Global Information Assurance Certification Paper

Hybris – Stealth Worm+Trojan with plug-ins.

By Mark Laffan Sunday, April 01, 2001
Version 1.2

Introduction.

Russian developers at Kaspersky Labs (Cambridge, UK) first discovered the Hybris worm in October 2000, which originated from South America. "Hybris is one of the more common viruses we're seeing right now," said Brian Kinj, a member of the technical staff at Carnegie-Mellon's CERT Coordination Center.[1]

A virus' veraciousness is its downfall. New viruses can be detected by their payload, like the Melissa virus, which caused a denial of service to the email system on which it has infected. As soon as a virus is detected, by such an obvious effect, anti-virus protection software is rapidly updated. The more destructive the payload, the faster the detection, the quicker the update to the anti-virus software. Thus viruses tend to have a short life span as seen with the Melissa virus. But the hybris worm breaks this cycle. It is slow and subtle, it can linger in a persons system for months without detection. Since many people do not spend the extra effort to keep their anti-virus software up to date on their home PC or worse, don't use any anti-virus product at all, we will see this worm around a lot longer than most.

The Hybris worm is believed to have the same author as the Babylonia worm (believed to be a member of the VX-Brazil group), a concept virus that connected to a Japanese Web site known as the "Source of Chaos" and updated itself using files found on the site. Further investigation has revealed that the Hybris worm contains a copyright notice from the author known as "Vecna" which also appears in the Babylonia code.

The security firm Aladdin Knowledge Systems announced on their web page that they had proof that the virus had been created by the so-called VX-Brazil group. They claim that Vecna is a member of that group. It was also noted that:
"..Brazil continues to be a popular headquarters for hacker groups due to the lack of computer crime laws." [9]

Personal investigations and Internet searches also discovered the VX-Brazil Group [7] web page and a copy of the Hybris VBS dropper script was found in their latest news letter which did indeed include Vecna as the author of the Hybris worm.

What it does and how it works.

Everyone loves getting e-mail, even better when it comes with a little game or picture! Most users, no matter how much they have been told not to by the IT department, will run almost any attachment they receive. This is the most common form of virus infection know today, it's called social engineering.

I believe that the Hybris worm is based on the infamous Happy99 worm, also known as Win32/Ska, a program that was sent out to unwary users in the beginning of 1999 and remained active for almost a year. Once run, the Happy99 worm displayed a "fireworks" show and displayed "Happy New Year 1999!!" while in the background it modified the wsock32.dll file. From then on, providing the e-mail application supported SMTP e-mail communication, every time the user sent an e-mail the worm would immediately follow with an e-mail message containing itself in an attachment called "happy99.exe". Although this worm sends messages immediately, it was in the wild and infecting PC's for many months after its first release.

The Hybris worm also monitors the PC's network connection and builds a list of e-mail addresses from outgoing e-mail, but it does not send itself until a later date. To avoid detection the Hybris worm sends a slow and steady copy of itself instead of sending a torrent of e-mails to everyone on its list like the Melissa and LoveLetter viruses. Unlike Melissa and LoveLetter viruses, this worm has not been written as a script, it's a 32-bit windows program. Since 32-bit programs are optimized to run under windows, these programs run relatively fast compared to Visual basic script programs and can infect a lot of files in a short amount of time. This can make the virus spread throughout your system like wild fire with little outward appearance that it is doing so.

Once the attachment is executed (there is a list of names that it uses but it will have a EXE or SCR extension) it will modify or replace the wsock32.dll file which allows itself to communicate to the outside world. This enables it to hook to some of the Windows Sockets functions, namely connect(), send(), and recv(). If the wsock32.dll file is in use, it will add one of these registry keys to install itself on the next boot, this can change from PC to PC:

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

Until the next boot, the worm will be stored in %WinSystem% directory, under one of the names:

CCMBOIFM.EXE
LPHBNGAE.EXE
LFPCMOIF.EXE

Once the worm has attached itself to the system it will download updates (or plug-ins) from a WebPage or from alt.comp.virus. A similar behaviour was exhibited by the W95/Babylonia worm, which was propagated on the alt.crackers news group in Dec 3, 1999. The web pages hosting these files have been taken down by the Anit-virus community, but because their own news group, alt.comp.virus is being used to distribute the virus code, they can't shut it down as this will hamper their own ability to fight viruses. This still allows the plug-ins to be uploaded to infected Machines before a NNTP cancel message can be sent to remove the plug-in.

There are several different plug-ins known:

1. Infect all ZIP and RAR archives on all available drives from C: till Z:. While infecting the worm renames EXE files in archive with .EX$ extension and add its copy with .EXE extension to the archive (companion method of infection).

2. Send messages with encoded plug-ins to "alt.comp.virus" newsgroup, and gets new plug-ins from there.

3. Spread virus to remote machines that have SubSeven backdoor trojan installed. The plug-in detects such machines on the net, and by using SubSeven commands uploads the worm to the machine and spawns it in there.

