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

		에서 한 것 같은 것은 것이다는 것이 있는 것은 것이다. 것은 것이다. 한것을 가지 않았다. 것은 이것은 것은 것은 것은 것을 가지 않았다. 같은 것은
File Help		
🗃 🖆 🗡 🗎 🔻 🤋		
d:\wnhelp_exe.livebin	Property	Value
🗆 Indicators (17/29)	Age	6
Virustotal (45/57 - 04.03.20	Size (bytes)	45
DOS Stub (160 bytes)	Format	RSDS
·····□ DOS Header (64 bytes) ·····□ File Header (20 bytes)	GUID	841EF3D9-449C-4D8E-B545-A0B5F38424DF
Optional Header (20 bytes)	TimeDateStamp	Tue Oct 12 20:37:51 2010
Directories (6/15)	File Name	c:\r1\release\r1.pdb
Sections (5)		
Imported Libraries (1/6)		
Imported Symbols (67/111		
Exported Symbols (0)		
D Exceptions (0)		
🗆 Relocations (5230)		
Certificates (0)		
Thread Local Storage (n/a)		
C Resources (1)		
🗆 Strings (89/2211)		

This morning I woke up to find Trend Micro/Trend Labs had a new post on an "<u>old</u> <u>undetected PoS malware</u>" 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.

ile Help		
ŝ 🖾 🗡 🗎 🔻 😵		
d:\wnhelp_exe.livebin	Property	Value
Indicators (17/29)	Age	6
Virustotal (45/57 - 04.03.20	Size (bytes)	45
DOS Stub (160 bytes)	Format	RSDS
DOS Header (64 bytes)	GUID	841EF3D9-449C-4D8E-B545-A0B5F38424DF
Dile Header (20 bytes) Doptional Header (224 byte	TimeDateStamp	Tue Oct 12 20:37:51 2010
Directories (6/15)	File Name	c\r1\release\r1.pdb
Sections (5)		
Imported Libraries (1/6)		
Imported Symbols (67/111		
Exported Symbols (0)		
Exceptions (0)		
Relocations (5230)		
···· Certificates (0)		
Thread Local Storage (n/a)		
🗆 Resources (1)		
🗆 Strings (89/2211)		
🗗 Debug (RSDS)		

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.

2014.06.24 18:3	3:33: pid:0 START					
2014.06.24 18:3	3:51: \Device\Hard	diskVolume1\Documents	and	Settings\Administrator\Desktop\pos.exe	pid:1500	N/FCAAA C^1207101117
2014.06.24 18:3	3:51: \Device\Hard	diskVolume1\Documents	and	Settings\Administrator\Desktop\pos.exe	pid:1500	AAE/CFABA^1107101133
2014.06.24 18:3	3:51: \Device\Hard	diskVolume1\Documents	and	Settings\Administrator\Desktop\pos.exe	pid:1500	10000000000000000000000
2014.06.24 18:3	3:51: \Device\Hard	diskVolume1\Documents	and	Settings\Administrator\Desktop\pos.exe	pid:1500	A ^1100101:
2014.06.24 18:3	3:51: \Device\Hard	diskVolume1\Documents	and	Settings\Administrator\Desktop\pos.exe	pid:1500	A^120110100000000000
2014.06.24 18:3	3:51: \Device\Hard	diskVolume1\Documents	and	Settings\Administrator\Desktop\pos.exe	pid:1500	ACABB/F F^1202101100
2014.06.24 18:3	3:51: \Device\Hard	diskVolume1\Documents	and	Settings\Administrator\Desktop\pos.exe	pid:1500	^111210112321000000
2014.06.24 18:3	3:51: \Device\Hard	diskVolume1\Documents	and	Settings\Administrator\Desktop\pos.exe	pid:1500	CF/AAACAA^1312101000
014.06.24 18:3	3:51: \Device\Hard	diskVolume1\Documents	and	Settings\Administrator\Desktop\pos.exe	pid:1500	^120110113025110000
014.06.24 18:3	3:51: \Device\Hard	diskVolume1\Documents	and	Settings\Administrator\Desktop\pos.exe	pid:1500	^110210100000000000
014.06.24 18:3	3:51: \Device\Hard	diskVolume1\Documents	and	Settings\Administrator\Desktop\pos.exe	pid:1500	A^120510100000000000
014.06.24 18:3	3:51: \Device\Hard	diskVolume1\Documents	and	Settings\Administrator\Desktop\pos.exe	pid:1500	CAACA C ^12
014.06.24 18:3	3:51: \Device\Hard	diskVolume1\Documents	and	Settings\Administrator\Desktop\pos.exe	pid:1500	^121110112250000000
014.06.24 18:3	3:51: \Device\Hard	diskVolume1\Documents	and	Settings\Administrator\Desktop\pos.exe	pid:1500	00000000000000000000000
014.06.24 18:3	3:51: \Device\Hard	diskVolume1\Documents	and	Settings\Administrator\Desktop\pos.exe	pid:1500	E^120110131321000000
014.06.24 18:3	3:51: \Device\Hard	diskVolume1\Documents	and	Settings\Administrator\Desktop\pos.exe	pid:1500	B^110110100333000000
				Settings\Administrator\Desktop\pos.exe		
C 00 00 10.0	0.F4. \ D \ II	22 - 147 - 1 1 \ Pi		·····		3/300330301107101100

