malware-analysis-writeups/Conficker/Conficker.md at main · itaymigdal/malware-analysis-writeups

By itaymigdal

Archived: 2026-04-05 14:01:15 UTC

Malware Name	File Type	SHA256
Conficker	x32 dll	a30b63e1ed900d3f223277b1d3b09b045abc85600da0d3102fa61fb2bfc2ff99

Intro

Almost 15 years old ago, a worm named Conficker did a LOT of trouble. to this day, there are some Windows environments (mainly XP based networks) which are still infected with this piece of code (brilliant code for 2008). With millions of infections all over the world, 5 variations, and a lot of damage, some say this is the most remarkable worm that was ever made.
So i took it for a ride in my lab.

Analysis process

I first encountered that worm when i received a Disk On Key with an `autorun.inf` file and weird file with suspicious extension `jwgkvsq.vmx` which both were super infected in AV engines. Any time an infected DOK inserted into a computer, it pops up this window:

This is a very nice social engineering trick, the `autorun.inf` is disguised as the explorer icon and caption (look at the duplicated explorer actions, one under "Install or run a program" - which invoking the `autorun.inf`, and the other under "General options" - the benigh one). Observing the autorun file:

We see a lot of shity unclear randomness which not clear if this is obfuscation or a binary. By scrolling down (how down? line 1227) some few strings are exposed inside this sea of garbage:

Cleaning it up:

```
icon = %syStEmrOot%\sySTEM32\sHELL32.Dll,4

shellExECUte = RuNdLl32.EXE .\RECYCLER\S-5-3-42-2819952290-8240758988-879315005-3665\jwgkvsq.vmx,ahaezedrn

useAuTopLAY = 1
```

The first line bind the `autorun.inf` to explorer icon. The second line executes the other file using Rundll32.exe which invokes a gibberish export function (actually, this method isn't even exist in `jwgkvsq.vmx` dll. before validating the export name - DllMain is called).

Opening `jwgkvsq.vmx` in Pestudio:

property	value	value	value
name	UPX0	UPX1	UPX2
md5	n/a	89FFC709E081FAB549538498...	1F48A96EFFAE875C9C674C8...
entropy	n/a	7.787	3.663
file-ratio (52.76%)	n/a	52.45 %	0.31 %
raw-address	0x00000400	0x00000400	0x00015200
raw-size (86016 bytes)	0x00000000 (0 bytes)	0x00014E00 (85504 bytes)	0x00000200 (512 bytes)
virtual-address	0x10001000	0x10006000	0x1001B000
virtual-size (110592 bytes)	0x00005000 (20480 bytes)	0x00015000 (86016 bytes)	0x00001000 (4096 bytes)
entry-point	-	0x0001ABC0	-
writable	x	x	x
executable	x	x	-
shareable	-	-	-
discardable	-	-	-
initialized-data	-	x	x
uninitialized-data	x	-	-
readable	x	x	x
self-modifying	x	x	-
blacklisted	x	x	x
virtualized	x	-	-

