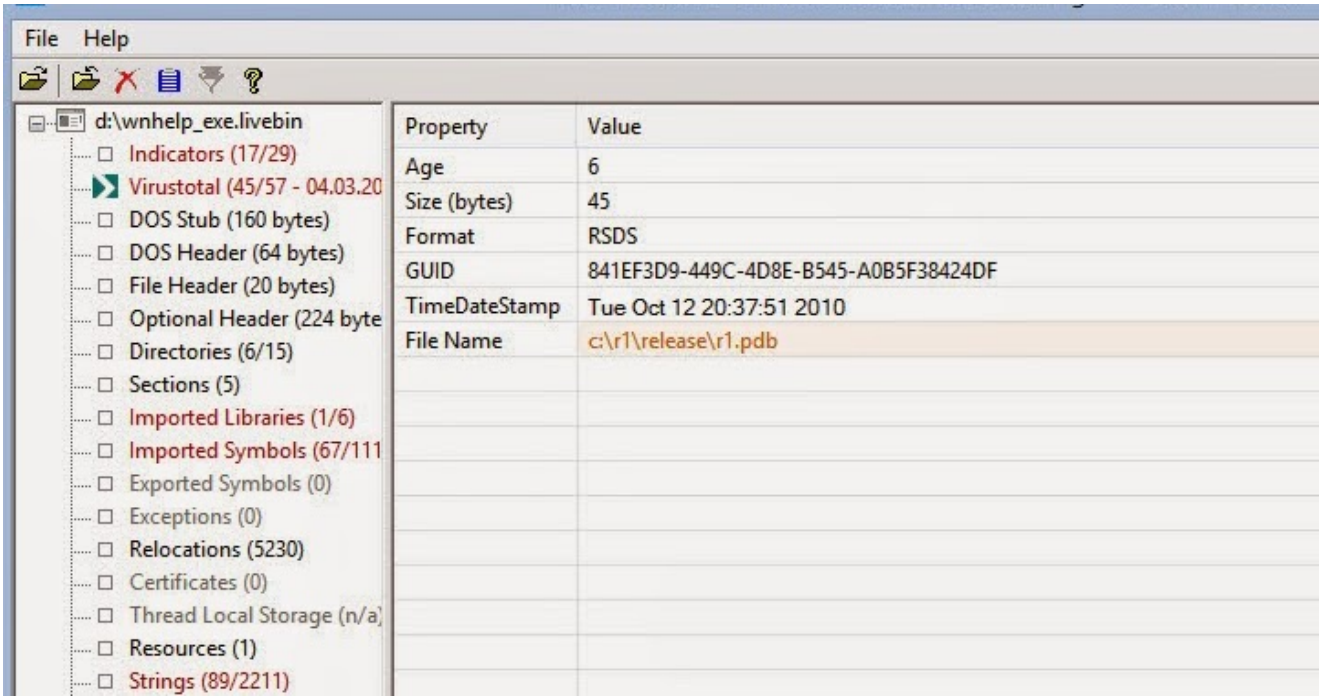
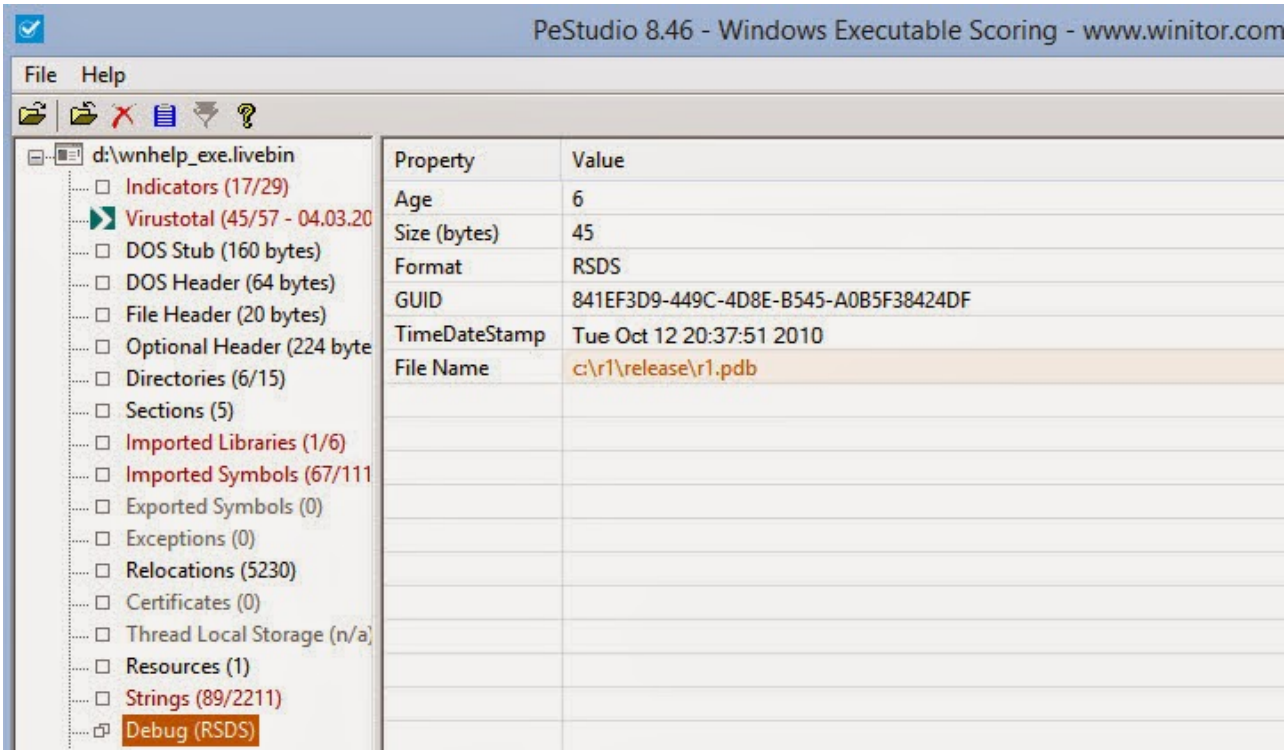
And you get a POS malware name...and you get a POS malware name....and you get a POS malware name....

