



Pinwheel: Pinfi-Infected Malware
infectionvectors.com
January 2006

Overview

Like any other discipline, writing malware requires that one learn from the successes of previous crafters. Malware authors are interested, by and large, in the tactics and tricks of widespread code. They may be led to keeping large zoos of code on personal machines. Often times, keeping a library of such applications can lead to unintended consequences, including infection of new code with old viruses. Such admiration of previous attacks is part of the professional cycle; every professional studies the work of others, modifies those pieces that can be used, discards the irrelevant, and hopes to build on the body of work – adding something meaningful to the community. In one way or another, that is achieved almost everyday in the malware world.

Pending

In October of 2001, the virus known as Pinfi (or Parite) was discovered. It infected EXE and SCR files in the way a true parasitic virus would (in this particular case, the infection comes by way of appending the viral components onto the discovered files), but also left an infection marker in the Windows Registry:

```
HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer PINF
```

The virus infected a regimented number of programs at a time, preventing the viral routine from overwhelming system resources and possibly alerting the user. Pinfi then created a randomly named file in the %TEMP% directory. This file was an executable, which the malware then kicked off. In addition, Pinfi itself attaches to Explorer.exe to remain memory resident. Infected files are also appended with “junk” data, impacting the virus and remediation efforts in two ways: 1) it makes the virus classification polymorphic, 2) when combined with the fact that Pinfi does not record the original file size of its targets, cleaning the appended pieces is impossible for an automated tool. Therefore, when cleaned, some self-checking applications would no longer run.

The code used to create and execute the second piece of malware (loaded into the %TEMP% directory) is written in assembler, making it appear to have come from a rather skilled coder. The “dropped” malware is C++ (Borland). As is evident, the dropped piece of malware could have been anything. However, the Pinfi portion of the code would be discovered fairly readily by any anti-virus updated since the fall of 2001. Consider a threat that is dropped by a file infector like Pinfi. The Pinfi “wrapper” is immediately discovered by the resident anti-virus and removed. The “clean” file underneath (assuming, as in the case below, that the anti-virus software did not recognize

the new code as a threat) would then seem harmless to many users, as it has been scanned, and cleared.

Pinfi provides a powerful vehicle to malware creators as it can give any piece of code classic virus properties, the ability to infect executable files. Nonetheless, attacks of this type are rare and are often the result of an executable being accidentally infected.

Popular Cuts

Within the last 18 months, a few worms have been found in circulation infected with Pinfi. Mytob, one of the most widely successful malware applications of 2005 had Pinfi in its Q iteration. Dinfor, a worm that used the familiar RPC DCOM (MS03-039) exploit, also came pre-packaged with Pinfi. One may recall that phony Microsoft patches have been the hook to get users to download Pinfi and its cohorts throughout 2005.

A number of the “bot” variants make use of Pinfi. As the Codbot, Agobot, etc. families of the world are rather adept at network propagation, replacing the “dropped” portion of Pinfi with them makes pretty good sense. It would be possible to fool anti-malware software by changing the appearance of a Trojan by infecting it with a virus. But, that seems an unlikely strategy with Pinfi as it so old there is much more risk that it would trigger an alert than the Trojan underneath.

It is also quite possible that each of the above mentioned executables was unwittingly infected and released. Malware authors are apt to keep a number of samples on their system, quite possibly a copy of Pinfi was running live.

In January of 2006, another new copy of the “postcards” scam was received by infectionvectors.com, postcards.gif.exe. The Trojan itself works like the previous incarnations of this attack (see below for more information), however, there was a new wrinkle to the malware.

As seen below, the installation (this time on a Win9x machine, for no scientific reason) shows the new files, related to the IRC Trojan. These have no size prior to the installation, as the files did not exist. However, note the files at the bottom of the table. These did exist prior to the installation, and now show an increase in size of approximately 170KB, an indication that they have been infected with Pinfi.