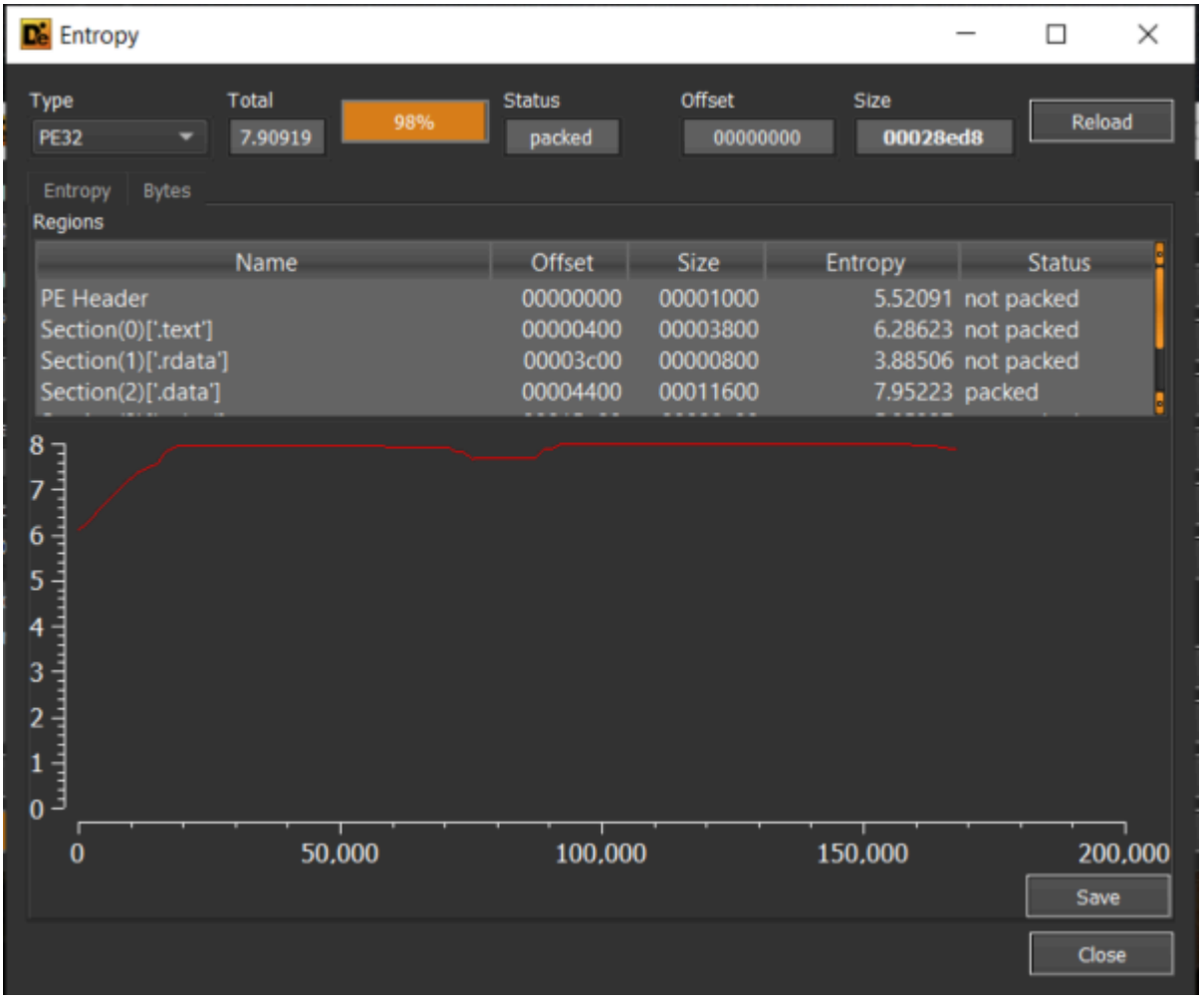
First stage is packed by UPX. unpacking:

```
PS C:\Windows\system32> upx.exe -d C:\Users\IEUser\Desktop\jwgkvsq.vmx -o C:\Users\IEUser\Desktop\confi_unpacked.dll
                       Ultimate Packer for eXecutables
                          Copyright (C) 1996 - 2020
UPX 3.96w       Markus Oberhumer, Laszlo Molnar & John Reiser   Jan 23rd 2020

        File size         Ratio      Format      Name
   --------------------   ------   -----------   -----------
    167640 <-    163032   97.25%    win32/pe     confi_unpacked.dll

Unpacked 1 file.
PS C:\Windows\system32>
```

For my convenience, here i converted the dll to exe (the tool just changed a single bit in PE header):

