Global Information Assurance Certification Paper

W95.Hybris Virus AKA: Snow White and The Seven Dwarfs

Aaron King
5th April, 2001
Version 1.2b
Current as of December, 2000 (amended March 28, 2001)

Overview

The W95.Hybris.gen Virus has many names or aliases; Snow White virus, W32.Hybris.gen, W32.Hybris.gen.dr, Bris, W32.Hybris.22528.dr, W32/Hybris.gen.dll@M, W32/Hybris.plugin@M, W32/Hybris.gen@M, dwarf4you.exe, W95/Hybris.worm, Win98.Vecna.23040, I-Worm.Hybris.b and I-Worm.Hybris. Why so many names you ask, well that is simple. There are so many hacker tools out there, it is easy for a hacker or script kiddy to modify and change lines of code to have slightly different attributes.

This virus was discovered on 25th September 2000, it is believed to be of South American Origin. The W95.Hybris.gen virus has been categorized by SARC into the worm category. This means it will make copies of itself and propagate via the machine to the internet. The SARC has increased the level of threat to 4 (severe) for this virus as the Damage and distribution of this virus is HIGH.

The W95.Hybris.gen virus uses certain phrases in the subject and body.

From: HaHaHa@sexyfun.net

Subject: "Snowhite and the Seven Dwarfs - The REAL story!"

Body: "Today, Snowhite was turning 18. The 7 Dwarfs always where very educated and polite with Snowhite. When they go out to work at mornign, they promissed a *huge* surprise. Snowhite was anxious. Suddenly, the door open, and the Seven Dwarfs enter..."
(Obviously the authors didn't use a spell checker or grammar checker)

The filename can be chosen at random from a huge list found at http://securityportal.com/research/virus/profiles/w32hybris.html, but these are the four most common attachment names:

"dwarf4you.exe"
"joke.exe"
"sexy virgin.scr"
"midgets.scr"

The Owners of the “sexyfun.net” domain name have even gone to great efforts to clear their name and warn others of possible virus infection. They have created a site that gives information on the virus, explains that they are not affiliated with the virus and educates the public, that if you receive this email you are not on their mailing list

How the Virus Infects.

The prefix at the start of the virus name, W95 tells users that this virus replicates and operates on windows 95 and windows 98 operating systems. However this virus has been known to affect windows ME/2000 and Win NT 4.0.

When the worm attachment is executed, the Wsock32.dll file is modified or replaced. The temporary copy of WSOCK32.DLL is given a random filename consisting of 8 capital letters from A to P, for example "BFFKKCAL". It constantly checks to see if there is an active internet connection. When active the worm monitors all inbound and outgoing mail for SMTP addresses. This enables the worm to attach itself to all SMTP addresses and sends itself without the sender’s knowledge.

If Wsock32.dll is being used by the system, the worm cannot modify it. In this situation, the worm will add a registry entry to one of the following subkeys:

HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce

It always alternates between these two keys as the worm spreads from one computer to another. Whenever you send email, the worm sends a second message to the same person, attaching a copy of itself using a randomly generated file name.

Symptoms.

The worm attempts to connect to the alt.comp.virus newsgroup. If it connects successfully, the worm uploads its own plug-ins to this newsgroup in an encrypted form. It then does a comparison of version numbers and if necessary it downloads the latest plug-ins.

“F-SECURE, SARC, & McAfee Virus Definitions listed variations of these plug-ins”

The plug-ins are retrieved and stored in encrypted form (128 bit strong cryptography) and decrypted when needed. The worm supports up to 32 different plug-ins.

These plug-ins can do many things, below is a small list of known plug-ins.

1. Checks and updates plug-ins with the alt.comp.virus newsgroup, and then gets new plug-ins from there.

2. Spreads the worm to remote computers that are infected with the Backdoor. SubSeven Trojan. The plug-in detects such computers on the Web, and by using SubSeven commands, uploads a copy of the worm to the SubSeven infected computer.
3. It encrypts with a polymorphic encryption loop before sending the copy to others as an email attachment.
4. Display the text in French, Spanish or Portuguese, depending on the language setting on your computer.
5. Infects DOS executable programs. The DOS .exe infection is a fairly simple dropping technique. The virus code is appended to the end of the file with a small 16-bit dropper routine. This routine creates a temporary file with an .exe extension in the \Temp folder, and then executes it. After that, the routine deletes the temporary executable. This infects the Wsock32.dll file with the worm.
6. It can infect PE executable programs. Only large PE files that have a code section long enough will be infected. The virus infection plug-in packs the original code area and overwrites it, if it will fit in the same place.
7. Infects all .zip and .rar archives on all available drives from C: to Z:. While infecting the .zip and .rar files, the worm renames .exe files in the archive to .ex$ extensions, and adds its copy of the worm to the archive with a .exe extension
8. Generates a spiral image. If your system date is September 16 and 24, and on 59 minutes of any hour starting in 2001, the spiral image file is run. It loads some OpenGL libraries that are used to display a large black and white spiral image. It also registers itself as a service, which prevents the process from being displayed in the Close Program dialog box.

9. Another plug-in blocks access to particular web sites related to anti-virus organizations (not just anti-virus websites), based on their IP addresses. For example, infected machines will not be able to connect to:

www.vet.com.au
www.nai.com
www.sophos.com
www.pandasoftware.com
www.kasperksy.com
www.wildlist.org
www.symantec.com
www.irisav.com
www.antivirus.com

How to Clean-up or Repair.