brimorlabsblog.com/2015/03/and-you-get-pos-malware-nameand-you-get.html

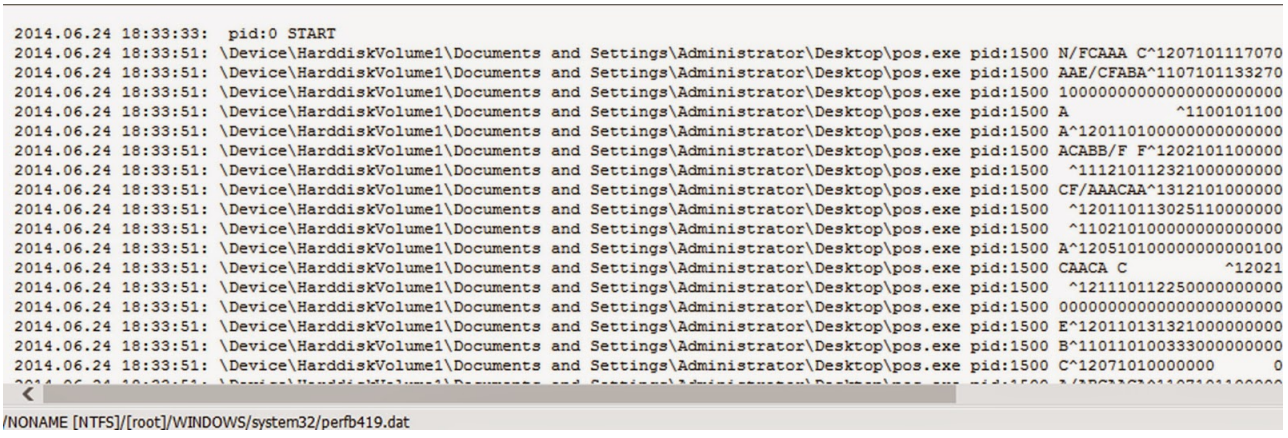


This morning I woke up to find Trend Micro/Trend Labs had a new post on an "old undetected PoS malware" which they have called "PwnPOS". I was interested at first, but this looks like just another case of randomly assigning names to malware and/or threat actors. Unfortunately for the folks at Trend, who usually put out pretty good work, the scraper in question (which is an executable file that I have personally seen with many names, but we will refer to it as "wnhelp.exe") is old. Very, very old. In fact, the date/time stamp embedded into the file itself is from 2010.



wnhelp as seen in PEStudio 8.46

The scraper is very basic, it looks through memory looking for Track data, and when it finds matching data, it saves it to a file "perfb419.dat" which is under the Windows/System32 folder. There are sometimes legitimate files with similar names under this path, no doubt it was an effort for the attackers to try to make the data blend in.