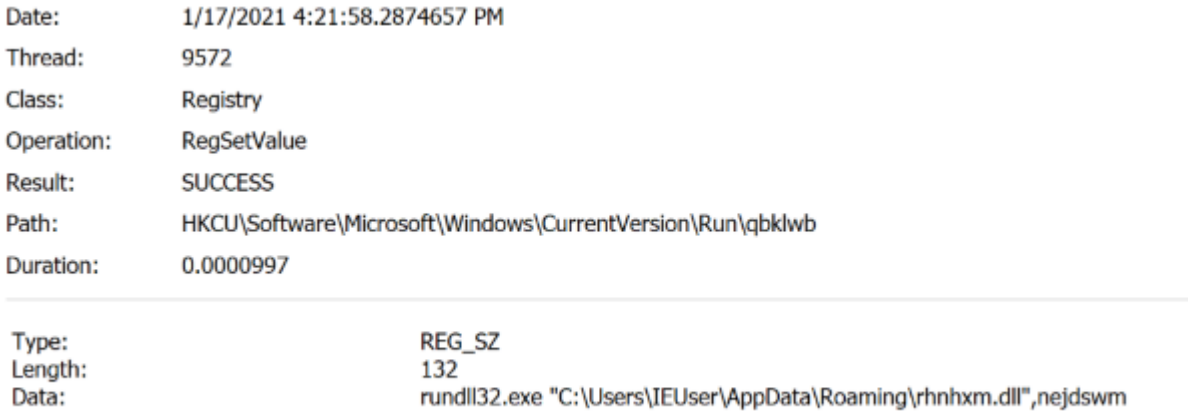
```
PS C:\Users\IEUser\Desktop> .\dll_to_exe.exe
DLL to EXE converter v1.1
- for 32 & 64 bit DLLs -
args: <input_dll> <output_exe>
Press any key to continue . . .
PS C:\Users\IEUser\Desktop> .\dll_to_exe.exe .\confi_unpacked.dll confi.exe
[OK] Converted successfuly.
[OK] Module dumped to: confi.exe
PS C:\Users\IEUser\Desktop>
```

Entropy is 8 so the file is still packed:



We will try to unpack it later, for now let's run the file under Procmon to get a general idea of the file operations. The file is very noisy and many operation were seen.

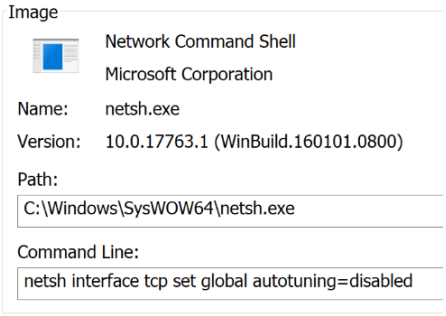
The file persists itself in a run key:



Deletes Windows Defender from run key:

Date:	1/17/2021 4:22:18.8731549 PM
Thread:	9572
Class:	Registry
Operation:	RegDeleteValue
Result:	ACCESS DENIED
Path:	HKLM\SOFTWARE\WOW6432Node\Microsoft\Windows\CurrentVersion\Run\Windows Defender
Duration:	0.0000348

Resets the TCP receive window using Netsh.exe (not sure exactly why, but it's part of the setup for the upcoming Brute Force).



Probes for live hosts in the internal network by trying to connect to their SMB share:

4:22:55...	confi.exe	2360 TCP Reconnect	10.0.2.15:50669 -> 10.0.2.1:445
4:22:56...	confi.exe	2360 TCP Disconnect	10.0.2.15:50669 -> 10.0.2.1:445
4:22:56...	confi.exe	2360 TCP Connect	10.0.2.15:50674 -> 10.0.2.2:445
4:22:56...	confi.exe	2360 TCP Send	10.0.2.15:50674 -> 10.0.2.2:445
4:22:56...	confi.exe	2360 TCP Disconnect	10.0.2.15:50674 -> 10.0.2.2:445
4:22:56...	confi.exe	2360 TCP Connect	10.0.2.15:50675 -> 10.0.2.3:445
4:22:56...	confi.exe	2360 TCP Send	10.0.2.15:50675 -> 10.0.2.3:445
4:22:56...	confi.exe	2360 TCP Disconnect	10.0.2.15:50675 -> 10.0.2.3:445
4:22:56...	confi.exe	2360 TCP Connect	10.0.2.15:50676 -> 10.0.2.4:445
4:22:56...	confi.exe	2360 TCP Send	10.0.2.15:50676 -> 10.0.2.4:445
4:22:56...	confi.exe	2360 TCP Disconnect	10.0.2.15:50676 -> 10.0.2.4:445
4:23:00...	confi.exe	2360 TCP Reconnect	10.0.2.15:50677 -> 10.0.2.5:445
4:23:01...	confi.exe	2360 TCP Disconnect	10.0.2.15:50677 -> 10.0.2.5:445
4:23:04...	confi.exe	2360 TCP Reconnect	10.0.2.15:50678 -> 10.0.2.6:445
4:23:05...	confi.exe	2360 TCP Disconnect	10.0.2.15:50678 -> 10.0.2.6:445
4:23:08...	confi.exe	2360 TCP Reconnect	10.0.2.15:50679 -> 10.0.2.7:445
4:23:09...	confi.exe	2360 TCP Disconnect	10.0.2.15:50679 -> 10.0.2.7:445

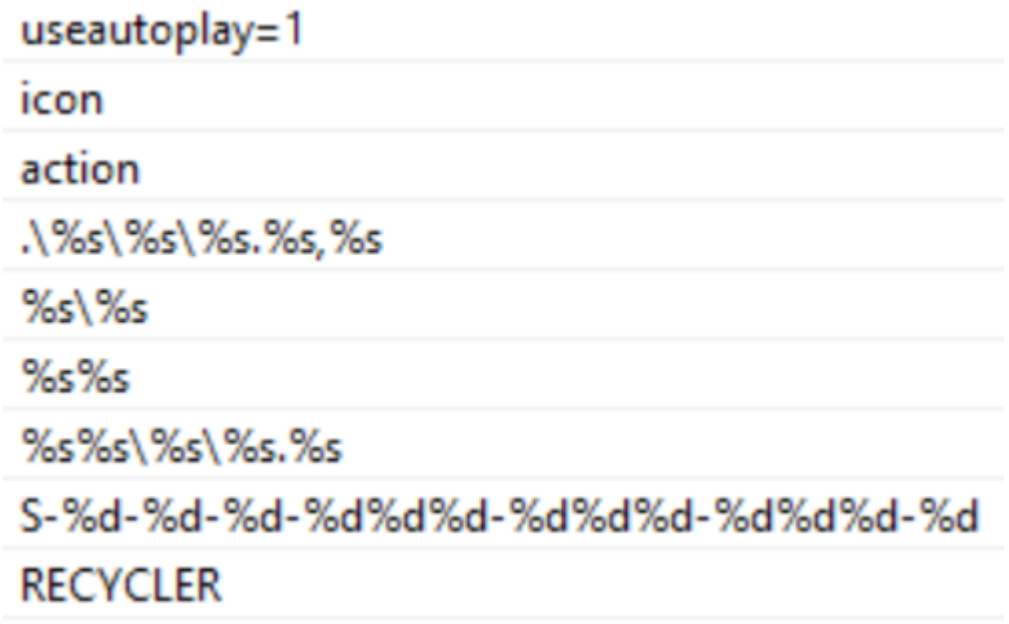
In this part i started to debug the file under debugger in order to unpack it. Even though this is an old malware and fair to think that it is lacking protections, it's not true. it contains polymorphism, obfuscation and anti-analysis tricks. after some struggling with it and at least 5 `VirtualAlloc`, I saw a PE file that was written to a newly allocated memory:

confi_unpacked_02C50000.bin

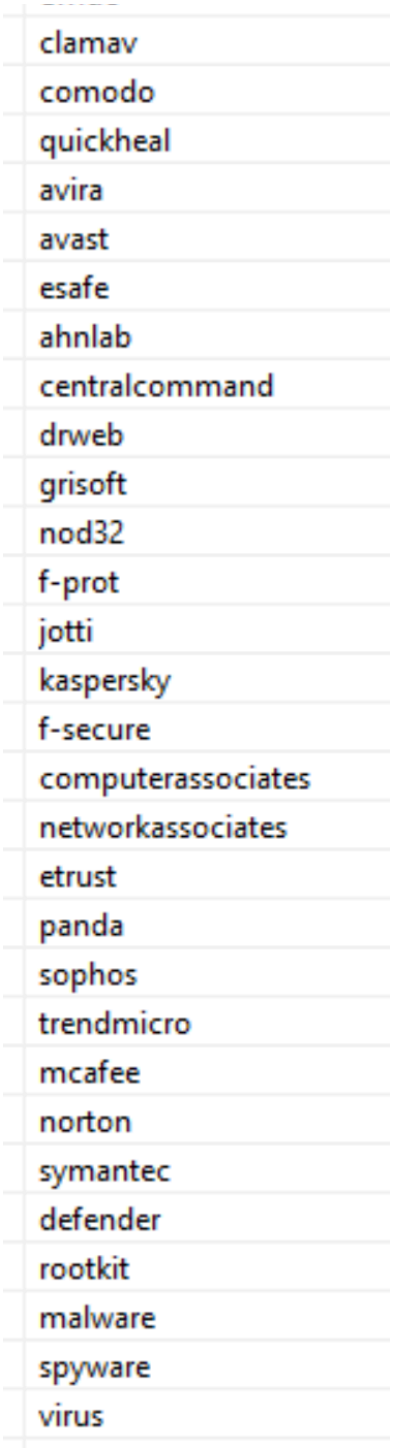
Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00001570	75	72	72	65	6E	74	56	65	72	73	69	6F	6E	5C	52	75	urrentVersion\Ru
00001580	6E	00	00	00	57	69	6E	64	6F	77	73	20	44	65	66	65	n...Windows Defe
00001590	6E	64	65	72	00	00	00	00	57	69	6E	44	65	66	65	6E	nder....WinDefen
000015A0	64	00	00	00	42	49	54	53	00	00	00	00	77	75	61	75	d...BITS....wuau
000015B0	73	65	72	76	00	00	00	00	53	6F	66	74	77	61	72	65	serv....Software
000015C0	5C	4D	69	63	72	6F	73	6F	66	74	5C	57	69	6E	64	6F	\Microsoft\Windo
000015D0	77	73	5C	43	75	72	72	65	6E	74	56	65	72	73	69	6F	ws\CurrentVersio
000015E0	6E	5C	65	78	70	6C	6F	72	65	72	5C	53	68	65	6C	6C	n\explorer\Shell
000015F0	53	65	72	76	69	63	65	4F	62	6A	65	63	74	73	5C	7B	ServiceObjects\{
00001600	46	44	36	39	30	35	43	45	2D	39	35	32	46	2D	34	31	FD6905CE-952F-41
00001610	46	31	2D	39	41	36	46	2D	31	33	35	44	39	43	36	36	F1-9A6F-135D9C66
00001620	32	32	43	43	7D	00	00	00	77	73	63	73	76	63	00	00	22CC}...wscsvc..
00001630	73	76	63	68	6F	73	74	2E	65	78	65	20	2D	6B	20	4E	svchost.exe -k N
00001640	65	74	77	6F	72	6B	53	65	72	76	69	63	65	00	00	00	etworkService...
00001650	73	76	63	68	6F	73	74	2E	65	78	65	20	2D	6B	20	6E	svchost.exe -k n
00001660	65	74	73	76	63	73	00	00	73	65	72	76	69	63	65	73	etsvcs..services
00001670	2E	65	78	65	00	00	00	00	47	6C	6F	62	61	6C	5C	25	.exe....Global\%
00001680	75	2D	25	75	00	00	00	00	53	65	44	65	62	75	67	50	u-%u....SeDebugP
00001690	72	69	76	69	6C	65	67	65	00	00	00	00	00	00	00	00	rivilege........
000016A0	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ..........ÿÿ..
000016B0	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00	¸.......@.......
000016C0	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
000016D0	00	00	00	00	00	00	00	00	00	00	00	00	D0	00	00	00	............Ð...
000016E0	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..°..´.Í!¸.LÍ!Th
000016F0	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00001700	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00001710	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode....$.......
00001720	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00001730	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00001740	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00001750	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00001760	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	....
00001770	50	45	00	00	4C	01	05	00	40	47	30	37	00	00	00	00	PE..L...@G07....
00001780	00	00	00	00	E0	00	02	21	0B	01	07	00	00	06	00	00	....à..!........
00001790	00	06	00	00	00	00	00	00	B0	10	00	00	00	10	00	00	........°.......
000017A0	00	20	00	00	00	00	00	10	00	10	00	00	00	02	00	00	. ...

