63d3fbc397585a45b01b456aab953abb

1.

name (4)	type (1)	ordinal (0)	blacklist (1)
LoadLibraryA	implicit	-	-
ExitProcess	implicit	-	-
GetProcAddress	implicit	-	-
VirtualProtect	implicit	-	x

There are very few imports which is very suspicious. Also the VirtualProtect function is used to change the read write permissions of a page.

2. All of the string except for the imports and the “this program cannot be run in dos mode” string are gibberish.

3. It is writable, executable, and self modifying. PE studio also flags the entry point as suspicious. In addition to this, the sections are labeled as UPX. This is a packer.

property	value	value	value
name	UPX0	UPX1	UPX2
md5	n/a	1A2DE04069B42921EF120157...	CDC4D9477CFA0AEFF70C71...
entropy	n/a	7.900	1.724
file-ratio (98.10%)	n/a	97.14 %	0.95 %
raw-address	0x00000400	0x00000400	0x0000D000
raw-size (52736 bytes)	0x00000000 (0 bytes)	0x0000CC00 (52224 bytes)	0x00000200 (512 bytes)
virtual-address	0x00401000	0x00412000	0x0041F000
virtual-size (126976 bytes)	0x00011000 (69632 bytes)	0x0000D000 (53248 bytes)	0x00001000 (4096 bytes)
entry-point	-	0x0001E860	-
writable	x	x	x
executable	x	x	-
shareable	-	-	-
discardable	-	-	-
initialized-data	-	x	x
uninitialized-data	x	-	-
unreadable	-	-	-
self-modifying	x	x	-
virtualized	x	-	-
file	n/a	n/a	n/a

4. This sample is packed. Most of the strings are unreadable, it has self modifying sections, and the entry point is suspicious, and the sections names indicate UPX, a known packer.

F55663305088f33b013c5a86bc9520a6

1.

There are many imports visible so it is unlikely that the file is packed.

2. There are many strings that are readable. So it is unlikely that the entire sample is packed. There is however an area that has high entropy. This program is likely a Trojan that is carrying an encrypted file.

3. The sections table is much more typical in this sample. The section names and entry point are all normal.

4. The overall program is not packed, but there is definitely an encrypted or compressed file inside of of the program. This is because the program has a typical sections table and readable strings.

69f27b07404cf9c51dd2d2e40fca4d65

1. This file is likely packed. The file has atypical sections that are blacklisted.

The executable contains unknown PE section names indicative of a packer (could be a false positive) (7 events)	
section	.t22112
section	.t2211
section	.t221
section	.t22
section	.t21
section	.t2
section	.rdat

It also allocates read-write-executable memory. This is often used to unpack itself.

Allocates read-write-execute memory (usually to unpack itself) (22 events)

Time & API	Arguments	Status	Return	Repeated
NtAllocateVirtualMemory Nov. 10, 2020, 12:23 a.m.	process_identifier: 2600 region_size: 552960 stack_dep_bypass: 0 stack_pivoted: 0 heap_dep_bypass: 0 protection: 64 (PAGE_EXECUTE_READWRITE) base_address: 0x01cf0000 allocation_type: 12288 (MEM_COMMIT|MEM_RESERVE) process_handle: 0xffffffff	1	0	0

In addition to this all of the strings are unreadable.