Global Information Assurance Certification Paper

The Hybris Virus
Ken Wolf
March 13, 2001

Articles written about the Hybris virus have used phrases such as “proof of concept” and “slow and steady wins the race” to describe it. One might agree with the authors when considering that this worm-type virus shows little sign of retreat since it was discovered “in the wild” in late September 2000. And, unlike mass mailer viruses such as Melissa and ILOVEYOU, Hybris produces a steady trickle of virulent e-mail, making infections less noticeable. The spread of this malicious code is largely due to successful social engineering; in this case, appealing to a individuals interested in viewing pornographic images. Hybris is written as a 32-bit Windows program, making it capable of infecting hundreds of files in a matter of seconds upon execution. While it currently carries a non-destructive payload, it contains a plug-in architecture allowing it to incorporate different extensions into its code, thus enabling it to evolve into a much more dangerous virus.

Hybris Virus - Description

Hybris has been classified as a worm by most anti-virus firms and security advisories because it distributes itself through email messages and newsgroup postings. A user, however, must execute an infected attachment received in email or from a newsgroup posting in order to infect a machine. Some Internet sources report other methods by which it can distribute itself; these include SubSeven commands and ICQ. According to information that CERT/CC is reporting to have received and information from other security advisories, Hybris works under Win32 systems only.

Upon execution, the virus infects the Windows Internet sockets library file WSOCK32.DLL, enabling it to monitor a PC’s network connection for e-mail messages. When an e-mail message is detected, Hybris collects sender addresses and compiles a list of addresses in a file. Later on, Hybris randomly selects destinations from this list to send copies of itself as attachments to e-mail.

Hybris is able to modify WSOCK32.DLL even if it has been write protected. It does so by first making a copy of WSOCK32.DLL, infecting that copy, and then writing the name of the infected copy in the WIN.INI initialization file. The next time Windows is rebooted, the system recognizes the infected library rather than WSOCK32.DLL. Hybris ensures its persistence by making a copy of itself with a random name such as FIDGFHIK, then writing an entry pointing to this copy in the Windows System Registry – specifically the *Run_Once* Registry key. Therefore, even if its original copy is erased, Hybris can recopy itself.[1]

Hybris can upgrade its own code modules by connecting to the alt.comp.virus

Usenet newsgroup or to a series of Web sites and downloading encrypted updates. Reportedly, most of the Web sites to which Hybris can connect have been shut down. According to information posted on F-Secure's anti-virus Web pages, there were up to 32 different plug-ins found in Hybris versions as of January 2001. All of the plug-ins are encrypted with a very strong RSA 128-bit crypto-algorithm key.

Hybris Virus - Plug-ins and alt.comp.virus Usenet[2]

Hybris' functionality depends on its host machine being able to download up to 32 encrypted plug-ins, which are stored in a 128-bit encrypted virus body. Once active on a host machine, Hybris will attempt to connect to a randomly selected news server (from a list of more than 70), convert its plug-ins to binary messages, and post them on the server.

Posted messages have a random subject, for example:

encr HVGT GTeLKzurGbGvqnuDqbivKfCHWbizyXiPOvKD
encr CMBK bKfOjafCjyfWnqLqzSTWTuDmfefyvurSLeXGHqR
text LNLM LmnajmnKDyfebuLuPaPmzaLyXGXKPSLSXWjKvWnyDWbGH
text RFRE rebibmTCDOzGbCjSZ

where the first four characters in the newsgroup postings represent plug-in "name", and the following four characters represent the encoded plug-in "version." In addition to sending encrypted plug-ins, Hybris reads such messages from alt.comp.virus, gets plug-in "name" and "version", and compares these with plug-ins that are currently stored on the host machine. When a higher plug-in version is found, Hybris extracts it and replaces the existing one.
Hybris drops its plug-ins to disk as random named files in the Windows system directory. (Kaspersky/Podrezov)

There are several different plug-ins known:

1. Search for executables in ZIP and RAR files, renaming any found to EX$ and then adding itself to the archive with the original name

