

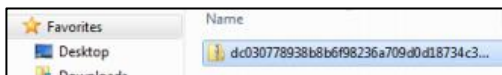
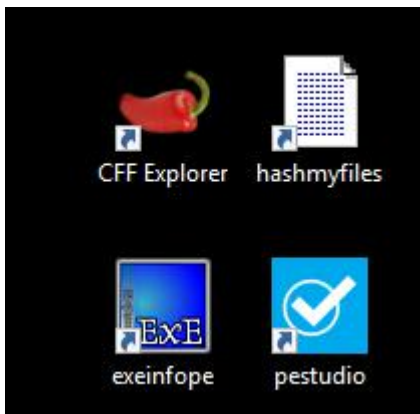
DIGITAL FORENSICS II

Experiment 10

Submitted to: Mr. Keshav Kaushik
Submitted by: Kashish Srivastava
500067405
R134218079

Aim: Pony Malware Analysis

We are going to perform static malware analysis using exeinfo PE



As we know the first step in Static analysis will be the **File type identification**, we will be doing this with a couple of tools, named as HxD, Exeinfo PE.

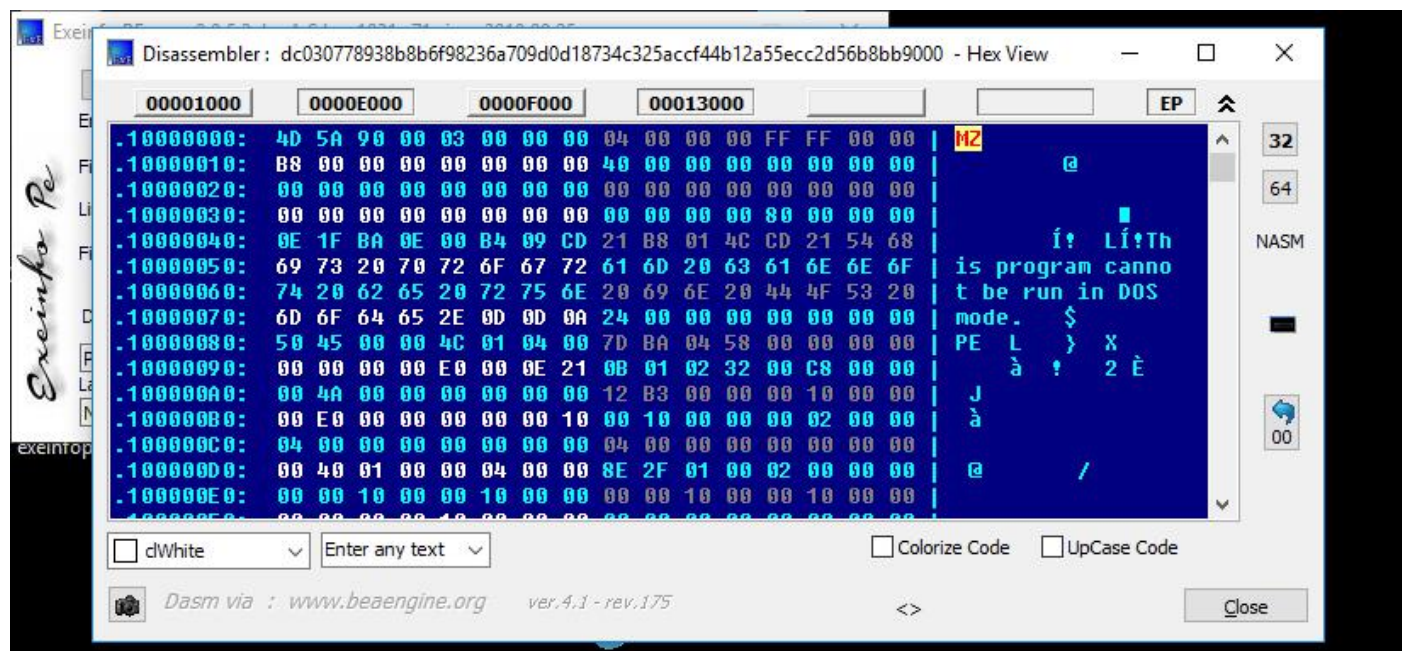
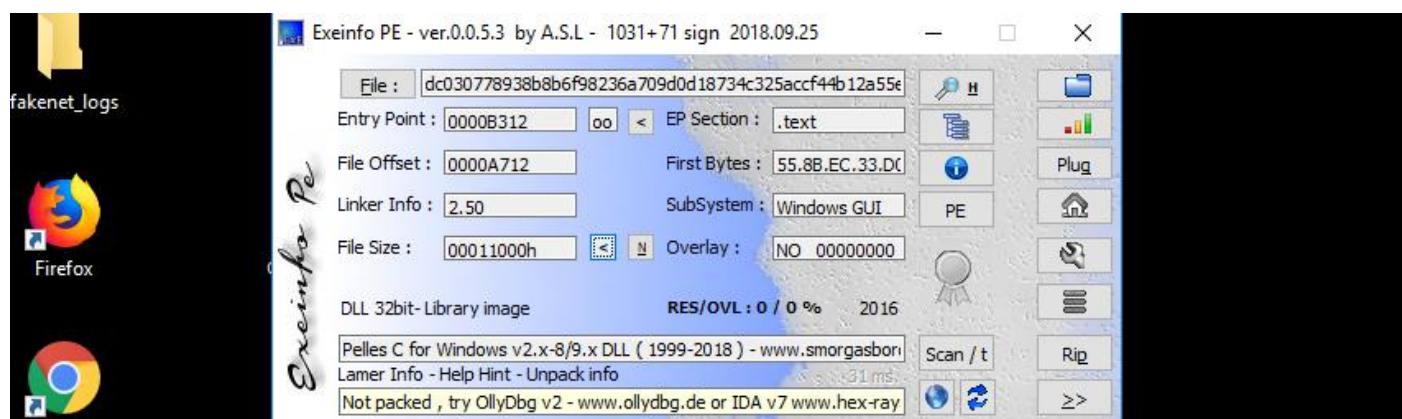
In this method we will be analysing the sample malware without executing or running it, we will be analysing the file in static condition, Extract as much of Data like strings, PE headers, etc.