The file was in its mapped format (reference), and for some reason i was unable to unmap it to its raw format, trying various methods. i suspect that the reason is because the PE headers were corrupted in some way. So in some point i gave up the unmapping, and moved on to the very JUICY strings armed with my prior knowledge on Conficker actions.

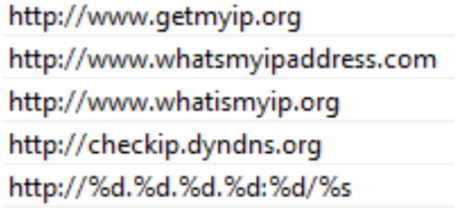
First were the `autorun.inf` strings which were written to every Disk on Key that inserted to an infected machine:



Then there are a big list of security producs and related names, which will compared against each DNS lookup the host makes, and if the DNS request contains any of these words, the request will be blocked! that is done by hooking the DNS library in every process!!



It also has the ability to retrieve the external IP address of the machine by quering each of those sites:



And there is the password list (part of it, it's longer):

super
secret
backup
manager
ihavenopass
nothing
nopassword
nopass
love123
home123
qwe123
pw123
root123
pass123
pass12
pass1
admin123
admin12
admin1
password123
password12
password1

Spreading

The worm spreads itself by 3 mechanisms:

1. By Brute Forcing SMB shares using the password list. when it guesses the right password, it writes the payload to the remote share and runs it by creating a remote service.
2. By Infecting DOKs and removable drives.
3. By ms08-067, which is being exploited heavily by it. for that, the worm creates a local HTTP server on the infected machine, which serves the payload for any host that is exploited successfuly.

More capabilities which not discussed

1. The worm contains a DGA algorithm (explained here).
2. The worm changes TCP settings, like the allowed current TCP connections, in order to optimize the Brute Force process.
3. The worm shuts down system services, like `Windows Defender` and `Background Intelligent Transfer Service` to disrupt automatic updates and protections.
4. The worm injects itself to system services like `Explorer.exe` and `Svchost.exe`.
5. The worm deletes the System Restore Points.
6. The worm contains anti-analysis, anti-sandbox and anti-vm capabilities, and a lot of obfuscation and "spaghetti code".

Conclusion

Conficker is a sophisticated, contagious, brutal and noisy Windows worm. In this writeup i discussed only a small part of Conficker whole story, there is a comprehensive article about it as well.

Hope you enjoyed :)

Source: https://github.com/itaymigdal/malware-analysis-writeups/blob/main/Conficker/Conficker.md