Example of "track" data collected in perfb419.dat.

The scraper itself does not have an active exfiltration mechanism, so either an additional file(s) is needed to exfil the collected data or the attacker(s) can remotely access the system and send the file out (email, ftp, file sharing site, etc). wnhelp uses a "service" persistence mechanism in order to stay running on the machine, so looking at just CurrentVersion/Run in

the Registry will not allow you to detect the file. The service is named "Windows Media Help", and the information that is collected from the Live Response Collection using SysInternals autorunsc is listed below:

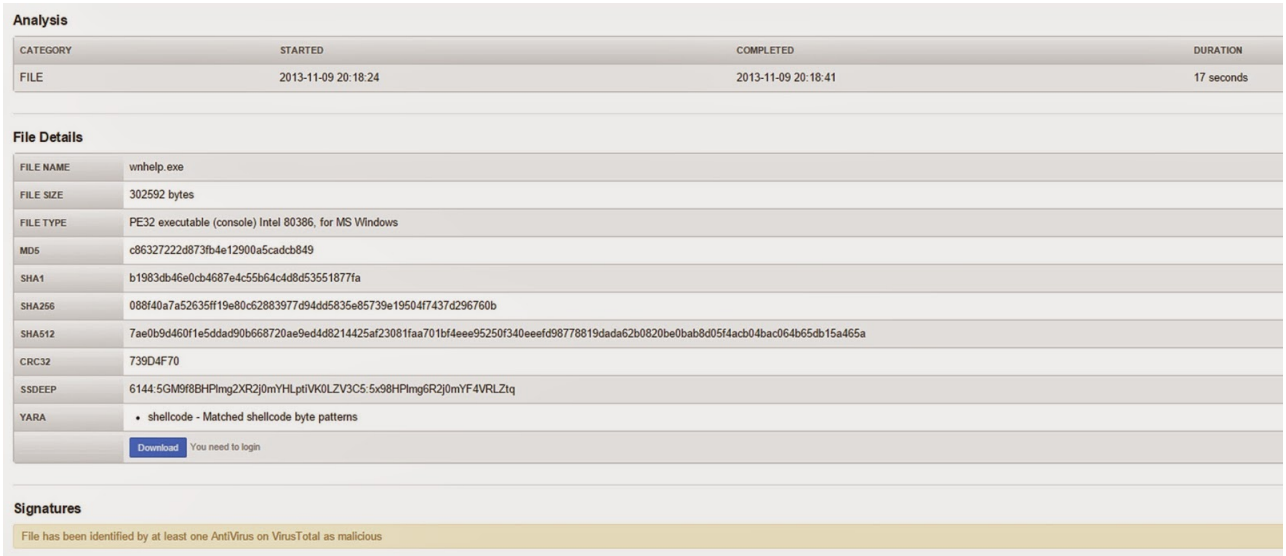
```
Windows Media Help
  "C:\WINDOWS\system32\wnhelp.exe" -service
  c:\windows\system32\wnhelp.exe
  10/12/2010 8:37 PM
  MD5:      c86327222d873fb4e12900a5cadcb849
  SHA1:     b1983db46e0cb4687e4c55b64c4d8d53551877fa
  PESHA1:   030880107F274FF416EE8326F878D14A7A4FB46D
  SHA256:   088f40a7a52635ff19e80c62883977d94dd5835e85739e19504f7437d296760b
```

wnhelp embedded under the "Windows Media Help" service

The exfiltration methods listed in the Trend article "might" be new, but I cannot be certain as I personally do not have access to those files (yet, I am working on that). I am leery of how new these files may be though, simply based on the liberties that Trend appears to have taken with the original wnhelp file. Additionally, of all the files listed in the Trend post, the most recent compile time is listed as 2012, with most of the compile times dating back to 2010. None of these files appear to be "new" at all.

Not "new" or "under the radar"

Back in 2013, the wnhelp sample was uploaded to malwr, among other sites, to use their automated malware analysis tool.