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). whele 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 <u>Live Response Collection</u> using <u>SysInternals autorunsc</u> 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	7ae0b9d460f1e5ddad90b668720ae9ed4d8214425af23081faa701bf4eee95250f340ee	efd98778819dada62b0820be0bab8d05f4acb04bac064b65db15a465a	
CRC32	739D4F70		
SSDEEP	6144:5GM9f8BHPImg2XR2j0mYHLptiVK0LZV3C5:5x98HPImg6R2j0mYF4VRLZtq		
YARA	shellcode - Matched shellcode byte patterns		
	Download You need to login		
Signatures			
File has been id	entified 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 whelp 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".

Web Maps Shopping Images News More - Search tools About 83 results (0.12 seconds) C86327222d873fb4e12900a5cadcb849 - Malwr - Malware https://malwr.com//YWMxNWNhMjc1ZjZINGM5Mml5Y2VmNzgxM + Nov 9, 2013 - File Size, 302592 bytes. File Type, PE32 executable (console) Intel 80386, for MS Windows. MD5, c86327222d873fb4e12900a5cadcb849. wnhelp.exe md5: c86327222d873fb4e12900a5cadcb849 greatissoftware.com/scan/c8/wnhelp-exe.shtml * EXE = C86327222D873FB4E12900A5CADCB849. WNHELP.EXE size is 302592 bytes. Full path on a computer: %SYSTEM%/WHHELP.EXE. Related Files:. malicious c86327222d873fb4e12900a5cadcb849.exe malicious c86327222d873fb4e12900a5cadcb849.exe malicious c86327722d873fb4e12900a5cadcb849.exe Malware scan of wnhelp.exe - 1 https://www.hybrid-analysis.com//088f40a7a52635ff19e80c62883977d9 malicious c86327222d873fb4e12900a5cadcb849.exe Trojan.Generic. Last analysis on March 4th 2015 14:06:04 CET with target system Windows 7 64 bit Malware scan of wnhelp.exe herdProtect www.herdproted.com/wnhelp.exe has been detected as malware by 40 anti-virus scanners. File name: wnhelp.exe has been detected as malware by 40 anti-virus scanners. File name: wnhelp.exe. MD5: c86327222d873fb4e12900a5cadcb849.	Google	c8632	7222d87	3fb4e12900a	5cadcb849)			Ŷ	٩
c86327222d873fb4e12900a5cadcb849 - Malwr - Malware https://malwr.com//YWMxNWNhMjc1ZjZINGM5Mml5Y2VmNzgxM * Nov 9, 2013 - File Size, 302592 bytes. File Type, PE32 executable (console) Intel 80386, for MS Windows. MD5, c86327222d873fb4e12900a5cadcb849. wnhelp.exe md5: c86327222d873fb4e12900a5cadcb849 greatissoftware.com/scan/c8/wnhelp-exe.shtml * EXE = C86327222D873FB4E12900A5CADCB849. WNHELP.EXE size is 302592 bytes. Full path on a computer: %SYSTEM%WNHELP.EXE. Related Files:. malicious c866327222d873fb4e12900a5cadcb849.exe https://www.hybrid-analysis.com//088f40a7a52635ff19e80c62883977d9 malicious c86327222d873fb4e12900a5cadcb849.exe https://www.hybrid-analysis.com//088f40a7a52635ff19e80c62883977d9 malicious c86327222d873fb4e12900a5cadcb849.exe. Trojan.Generic. Last analysis on March 4th 2015 14:06:04 CET with target system Windows 7 64 bit Malware scan of wnhelp.exe herdProtect www.herdprotect.com/wnhelp.exe -b1983db46e0cb4687e4c55b64c4d8d * The executable wnhelp.exe has been detected as malware by 40 anti-virus scanners.		Web	Maps	Shopping	Images	News	More -	Search tools		
https://malwr.com//YWMxNWNhMjc1ZjZINGM5MmI5Y2VmNzgxM • Nov 9, 2013 - File Size, 302592 bytes. File Type, PE32 executable (console) Intel 80386, for MS Windows. MD5, c86327222d873fb4e12900a5cadcb849. wnhelp.exe md5: c86327222d873fb4e12900a5cadcb849 greatissoftware.com/scan/c8/wnhelp.exe.shtml • EXE = C86327222D873FB4E12900A5CADCB849. WNHELP.EXE size is 302592 bytes. Full path on a computer: %SYSTEM%WNHELP.EXE. Related Files:. malicious c86327222d873fb4e12900a5cadcb849.exe https://www.hybrid-analysis.com//088f40a7a52635ff19e80c62883977d9 malicious c86327222d873fb4e12900a5cadcb849.exe. Trojan.Generic. Last analysis on March 4th 2015 14:06:04 CET with target system Windows 7 64 bit Malware scan of wnhelp.exe herdProtect www.herdprotect.com/wnhelp.exe has been detected as malware by 40 anti-virus scanners.		About 8	3 results (0.12 seconds)						