1. Identifying File type
2. Generating Hash
3. Strings
4. Packing & obfuscation
5. PEHeaders

Offset(h)	00	01	02	03	04	05	06	07	08	09	0A	0B	0C	0D	0E	0F	Decoded text
00000000	4D	5A	90	00	03	00	00	00	04	00	00	00	FF	FF	00	00	MZ.....ÿÿ..
00000010	B8	00	00	00	00	00	00	00	40	00	00	00	00	00	00	00@.....
00000020	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000030	00	00	00	00	00	00	00	00	00	00	00	00	80	00	00	00€...
00000040	0E	1F	BA	0E	00	B4	09	CD	21	B8	01	4C	CD	21	54	68	..°.!.Li!Th
00000050	69	73	20	70	72	6F	67	72	61	6D	20	63	61	6E	6E	6F	is program canno
00000060	74	20	62	65	20	72	75	6E	20	69	6E	20	44	4F	53	20	t be run in DOS
00000070	6D	6F	64	65	2E	0D	0D	0A	24	00	00	00	00	00	00	00	mode...\$.
00000080	50	45	00	00	4C	01	04	00	7D	BA	04	58	00	00	00	00	PE..L...}°.X...
00000090	00	00	00	00	E0	00	0E	21	0B	01	02	32	00	C8	00	00	...ä...!...2.È...
000000A0	00	4A	00	00	00	00	00	00	12	B3	00	00	00	10	00	00	..J.....'.....
000000B0	00	E0	00	00	00	00	00	10	00	10	00	00	00	02	00	00	..à.....
000000C0	04	00	00	00	00	00	00	00	04	00	00	00	00	00	00	00
000000D0	00	40	01	00	00	04	00	00	8E	2F	01	00	02	00	00	00	..@.....ž/.....
000000E0	00	00	10	00	00	10	00	00	00	10	00	00	10	00	00	00
000000F0	00	00	00	00	10	00	00	00	00	00	00	00	00	00	00	00
00000100	C4	1D	01	00	C8	00	00	00	00	00	00	00	00	00	00	00	Ä...È.....
00000110	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000120	00	30	01	00	7C	08	00	00	00	00	00	00	00	00	00	00	..0..
00000130	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000140	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00	00
00000150	00	00	00	00	00	00	00	00	14	20	01	00	88	01	00	00

Data inspector	
Binary (8 bit)	01010000
Int8	go to: 80
UInt8	go to: 80
Int16	go to: 17744
UInt16	go to: 17744
Int24	go to: Invalid
UInt24	go to: Invalid
Int32	go to: Invalid
UInt32	go to: Invalid
Int64	go to: Invalid
UInt64	go to: Invalid
AnsiChar / char8_t	P
WideChar / char16_t	瑞
UTF-8 code point	P (U+0050)
Single (float32)	Invalid
Double (float64)	Invalid
OLETIME	Invalid

Next, You can Drag the malware sample into Exeinfo PE launcher to check additional details like whether its packed or not, and we can check for the sections also,



We can use the Dis-assembler in this application too to check for the Hex Values, and PE header and the header string as we did with HxD application.

PE HEADER STRUCTURE

MZ Header/DOS Header	Executable Binary
DOS stub	Prints a message (Program cannot run in DOS mode)
PE File Heder(Signature)	Define exe as PE
Image optional Header	Important info like subsystem and entry point
Section Table	How to load the executable into memory
Sections	Executable sections of code and data

pestudio 8.96 - Malware Initial Assessment - www.winitor.com [c:\users\malware\desktop\samples\dc030778938b8b6f98236a709d0d18734c325accf44b12a55ecc2...