2. Send messages with encoded plug-ins to alt.comp.virus newsgroup, and download new plug-ins from newsgroup posts.

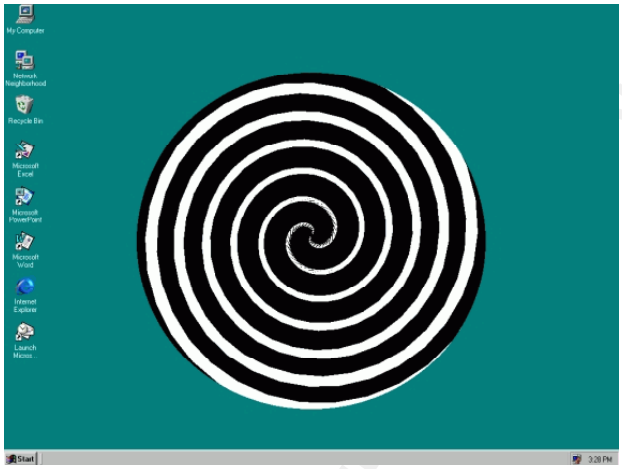
3. Spread virus to remote machines that have SubSeven backdoor trojan installed by using Subseven commands.

4. Encrypt virus with polymorphic routine before sending a copy as an attachment to email. By upgrading this component the author can change the appearance of the malicious code in an attempt to defeat anti-virus

scanners.

5. Infect DOS EXE and Windows PE EXE files. "The DOS EXE is 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 executes it. It then deletes the temporary executable. In this way, Wsock32.dll is infected with the actual worm body. The PE executables have a much more complicated file infection process. PE files become infected only if they have a long enough code section. The virus infection plug-in packs the original code area and overwrites it if it will fit in the same place."[3]

6. On September 24th of any year, or at one minute to every hour, display a large black and white spiral effect. The spiral effect looks like the picture below:



7. Randomly select Subject, Message text and Attach name while sending copies with email messages (Hybris checks the language settings of the computer it has infected and accordingly selects an English, French, Portuguese, or Spanish message to send):

   From:
   Hahaha <hahaha@sexyfun.net>

   Subjects:

   Snowhite and the Seven Dwarfs - The REAL story!
   Les 7 coquir nains
   Branca de Neve pornô!
   Enanito si, pero con que pedazo!

   Message texts:

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

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...

Faltava apenas um dia para o seu aniversario de 18 anos. Branca de Neve estava muito feliz e ansiosa, 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...

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 names:

enano.exe	midgets.scr	branca de neve.scr
enano porno.exe	dwarf4you.exe	atchim.exe
blanca de nieve.scr	blancheneige.exe	dunga.scr
enanito fisgon.exe	sexynain.scr	anão pornô.scr
sexy virgin.scr	blanche.scr	
joke.exe	nains.exe	

Depending on which plug-ins the malicious code has downloaded, recipients may receive a Hybris with no discernible sender (i.e, From: <>), no subject, and no text. Hybris can also send itself with a random, 8-letter attachment such as CGOJIFCG.EXE.

Hybris Virus - Basic Steps for Prevention and Containment

1. Exercise caution before opening any email attachments. Attachments should always be scanned by anti-viral software with current virus definitions and scan engine files before being opened. Users should only open file or image attachments that are expected, including those from known sources.

2. Stay informed of new Hybris threats by subscribing to virus and security e-mail lists from anti-virus firms and security advisories.

3. Where possible, deploy a multi-layered virus protection system. Anti-viral software should be deployed on e-mail gateway servers, file servers, and all networked desktops and notebooks. Protection should also be deployed on stand-alone desktops, portables, notebooks, and in conjunction with servers or appliances performing firewall or Web proxy functions. Employee-owned computers should also be protected with updated anti-viral software.

4. Keep signatures up to date on all systems running anti-viral software.

5. Schedule automated system scans, or run manual system scans, on a regular basis with updated signatures from software vendors.

6. Set up sender and/or subject type filters on mail servers and systems running mail clients to discard messages containing Hybris infected attachments.