greatissoftware.com/scan/c8/wnhelp-exe.shtml * EXE = C86327222D873FB4E12900A5CADCB849. WNHELP.EXE size is 302592 bytes. Full path on a computer: %SYSTEM%WNHELP.EXE. Related Files:. malicious c86327222d873fb4e12900a5cadcb849.exe https://www.hybrid-analysis.com//088f40a7a52635ff19e80c62883977d9 malicious c86327222d873fb4e12900a5cadcb849.exe. Trojan.Generic. Last analysis on March 4th 2015 14:06:04 CET with target system Windows 7 64 bit Malware scan of wnhelp.exe herdProtect www.herdprotect.com/wnhelp.exe-b1983db46e0cb4687e4c55b64c4d8d * The executable wnhelp.exe has been detected as malware by 40 anti-virus scanners.		https:// Nov 9, 2	malwr.con 2013 - File	N/YWMxNW Size, 302592 k	NhMjc1ZjZIN oytes. File Ty	NGM5Mml pe, PE32 e	SY2VmNzgx xecutable (c	M onsole) Intel		
https://www.hybrid-analysis.com//088f40a7a52635ff19e80c62883977d9 malicious c86327222d873fb4e12900a5cadcb849.exe. Trojan.Generic. Last analysis on March 4th 2015 14:06:04 CET with target system Windows 7 64 bit Malware scan of wnhelp.exe herdProtect www.herdprotect.com/wnhelp.exe-b1983db46e0cb4687e4c55b64c4d8d ~ The executable wnhelp.exe has been detected as malware by 40 anti-virus scanners.		greatis: EXE = 0	software.c C86327222	om/scan/c8/wr 2D873FB4E129	help-exe.sh 900A5CADCE	tml • 3849. WNH	ELP.EXE siz	te is 302592		
www.herdprotect.com/wnhelp.exe-b1983db46e0cb4687e4c55b64c4d8d The executable wnhelp.exe has been detected as malware by 40 anti-virus scanners.		https:// malicio	www.hybri us c86327	id-analysis.con 222d873fb4e1	n//088f40a 2900a5cado	7a52635ff b849.exe.	19e80c6288 Trojan.Gene	33977d9 eric. Last		
		www.he The exe	erdprotect. ecutable w	.com/wnhelp.e	xe-b1983db	46e0cb468 d as malwa	7e4c55b64d ire by 40 and	ti-virus scanners.		
Results for 69.89.31.110 - scumware.org - Just another free www.scumware.org/report/69.89.31.110 ▼ 2014-02-16 00:15:58, http://www.e-swipe.org/nan.exe, C86327222D873FB4E12900A5CADCB849, 69.89.31.110, US, Win32/Agent.UVD trojan. 2013-12-01		2014-0 C86327	cumware.o 2-16 00:15 7222D873F	org/report/69.8 58, http://www. B4E12900A50	9.31.110 • e-swipe.org/r	nan.exe,				
What is wnhelp.exe ? System Explorer systemexplorer.net/file-database/file/wnhelp-exe/7912390 * Apr 4, 2012 Version: (Empty Value); MD5: c863272224873fb4e12900a5cadcb849; SHA1: b1983db46e0cb4687e4c55b64c4d8d53551877fa; SHA256:		System Apr 4, 2 c86327	explorer.n 2 <mark>012 -</mark> Ve 222d873f	et/file-databas ersion: (Empty) b4e12900a5ca	e/file/wnhelp Value); MD5: dcb849; SH/	-exe/7912 A1:				
b1983db46e0cb4687e4c55b64c4d8d53551877fa Analysis totalhash.com/analysis/b1983db46e0cb4687e4c55b64c4d8d53551877fa Analysis Date, 2015-01-27 23:39:51. MD5, c86327222d873fb4e12900a5cadcb849. SHA1, b1983db46e0cb4687e4c55b64c4d8d53551877fa		totalha Analysi	sh.com/an s Date, 201	alysis/b1983dl 15-01-27 23:39	46e0cb468	7e4c55b64 6327222d	c4d8d5355 373fb4e129	1877fa 🝷		
Antivirus scan for VirusTotal https://www.virustotal.com/latest-report.html?c86327222d8 VirusTotal VirusTotal's antivirus scan report for the file with MD5 c86327222d873fb4e12900a5cadcb849 at 2015-02-05 05:09:55 UTC. 43 out of 56 antivirus detected the		https:// VirusTo c86327	www.virus otal's antivit 222d873f	total.com/lates rus scan report b4e12900a5ca	st-report.htm for the file wi	th MD5				

