

Logging on as an administrator.
On the “Desktop”, or in “Windows Explorer”, right-click on “My Computer”.
Select “Open” from the menu.
Select “View” menu.
Select “Options”.
Select “File Types” tabbed page.
Find “VBScript Script File” and select.
Select “Remove” button.
Confirm selection.

Removal Procedures:

The first recommendation from Anti-viral vendors is to perform a complete system scan of the infected system deleting all the infected files except the WSOCK32.DLL.

To make the clean up process easier several vendors have developed clean or fix-it tools to work in conjunction with their anti-viral software. One tool that is available is the Norton W95.HybrisF tool will repair any executable files that were infected the worm.

Nancy Roberts-GCIH (roberts005)
Mary Washington College/JMC
25 February, 2001

W32.HYBRIS prepared for this action, and one of the plugins acted to block access to the major anti-viral software sites. These systems would have to be cleaned manually prior to allowing an update of virus definitions/signatures. Manual cleaning can place your files as risk. If at all possible obtain a copy of the anti-viral software with the W32.HYBRIS signatures/definitions from an alternate source.

For any of the affected operating systems, cleaning the system will require a copy/backup or original installation disk with the WSOCK32.DLL program.

Booting in the MSDOS mode is required to clean the .exe system files that were infected by the virus. The DOS command line scanner, SCANPM, is effective on files like EXPLORER.EXE and TASKMON.EXE. SCANPM is available on Plus! 98 CD-ROM and located in the Plus98.cab file.

If the WSOCK32.DLL file could not be repaired in the "Normal" mode, next you can attempt to repair it in the "Safe" mode. If these attempts do not work to repair the file it will have to be replaced with the original file from the installation CD or from a backup.

Establishing SAFE MODE:

Win95:

Select "Shutdown" then select "restart", "okay".
When Win95 starts to load, press F8, then select the option for Safe Mode from the popup menu.

Win98/ME:

From the "Run" command, enter "msconfig", then "okay".
From the "System Configuration Utility" popup, select the "Advanced" tab, select "Enable Startup Menu", "okay" twice.
Close all programs.
Restart the system from the "Shutdown" menu.
When the system restarts, select "Safe Mode" from the menu.

Win NT 4.0 and earlier versions do not have a Safe Mode option. When you select F8 while booting and chose Safe Mode from the menu, you restart in the "Normal" mode. This problem is documented by Microsoft and is reported to be a problem in W2000 as well.

Replacing the infected WSOCK32.DLL file:

Win98/ME:

extract a/ d:\win98\prcopy1.cab wsock32.dll /L d:\windows\system

Nancy Roberts-GCIH (roberts005)
Mary Washington College/JMC
25 February, 2001

Win95:

extract /a x:\win95\win95_02.cab wsock32.dll /L c:\windows\system

WinNT/2000:

Rename the WSOCK32.DLL file to WSOCK32.OLD
Using "Run", go to a DOS command prompt.
Change directories up one level (cd\).
Enter the command string:

Expand d:\i386\wscok32.dl_ c:\windows\system32\wsock32.dll

Where d: is the drive letter mapped to the CDROM drive where you will be extracting the file, and c:\windows\system is the path to where Windows system files are store on the infected system. (Change the paths as required to match the actual paths on the infected system).

After the process is complete "Exit" will terminate the DOS command and return the system to Windows.

Removing the Spiral or Black Sphere screen:

Additional repair must be performed if the Spiral screen was displayed on the infected host. After performing a complete system scan, reboot the system in the Safe Mode. In Explorer, ensure that the system "shows all files". Under "View", "Folder Options", "View Tab" select Show all Files. Open WIN.INI in sysedit and remove the reference line to the Plugin. It will be listed under run=c:\windows\system\abcdefgh.ijk (The worm creates the plugin file names by randomly selecting letters from a-p.) After modifying the WIN.INI, delete the plugin file.

When these steps have completed successfully, the host can now be restarted in the Normal Mode.

Source Code/Pseduo Code: I could not locate any copies of the Source/Pseudo Code. This is possibly due to the encryption of the worm plugins and the PGP encryption keys used. A copy of the virus is included in a zipped file with the password "infected". The W32.Hybris worm was downloaded from http://www.apsoftware.it/~niccolo/comp/virus/

Nancy Roberts-GCIH (roberts005)
Mary Washington College/JMC
25 February, 2001

Footnotes.

(1) Stuple, Stuart J., ed. Microsoft Press, Microsoft Windows NT Server Networking Guide. Ed, 1996, p. 782.
(2) www.cai.com/virusinfo/encyclopedia/descriptions/hybris.htm
(3) www.securityportal.com/research/virus/profiles/w32hybris.htm
(4) vil.mcafee.com/dispVirus.asp?virus_k=98873 &

Additional Resources.

Support.microsoft.com, Knowledge Base Article ID: Q129605, How to Extract Original Compressed Windows Files.

Support.microsoft.com, Knowledge Base Article ID:Q250662, Description of the TCP/IP Registry Entries in the MSTCP\ServiceProvider Subkey.