Analysis

CATEGORY	STARTED	COMPLETED	DURATION
FILE	2013-11-09 20:18:24	2013-11-09 20:18:41	17 seconds

File Details

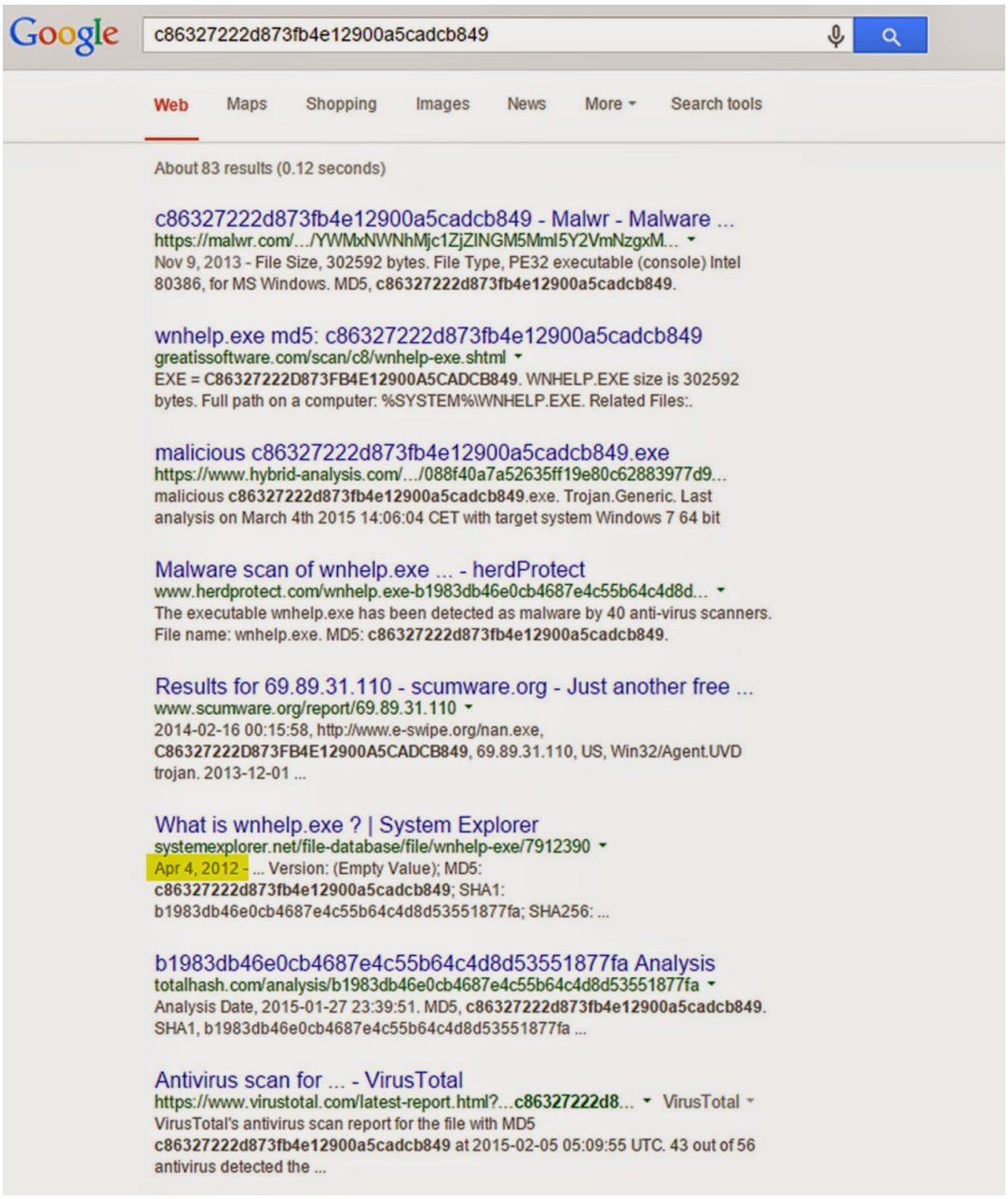
FILE NAME	wnhelp.exe
FILE SIZE	302592 bytes
FILE TYPE	PE32 executable (console) Intel 80386, for MS Windows
MD5	c86327222d873fb4e12900a5cadcb849
SHA1	b1983db46e0cb4687e4c55b64c4d8d53551877fa
SHA256	088f40a7a52635ff19e80c62883977d94dd5835e85739e19504f7437d296760b
SHA512	7ae0b9d460f1e5ddad90b668720ae9ed4d8214425af23081faa701bf4eee95250f340eeefd98778819dada62b0820be0bab8d05f4acb04bac064b65db15a465a
CRC32	739D4F70
SSDEEP	6144:5GM9f8BHPlmg2XR2j0mYHLptiVK0LZV3C5:5x98HPlmg6R2j0mYF4VRLZtq
YARA	• shellcode - Matched shellcode byte patterns
	Download You need to login