4. Encrypt worm copies with polymorphic encryption loop before sending the copy attached to email.

5. Affects DOS EXE and Windows PE EXE files. The worm affects them so that they become worm droppers. When run, they drop worm's EXE file to TEMP directory and execute it.

Worm Payload

Since this worm can download new "updates" and incorporate them into new versions of itself, It can also change the entire base code of the virus and send this new version to other victims. This gives the worm the potential to bypass virus detectors, but Anti-virus firms have given it a low risk status since there is no destructive payload. Yet the Anti-virus Company McAfee has given this worm a medium risk status because of the worms widespread propagation. [8]

The reason that most anti-virus companies place this worm in a low risk category is that there are more malicious and destructive viruses in the wild than one like the Hybris worm which has the potential to be dangerous. Any virus or worm that has the potential to become dangerous should be carefully monitored, especially if it has been so widespread.

> Kaspersky Labs warns that the worm could, through some possible self upgrades, become malicious. Eugene Kaspersky, the firm's head of anti-virus research, said that the worm is possibly the most complex and refined malicious code in the history of virus writing.
> "Firstly, it is defined by an extremely complex style of programming. Secondly, all the plug-ins are encrypted with strong RSA 128-bit crypto algorithm key. Thirdly, the components themselves give the virus writer the possibility to modify his creation 'in real time' and in fact allow him to control infected computers worldwide," he said. [5]

Currently the only payload noticed has been a large animated spiral in the middle of the screen that is difficult to close and is activated on the 24th of September of any year, or at one minute before the hour during any day in the year 2001.

What is sent.

The Worm will arrive by email with the following fields:

From: Hahaha < hahaha@sexyfun.net >

Subject
One of the following:
Snowhite and the Seven Dwarfs - The REAL story!
Branca de Neve porne!
Les 7 coquir nains
Enanito si, pero con que pedazo!

Message body
One of the following:

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

Faltaba apenas un dia para su aniversario de de 18 anos. Blanca de Nieve fuera siempre muy bien cuidada por los en anitos. Ellos le prometieron una *grande* sorpresa para su fiesta de compleanos. Al entardecer, llegaron. Tenian un brillo incomun en los ojos...

C'etait un jour avant son dix huitieme anniversaire. Les 7 nains, qui avaient aide 'blanche neige' toutes ce s annees apres qu'elle se soit enfuit de chez sa belle mere, lui avaient promis une *grosse* surprise. A 5 heures comme toujours, ils sont rentres du travail. Mais cette fois ils avaient un air coquin...

Faltava apenas um dia para o seu aniversario de 18 anos. Branca de Neve estava muito feliz e ansiosa, porque os 7 annes prometeram uma *grande* surpresa. As cinco horas, os annezinhos voltaram do trabalho. Mas algo nao estava bem... Os sete annezinhos tinham um estranho brilho no olhar...

Attached file (strong language edited)
The attached file will have one of the following names:

midgets.scr, dwarf4you.exe, blancheneige.exe, s*xynain.scr, blanche.scr, nains.exe, branca de neve.scr, atchim.exe, dunga.scr, anno pomo.scr, enano.exe, enano porne.exe, blanca de nieve.scr, enanito fisgon.exe, s*xy virgin.scr, joke.exe

Variations
Depending on various plugins that could be installed the following variations might exist:

Subject
May contain random combination of the following words:

Anna, Raquel Darian, s*x, s*xy, Xena, Xusa, hot, hottest, Suzzete, c*m, famous, c*mshot, celebrity r*pe, hor*y, leather

Attached file.
May contain a random file from the list:

virgins.exe, boys.exe, girls.exe, SM.exe, sado.exe, cheerleader.exe, orgy.exe, black.exe, blonde.exe, sodomized.exe, hardcore.exe, sl*t.exe, doggy.exe, suck.exe, messy.exe, kinky.exe, fist-f*cking.exe, amateurs.exe, Anna.exe, Raquel Darian.exe, Xena.exe, Xuxa.exe, Suzete.exe, famous.exe, celebrity r*pe.exe, leather.exe, s*x.exe, s*xy.exe, hot.exe, hot test.exe, c*m.exe, c*mshot.exe, horny.exe, anal.exe, gay.exe, oral.exe, pleasure.exe, asian.exe, lesbians.exe, teens.exe

The Worm can also arrive with an empty message.

A sample plug-in was found during the writing of this assignment from the alt.comp.virus newsgroup before the message was canceled. Part of the message has been reproduced here.

