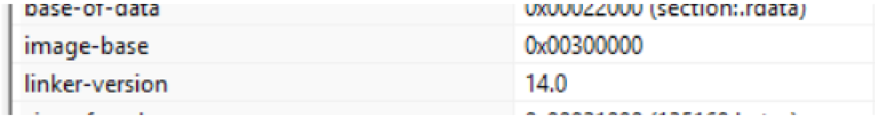
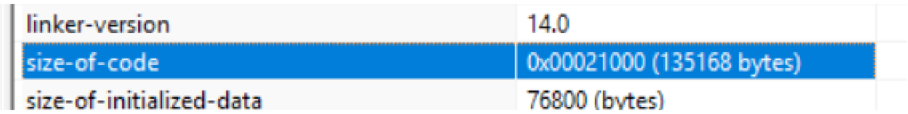
1. 0x00300000. The normal image base is 0x00400000.



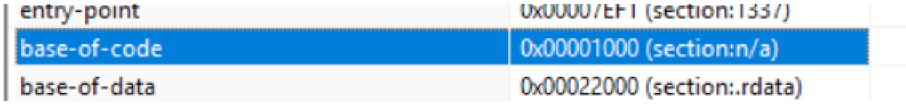
base-of-data	0x00022000 (section:.rdata)
image-base	0x00300000
linker-version	14.0
size-of-code	0x00021000 (135168 bytes)

2. 135168 bytes



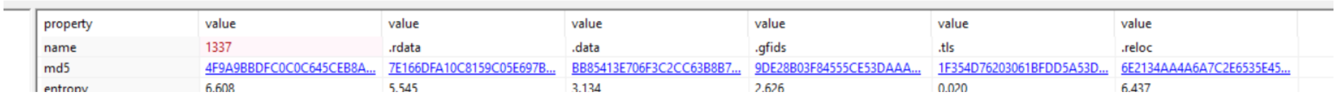
linker-version	14.0
size-of-code	0x00021000 (135168 bytes)
size-of-initialized-data	76800 (bytes)

3. 0x00001000   PE Studio cannot tell what section it is in. This is likely because it is in section 1337 which is not standard.



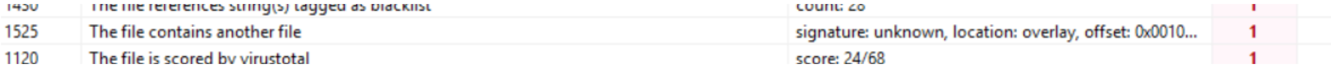
entry-point	0x00007EF1 (section:1337)
base-of-code	0x00001000 (section:n/a)
base-of-data	0x00022000 (section:.rdata)

4. 1337, .rdata, .data, .tls, .reloc. 1337 is not a normal section

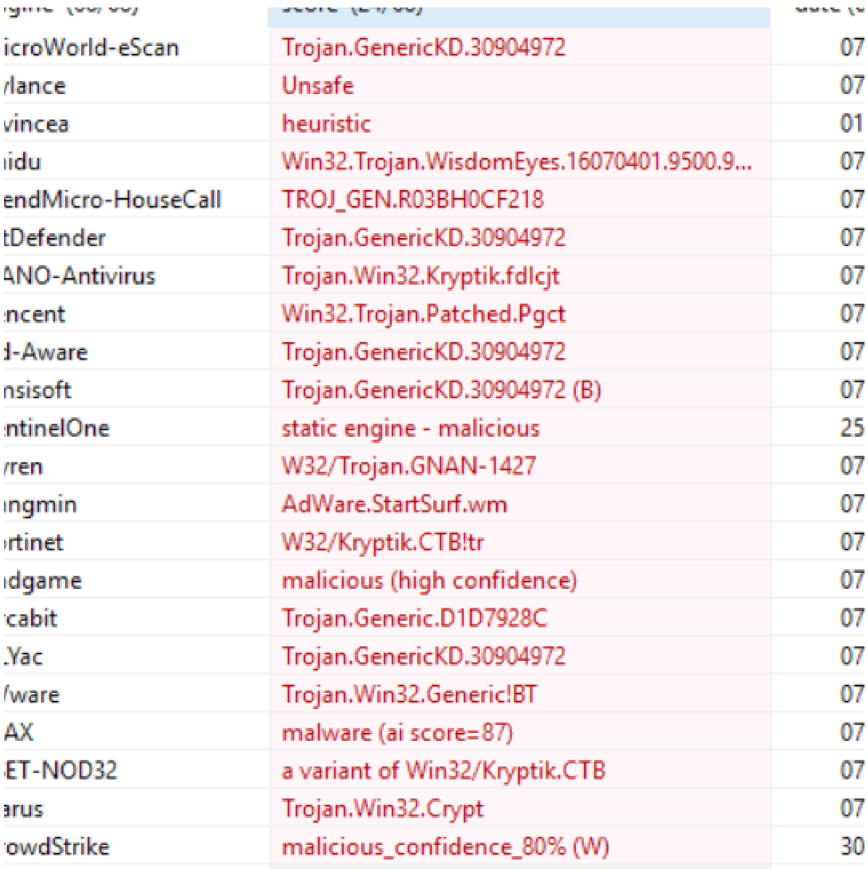


property	value	value	value	value	value	value
name	1337	.rdata	.data	.gfids	.tls	.reloc
md5	4F9A9BBDFC0C0C645CEB8A...	7E166DFA10C8159C05E697B...	BB85413E706F3C2CC63B8B7...	9DE28B03F84555CE53DAAA...	1F354D76203061BFDD5A53D...	6E2134AA4A6A7C2E6535E45...
entropy	6.608	5.545	3.134	2.626	0.020	6.437

5. It is some sort of Trojan. When it is run, it drops malicious code into the computer. Virus Total picks up several signatures that indicate that it is a trojan. There is also a file embedded into the main file.



1430	The file references string(s) tagged as blacklist	count: 28	1
1525	The file contains another file	signature: unknown, location: overlay, offset: 0x0010...	1
1120	The file is scored by virustotal	score: 24/68	1



gine (66/66)	score (24/66)	date (u
icroWorld-eScan	Trojan.GenericKD.30904972	07
ylance	Unsafe	07
vincea	heuristic	01
idu	Win32.Trojan.WisdomEyes.16070401.9500.9...	07
endMicro-HouseCall	TROJ_GEN.R03BH0CF218	07
tDefender	Trojan.GenericKD.30904972	07
ANO-Antivirus	Trojan.Win32.Kryptik.fdlcjt	07
ncent	Win32.Trojan.Patched.Pgct	07
d-Aware	Trojan.GenericKD.30904972	07
nsisoft	Trojan.GenericKD.30904972 (B)	07
ntinelOne	static engine - malicious	25
yren	W32/Trojan.GNAN-1427	07
ngmin	AdWare.StartSurf.wm	07
rtinet	W32/Kryptik.CTB!tr	07
dgame	malicious (high confidence)	07
cabit	Trojan.Generic.D1D7928C	07
.Yac	Trojan.GenericKD.30904972	07
'ware	Trojan.Win32.Generic!BT	07
AX	malware (ai score=87)	07
ET-NOD32	a variant of Win32/Kryptik.CTB	07
arus	Trojan.Win32.Crypt	07
owdStrike	malicious_confidence_80% (W)	30