Signatures

File has been identified by at least one AntiVirus on VirusTotal as malicious

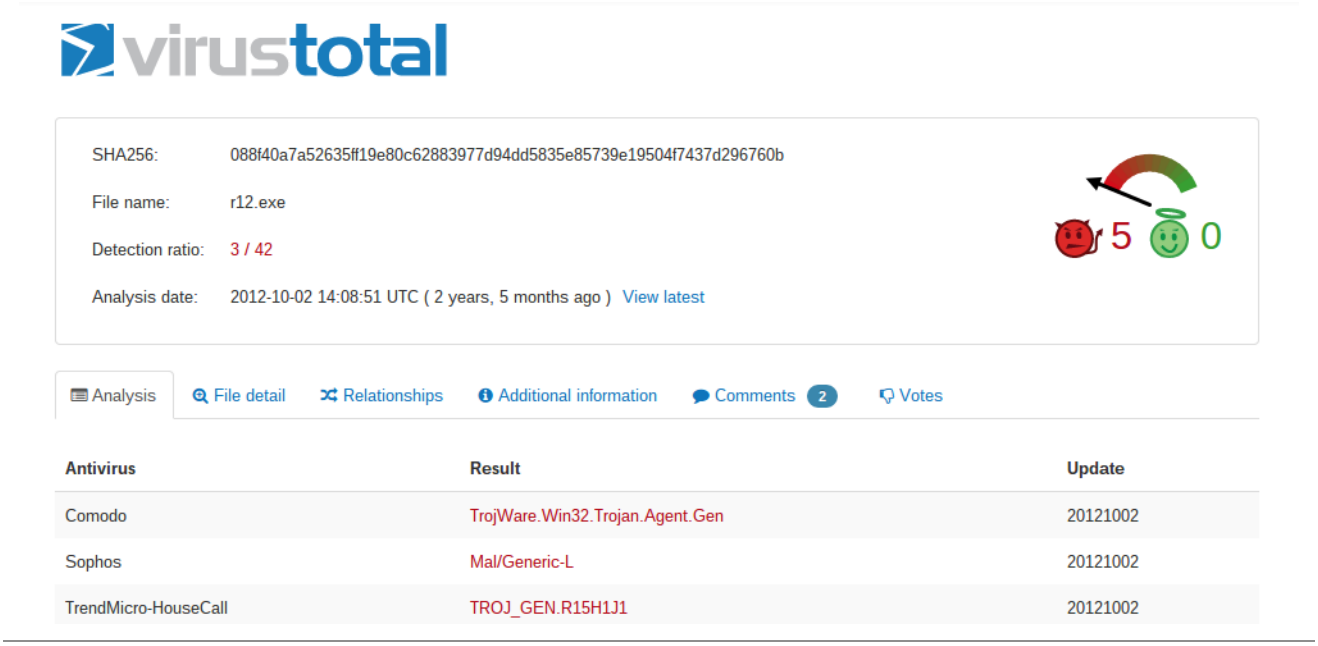
malwr results from 2013

Additionally, a Google search for the md5 hash (c86327222d873fb4e12900a5cadcb849) shows that, at the very least, a user of the domain "systemexplorer.net" posed a question about wnhelp back in 2012. I did not dig through all of the results, but 83 search results, with several entries on the first page relating to "malware" in one form or another, is hardly flying "under the radar".



systemexplorer.net query of wnhelp from 2012

UPDATE (March 6, 2015): As @maldr0id pointed out, the wnhelp file was submitted to virustotal back on October 2, 2012, with a 3/42 detection ratio. Interestingly enough, Trend Micro was one of the three that detected the file as malicious. The same file was uploaded to virustotal on February 16, 2011. At that time it had a 0/43 detection ratio.