From: Ann Onim <nobody@paracrypt.com>
Subject: h_2k DABA BAKnGhSnMhI
Date: Thu, 22 Feb 2001 23:46:03 +0100
Organization: mail2news@nym.alias.net

LIQLFPLCPPBCQFMG PENP{IAMKPJCFCIBHLFLNCLEJGBQHMFGFCG9MO
KLMEQJNCJBCLJJDPFJMAMGKOMJLB:IFQBJCILCIKJPLNCFELGFBNCEBL
NIP&BDPAGPIFNGOMQKPOMPNKIBKDFFPEEMMEFENNMOMAFCIDIMGL
HANGQMMOMDMJLPENICNQHDKOBBPHNKPOJDGCFBMFLBLEPJHFPDJH
FHHKGOAMAQJKECJFMIN*KBBMHPKGDPLPQACBJMFFPNLNMPCBFK3D
MPKNICKQIJNPMHMFDNGFEBM [snip]

Hybris.B Removal Instructions

A long hand method of virus removal was found on a Anti-virus web-site below [8]. An easier automated method created by the alt.comp.virus newsgroup participants, that would suit the everyday home computer user, can be found on their web site. See reference #2.

Windows 95/98 systems require rebooting to MS-DOS mode and run a DOS virus scanner in order to clean such files as EXPLORER.EXE and TASKMON.EXE. The WSOCK32.DLL file can be restored from backup. This can be done by:

Windows 98/2000/ME
1. Click the START MENU|RUN, type SFC and click OK.
2. Choose *Extract one file from the installation disk*
3. Type C:\WINDOWS\SYSTEM\WSOCK32.DLL in the box and click Start.
4. In the *Restore from* box type C:\WINDOWS\OPTIONS\CABS or browse to the Win98 directory on your Windows 98 CD-ROM
5. 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
1. Click the START MENU|SHUTDOWN choose RESTART IN MS-DOS MODE
2. 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

WindowsNT 4.0

Rename the Wsock32.dll file in the Windows \System32 folder to Wsock32.old. For information about how to rename a file, click Start, click Help, click the Index tab, type renaming, and then double -click the "Renaming files" topic.

1. Click Start, point to Programs, and then click Command Prompt.
2. Type cd\, and then press ENTER.
3. Insert the Windows NT CD -ROM into the CD -ROM drive, and then close the Windows NT screen if it appears.
4. Type the following line at the command prompt, and then press ENTER.

expand : \i386\wsock32.dl_ c: \\system32\wsock32.dll

where is the drive letter assigned to your CD -ROM drive, and where is the name of the folder in which Windows NT is installed.
5. Type exit, and then press ENTER to return to windows.
6. Finally, scan/clean using a updated antivirus scanner.

Prevention and Protection.

To prevent this worm infecting your PC, users should stick to a few simple rules.

- Beware any file sent by someone you don't know.
- Beware any file sent by someone you DO know.
- Check with the person who sent the email to verify that they sent it.
- Keep your virus scanning software up to date (even this does not protect you from new viruses!).
- Always scan attachments for viruses.
- If in doubt, throw it out!
- Common sense is a necessary part of virus protection.

Another good source of information about personal protection from viruses can be found on the "Safe Hex" web page provided by the alt.comp.virus news group, http://claymania.com/safe-hex.html

As for protection, system administrators should consider filtering all e-mail entering their e-mail server for executables using third party software like Mail Marshal (*http://www.mailmarshal.com/*) or using in-build file filtering if their server provides it.

As a Email administrator, I have to clean out our dead mail box every day as we currently receive over 30 Hybris worms being sent to our users. The only way we can stop the spread of this virus is to stop it at the source, the users, by educating them in safe email practices such as the list above.

References.

[1]. Louis, Tristan. "Hybris: A Stealth Virus With Plug-ins" 9th January 2001
URL: http://www.PlanetIT.com/docs/PIT20010109S0021

[2]. Courtesy of the alt.comp.virus newsgroup participants. "Hybris.B Removal Instructions" Rev. "G" 03/12/2001
URL: http://claymania.com/hybris-removal.html

[3]. Lemos, Robert "Hybris Worm: Sleeper hit of 2001" 12th January 2001
URL: http://aunz.yimg.com/computers/20010112/news/979301222-2013560837.html

[4]. "I-Worm.Hybris - AVP Virus Encyclopedia" 26th February 2001
URL:
http://www.viruslist.com/eng/viruslist.asp?id=4112&key=000010001300001000044

[5]. Dennis, Sylvia. "ComputerUser - Kaspersky Lab Warns Over Revamped Hybris Worm" 14th November 2000
URL: http://www.computeruser.com/news/00/11/14/news3.html

[6]. "Hybris: The Story Continues" Monday, November 13, 2000
URL: http://www.kaspersky.com/news.asp?tnews=0&nview=1&id=134&page=2

[7]. VX-Brazil Home page - [WARNING: Contains actual virus material]
URL: http://virusbrasil.8m.com/

[8]. "Mcfee W32/Hybris.gen@MM Virus Profile" 1st November 2000, 2:37:27 PM
URL: http://vil.mcafee.com/dispVirus.asp?virus_k=98873&

[9]. "Aladdin Discovers Creators of Common Hybris Vandal" 9th January 3:30pm
URL: http://biz.yahoo.com/bw/010109/il_aladdin_2.html