file help

c:\users\malware\desktop\samples\dc030778938

- indicators (6/18)
 - virustotal (warning)
- dos-header (64 bytes)
- dos-stub (64 bytes)
- file-header (Oct.2016)
 - optional-header (file-checksum)
- directories (2)
 - sections (98.53%)
- libraries (4/9)
- imports (33/89)
- exports (n/a)
- tls-callbacks (n/a)
- resources (n/a)
- strings (106/934)
- debug (n/a)
- manifest (n/a)
- version (n/a)
- certificate (n/a)
- overlay (n/a)

property	value	value	value	value
name	.text	.rdata	.data	.reloc
md5	0475EEBBDf0316A70495FCA...	62B50172BB46AC5AD3E41D...	D7A50192E6E163F3AA0F3E3...	B152A3...
file-ratio (98.53%)	73.53 %	0.74 %	20.59 %	3.68 %
file-cave (1001 bytes)	51200 bytes	512 bytes	14336 bytes	2560 by
entropy	0.000	0.000	0.000	0.000
raw-address	0x00000400	0x0000CC00	0x0000CE00	0x00001100
raw-size (68608 bytes)	0x0000C800 (51200 bytes)	0x00000200 (512 bytes)	0x00003800 (14336 bytes)	0x00000100 (256 bytes)
virtual-address	0x10001000	0x1000E000	0x1000F000	0x10010000
virtual-size (68971 bytes)	0x0000C69B (50843 bytes)	0x00000100 (256 bytes)	0x00003D54 (15700 bytes)	0x00000100 (256 bytes)
entry-point (0x0000B312)	x	-	-	-
writable	-	-	x	-
executable	x	-	-	-
shareable	-	-	-	-
discardable	-	-	-	x
initialized-data	-	x	x	x
uninitialized-data	-	-	-	-
readable	x	x	x	x
self-modifying	-	-	-	-
blacklisted	-	-	-	-
virtualized	-	-	-	-

PE SECTIONS

.code/.text	Executable code
.data	Stores data(R/W)
.rdata	Stores data (Read only)
.idata	Stores import data
.edata	Stores export data
.rsc	Stores resources(strings and icons)

Interactive malware hunting service

[General](#)
[Behavior activities](#)
[Screenshots](#)
[Process](#)
[Registry](#)
[Files](#)
[Network](#)
[Debug](#)

General Info

File name	dc030778938b8b6f98236a709d0d18734c325accf44b12a55ecc2d56b8bb9000
Full analysis	https://app.any.run/tasks/b21009dc-99dc-4082-a370-7b358bfe114b
Verdict	Malicious activity
Analysis date	8/19/2019, 12:02:20
OS	Windows 7 Professional Service Pack 1 (build: 7601, 32 bit)
Tags	trojan pony fareit
Indicators	
MIME	application/x-dosexec
File info	PE32 executable (DLL) (GUI) Intel 80386, for MS Windows
MD5	3c4de20e464146bec844471867bd1628
SHA1	32f5611459b9b63145895926b26f949d8ce7ac79
SHA256	dc030778938b8b6f98236a709d0d18734c325accf44b12a55ecc2d56b8bb9000
SSDEEP	1536:NL2LANTQTJKNV80439AUREHNOUQVVFkZLA/0Zd/:z40N0439aceIOU/0Z

TAKE YOUR SECURITY TO THE NEXT LEVEL

- ✓ Realtime interaction
- ✓ Process monitoring
- ✓ Network tracking
- ✓ Inspect behavior graph
- ✓ IOC gathering

JOIN FREE!

with ANY.RUN Community Version

ANY.RUN is an interactive service which provides full access to the guest system. Information in this report could be distorted by user actions and is provided for user acknowledgement as it is. ANY.RUN does not guarantee maliciousness or safety of the content.

Just copy Hash and put it in virus total.com and google it to analyze the hashed files. We look for the pony malware file type.

53 / 63

63 engines detected this file

dc030778938b8b6f98236a709d0d18734c325accf44b12a55ecc2d56b8bb9000

8bcac011-ac06-11e6-af10-80e65024849a file

pecl

68 KB
Size

2019-10-10 22:38:12 UTC
6 days ago

DLL

[DETECTION](#)
[DETAILS](#)
[RELATIONS](#)
[BEHAVIOR](#)
[COMMUNITY](#)

Basic Properties

MD5	3c4de20e464146bec844471867bd1628
SHA-1	32f5611459b9b63145895926b26f949d8ce7ac79
SHA-256	dc030778938b8b6f98236a709d0d18734c325accf44b12a55ecc2d56b8bb9000
Vhash	164046651d5560b8z327z69z601011z2bz
Authenticash	fe7dbfcedad1d9f3d92b0e790b58aa97680e08a3e78b7806511c42247a5a7e4
ImpHash	f689a921f86af3457d79140d57e81982
SSDEEP	1536:NL2LanYqTjKNvS0439aureEhOUqvFkZLA/0Zd/:z40N0439aceIOU/0Z
File type	Win32 DLL
Magic	PE32 executable for MS Windows (DLL) (GUI) Intel 80386 32-bit
File size	68 KB (69632 bytes)

History

Creation Time	2016-10-17 11:48:13
First Seen in The Wild	2016-10-17 04:48:13

In virus total website we can see where the malware is first found and the history about it.