File	Size Prior	Size After
C:\WINDOWS\SYSTEM\nicks.txt		177KB
C:\WINDOWS\SYSTEM\aliases.ini		1KB
C:\WINDOWS\SYSTEM\control.ini		1KB
C:\WINDOWS\SYSTEM\mirco.ini		4KB
C:\WINDOWS\SYSTEM\remote.ini		1KB
C:\WINDOWS\SYSTEM\script.ini		9KB
C:\WINDOWS\SYSTEM\servers.ini		3KB
C:\WINDOWS\SYSTEM\users.ini		1KB
C:\WINDOWS\SYSTEM\sup.bat		1KB

C:\WINDOWS\SYSTEM\svchost.exe		1,969KB
C:\WINDOWS\SYSTEM\download		1KB
C:\WINDOWS\SYSTEM\logs		1KB
C:\WINDOWS\SYSTEM\sounds		1KB
C:\WINDOWS\SYSTEM\mirco.ico		6KB
C:\WINDOWS\SYSTEM\sup.reg		1KB
C:\WINDOWS\HWINFO.EXE	111KB	289KB
C:\WINDOWS\ASD.EXE	62KB	240KB
C:\WINDOWS\CLEANMGR.EXE	132KB	309KB
C:\WINDOWS\CVTAPLOG.EXE	78KB	256KB
C:\WINDOWS\DRWATSON.EXE	140KB	317KB

Upon further analysis, the files were, in fact, found to be infected with the parasite. Additional information on Pinfi itself can be found in the References section.

The Trojan encased in the virus is an IRC-based backdoor, equipped with a copy of mIRC, numerous configuration files, and installation scripts for Registry modifications. The Trojan is nearly identical (with only nick, server, etc. changes being immediately noticeable) to previous IRC Trojans analyzed along with the “postcard” scams.

The Trojan drops “svchost.exe” into the %SYSTEM% directory and then inserts a Registry entry to start the application each time Windows loads:

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
"GNP Generic Host Process"="C:\\Windows\\System32\\svchost.exe"
```

Also in this directory are nine INI files and three additional directories named, “download,” “sounds,” and “logs.” The svchost.exe file is mIRC, and the customizations direct the client to an IRC channel where it awaits commands, likely from one or more of the four handles it notifies upon startup. There are numerous servers listed in the servers.ini file and thousands of possible NICKS in the nicks.txt file.

The icon used, “mirco.ico” is blank, it will display no obvious clue to the machine’s operator. Startup controls are defined by the script.ini file, now well known to mIRC users as generally malicious, which assures that notification and proper connections to the server/channel are established.

Classical

The network worm, the rootkit, and mass mailer have overshadowed the file-infector in recent years, however, it manages to live on, in the form of new inventions (although much fewer than in years past) and successful variants from the past, such as Pinfi. Most likely, Pinfi was most likely introduced to this Trojan by mistake, as it only leads to a greater likelihood of detection. It is always possible though that it is a case of an admirer hoping to further the life of this classic parasite by adding it to a new strain of his or her own code. A sort of homage to the code of the past...

References

Pinfi at Symantec

<http://securityresponse.symantec.com/avcenter/venc/data/w32.pinfi.html>

Parite at Kaspersky/Viruslist

<http://www.viruslist.com/en/viruses/encyclopedia?virusid=20924>

Pate at McAfee

http://vil.nai.com/vil/content/v_99690.htm

Mytob.Q infected with Pinfi

<http://securityresponse.symantec.com/avcenter/venc/data/w32.mytob.q@mm.html>

Dinfor dropped a Pinfi-infected file

<http://securityresponse.symantec.com/avcenter/venc/data/w32.dinfor.worm.html>

Fake Microsoft patch infected with Pinfi

<http://www.eweek.com/article2/0,1895,1817915,00.asp>

“Fake Microsoft Patch Triggers Virus Attack.” eWeek, Ryan Naraine, 19 May 2005.

IRC Trojan from postcard malware

http://infectionvectors.com/vectors/mail_call_pt4.htm

IRC Trojan described as Zapchas at Sophos

<http://www.sophos.com/virusinfo/analyses/trojzapchasaa.html>