systemexplorer.net query of wnhelp from 2012

UPDATE (March 6, 2015): As <u>@maldr0id</u> pointed out, the wnhelp file was submitted to <u>virustotal back on October 2, 2012</u>, 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 <u>virustotal on February 16, 2011</u>. At that time it had a 0/43 detection ratio.

	rus	total		
SHA256:	088f40a7a	a52635ff19e80c62883	977d94dd5835e85739e19504f7437d296760b	
File name:	r12.exe			1 1 1 1 1 1 1 1 1 1
Detection ra	atio: 3 / 42			🕑 5 🕚 0
Analysis da	te: 2012-10-0	02 14:08:51 UTC (2 y	ears, 5 months ago) View latest	
Analysis	Q File detail	ズ Relationships	Additional information Comments 2	© Votes
ntivirus			Result	Update
omodo			TrojWare.Win32.Trojan.Agent.Gen	20121002
ophos			Mal/Generic-L	20121002
			TROJ GEN.R15H1J1	

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

SHA256:	088f40a7	a52635ff19e80c62883	977d94dd5835e85739e19504	lf7437d296760b		
File name:	wnhelp.e	xe				1 ()
Detection r	ratio: 0 / 43					🕑 5 💽 0
Analysis d	ate: 2011-02-	16 14:11:57 UTC (4 y	ears ago) View latest			
		ズ Relationships	6 Additional information	Comments	Votes	
Analysis	Q File detail	A Relationships	• Additional Information	Comments 2	Voles	
2	C File detail	A Relationships	Result	Upd	•	
ntivirus		A Relationships	-	Upd	•	
Analysis		A Relationships	Result	Upd 201:	ate	

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 redirected it to "fbi.gov" (my own way of "getting back" at bad actors). If you are interested please feel free to <u>contact me</u>, 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).