Hybris Virus – Links to Removal Tools and Removal Information

F-Secure Corp.: ftp://ftp.europe.F-Secure.com/anti-virus/free/ ftp://ftp.europe.F-Secure.com/anti-virus/updates/f-prot/dos/

> It is a requirement to clean system from pure DOS.
>
> Note: Since Hybris has a plug-in that infects EXE files, it is advised to clean all infected files first, then remove all locked Hybris components manually afterwards. (Kaspersky/Podrezov)

Symantec Corporation:
http://www.symantec.com/avcenter/venc/data/w95.hybris.gen.html
http://www.symantec.com/avcenter/venc/data/w95.hybris.plugin.html

Hybris Virus – My Personal Experience

This particular virus has been a concern at my workplace for several months, as our anti-viral software has logged several hundred blocked messages. Significant time and resources have been spent analyzing anti-viral software logs and email headers trying to determine original IP sources addresses of infected messages. Because of Hybris and other "malware" threats, we have intensified our efforts to load anti-viral software on notebooks and on employees' home PC's; these are the two areas where we determined anti-viral software is least likely to have current signatures. In addition, it has caused us to re-evaluate our e-mail use policies as they relate to downloading personal Web-based e-mail and procedures for e-mail users to follow before opening file and image attachments.

We have had some initial success blocking Hybris by modifying a patch written by Sendmail for the Melissa virus. This was done to avoid a stream of notifications to our users from our anti-viral software. The patch will filter messages based on specific subject text. Detailed information of the patch can be found at: http://www.sendmail.com/alert/melissa/ .

The following is an example of commands inserted into our sendmail.cf file(s):

```
##############################################
###  Local Rulesets  ###
##############################################

# ILOVEYOU Worm

HSubject: $>Check_Subject
D{MPat}ILOVEYOU
D{MMsg}This message may contain the LoveLetter virus.

# Snowhite
D{Mpat2}Snowhite and the Seven Dwarfs - The REAL story!
D{MMsg2}This message may contain the Dwarf virus.

#####################################################
# Be sure to use tab characters between the "$*" and the "$#".
#####################################################

SCheck_Subject
R${MPat} $*     $#error $: 553 ${MMsg}
RRe: ${MPat} $* $#error $: 553 ${MMsg}
R${MPat2} $*    $#error $: 553 ${MMsg2}
RRe: ${MPat2} $*        $#error $: 553 ${MMsg2}

#####################################################
```

References

1. Robert Lemos, Hybris virus: Sleeper hit of 2001, ZDNet News, January 11, 2001
   URL: http://www.zdnet.com/zdnn/stories/news/0,4586,2673789,00.html
2. Catherine Par, Hybris Virus Understated But Dangerous, Newsfactor Network, January 17, 2001
   URL: http://www.newsfactor.com/perl/story/6774.html
3. Tristan Louis, Hybris: A Stealth Virus With Plug-Ins, Planet IT, January 9, 2001
   URL: http://www.planetit.com/techcenters/docs/security-

hostile_content/news/PIT20010109S0021

4. CERT® Coordination Center, Open Mail Relays used to deliver “Hybris Worm”, March 2, 2001
   URL: http://www.cert.org/incident_notes/IN-2001-02.html
5. Eugene Kaspersky, KL; Alexey Podrezov, F-Secure Corp.; F-Secure Virus Definitions: Hybris; Nov 2000 – Jan 2001
   URL: http://www.f-secure.com/v-descs/hybris.shtml
6. Cary Ng; Peter Ferrie, W95.Hybris.gen, Symantec AntiVirus Research Center, September 25, 2000
   URL: http://www.symantec.com/avcenter/venc/data/w95.hybris.gen.html
7. W32/Hybris-B; W32/Hybris-C; W32/Hybris-D, Sophos Virus Analyses
   URL: http://www.sophos.com/virusinfo/analyses/w32hybrisb.html
   URL: http://www.sophos.com/virusinfo/analyses/w32hybrisc.html
   URL: http://www.sophos.com/virusinfo/analyses/w32hybrisd.html
8. Robert Vamosi, Hybris Displays Some Hubris, ZDNet Help & How-To, November 14, 2000, revised January 11, 2001
   URL: http://www.zdnet.com/zdhelp/stories/main/0,5594,2653488,00.html

---

[1] Tristan Louis, Hybris: A Stealth Virus With Plug-Ins, Planet IT, January 9, 2001
[2] Eugene Kaspersky, KL; Alexey Podrezov, F-Secure Corp.; F-Secure Virus Definitions: Hybris; Nov 2000 – Jan 2001; and W32/Hybris-B; W32/Hybris-C; W32/Hybris-D, Sophos Virus Analyses
[3] Cary Ng; Peter Ferrie, W95.Hybris.gen, Symantec AntiVirus Research Center, September 25, 2000