virustotal

SHA256: 088f40a7a52635ff19e80c62883977d94dd5835e85739e19504f7437d296760b

File name: r12.exe

Detection ratio: 3 / 42

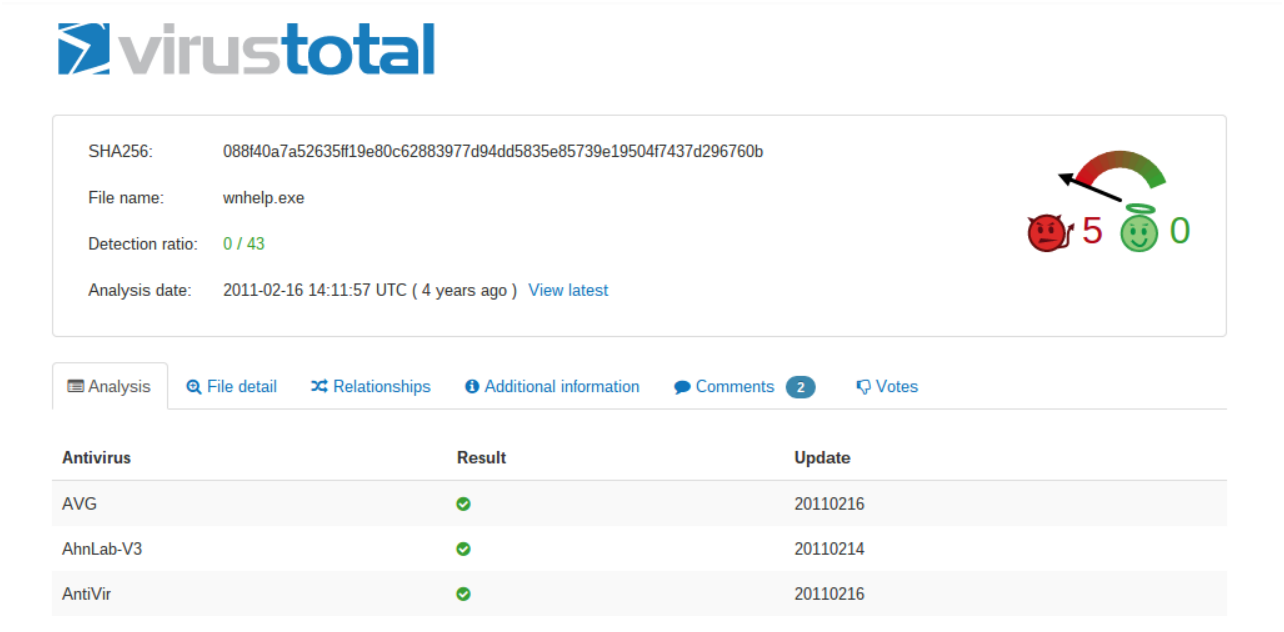
Analysis date: 2012-10-02 14:08:51 UTC (2 years, 5 months ago) View latest

5 0

Analysis | File detail | Relationships | Additional information | Comments 2 | Votes

Antivirus	Result	Update
Comodo	TrojWare.Win32.Trojan.Agent.Gen	20121002
Sophos	Mal/Generic-L	20121002
TrendMicro-HouseCall	TROJ_GEN.R15H1J1	20121002

virustotal results of scraper file, performed on October 2, 2012



virustotal

SHA256: 088f40a7a52635ff19e80c62883977d94dd5835e85739e19504f7437d296760b

File name: wnhelp.exe

Detection ratio: 0 / 43

Analysis date: 2011-02-16 14:11:57 UTC (4 years ago) View latest

5 0

Analysis | File detail | Relationships | Additional information | Comments 2 | Votes

Antivirus	Result	Update
AVG	✓	20110216
AhnLab-V3	✓	20110214
AntiVir	✓	20110216

virustotal results of scraper file, performed on February 16, 2011

In the Trend post, the author stated "*PwnPOS is one of those perfect examples of malware that's able to fly under the radar all these years*". As you can see from just the examples that are listed above, that statement is simply not true. It does highlight the importance of understanding "what" is running within your POS environment. It also highlights the fact of regularly checking systems within your POS environment to make sure that they are running properly and there is nothing "else" (malicious or otherwise) running on those systems.

Several month ago I came across a domain that was hosting this (and other) samples of POS malware. I collected all of the samples and files on the domain. The owners of the domain let the registration lapse a few months ago, at which time I purchased it and re-directed it to "fbi.gov" (my own way of "getting back" at bad actors). If you are interested please feel free to contact me, I will share some of the files with you (I cannot share them all, as some of the files contained information that I legally cannot share).