Most viruses are easy to fix, there are normally 2 methods. The first method is to update your anti-virus definition files and use them to remove it, or the second (a little more complex) is to follow a step by step from the anti-virus company. These may include changing filenames, copy files and modifying the registry. This link will provide you with the details of removing the W95.Hybris.gen virus **http://vil.nai.com/vil/virusremovalInstructions.asp?virus_k=98873.**

"Below is a extract of the removal instructions for Windows ME/2000/95, from the above website."

Use specified engine and DAT files for detection and removal.

Windows 95/98 systems require rebooting to MS-DOS mode and scanning with the command line scanner SCANPM in order to clean such files as EXPLORER.EXE and TASKMON.EXE. Use the command line scanner such as
"SCANPM.EXE C: /CLEAN /ALL"

The WSOCK32.DLL file can be restored from backup. This can be done by:

Windows ME:
NOTE: Windows ME utilizes a backup utility that backs up selected files automatically to the C:_Restore folder. This means that an infected file could be stored there as a backup file, and VirusScan will be unable to delete these files. These instructions explain how to remove the infected files from the C:_Restore folder.

Disabling the Restore Utility

1. Right click the My Computer icon on the Desktop.
2. Click on the Performance Tab.
3. Click on the File System button.
4. Click on the Troubleshooting Tab.
5. Put a check mark next to "Disable System Restore".
6. Click the Apply button.

7. Click the Close button.
8. Click the Close button again.
9. You will be prompted to restart the computer. Click Yes.
NOTE: The Restore Utility will now be disabled.
10. Restart the computer in Safe Mode.
11. Run a scan with VirusScan to delete all infected files, or browse the the file's located in the C:_Restore folder and remove the file's.
12. After removing the desired files, restart the computer normally.
NOTE: To re-enable the Restore Utility, follow steps 1-9 and on step 5 remove the check mark next to "Disable System Restore". The infected file's are removed and the System Restore is once again active.

Use SFC to recover WSOCK32.DLL using instructions below for Windows 98/2000.

Windows 98/2000
- Click the START MENU|RUN, type SFC and click OK.
- Choose *Extract one file from the installation disk*
- Type C:\WINDOWS\SYSTEM\WSOCK32.DLL in the box and click Start.
- In the *Restore from* box type C:\WINDOWS\OPTIONS\CABS or browse to the Win98 directory on your Windows98 CD-ROM
- Click OK and follow remaining prompts

Wsock32.dll file exists within the Precopy1.cab cabinet file on the Windows 98 CD-ROM.

Windows95
WSOCK32.DLL can be found in the following CAB files:
Win95_11.cab on the Windows 95 CD-ROM
Win95_18.cab on the Windows 95 OSR2 CD-ROM
Win95_12.cab on the Windows 95 DMF disks
Win95_19.cab on the Windows 95 non-DMF disks

Below is an example for standard Windows 95
- Click the START MENU|SHUT DOWN choose RESTART IN MS-DOS MODE
- Type: EXTRACT /A C:\WINDOWS\OPTIONS\CABS\WIN95_11.CAB WSOCK32.DLL /L C:\WINDOWS\SYSTEM
or
- Insert your Windows95 CD-ROM and type:
EXTRACT /A D:\WIN95\WIN95_11.CAB WSOCK32.DLL /L C:\WINDOWS\SYSTEM Where *D:* is your CD-ROM drive.

As you can see this is a rather tedious way of removing something that could have been prevented in the first place.

How to avoid Viruses!

This is very simple, update your anti-virus software regularly and check all mail and file downloads from the internet. Educate your users not to open email attachments you are unfamiliar with, especially *.exe, *.scr and *.vbs. You can never beat all viruses as there are new viruses released every day. Be proactive, keep a watch on your favorite anti-virus and security websites for virus alerts, and remember the four main areas of security:

1) Defense in depth
2) Know your system
3) Principle of least privilege
4) Prevention is ideal but detection is a must.

References:

1. Symantec. "SARC Write up – W95,Hybris." 25 September 2000. URL: http://www.sarc.com/avcenter/venc/data/w95.hybris.gen.html (February 16, 2001)

2. McAfee. "W32/Hybris.gen@MM Virus removal Instructions" 16 September 2000 URL: http://vil.nai.com/vil/virusremovalInstructions.asp?virus_k=98873 (February 16, 2001)

3. Security Portal. "W32.Hybris Virus" URL: http://securityportal.com/research/virus/profiles/w32hybris.html (24 February, 2001)

4. Newsbytes. "Kaspersky Lab Warns Over Revamped Hybris Worm" 13 November 2000. URL: http://www.newsbytes.com/news/00/158042.html (1 March, 2001)

5. F-Secure. "Virus Definitions – Hybris" November 2000. URL: http://www.f-secure.com/v-descs/hybris.shtml (24 February, 2001)

6. Sexyfun.Net. "Disclaimer" (February & April 2001) URL: http://www.sexyfun.net (24 February, 2001 & 4 April 2001)

7. Planet IT. "Hybris: A Stealth Virus With Plug-ins" 9 January 2001 URL: http://www.planetit.com/techcenters/docs/security-hostile_content/news/PIT20010109S0021 (27 March, 2001)

8. Eric Cole. "Areas of Security, SANS GIAC Course" 12 February, 2001 (5 April 2001)