Malware Analysis, Tools & Techniques

[1]Rajesh Patil, [2]Vikas Jain, [3]Rajesh Pokhriyal, [4]Rajveer Rajawat, [5]Jatin Nagpal
[1]Manager, [2] Sr Manager, [3]Manager, [4]Dy Manager, [5]Dy Manager
[1]Data Center
[1]RailTel Corporation, Gurugram, India

Abstract: Malware analysis comprises of use of different tools & methods to identify the key activities being performed by the malware**.** The investigation also includes identifying the mischievous or hidden activity being performed by a genuine application program. Many times freeware/ shareware programs are distributed in the community for the purpose of stealing user information and to compromise the end user systems. With day by day increase in computation power & with ease of availability of resources (online tutorials, cloud hosting infra), attackers are now able to develop complex malwares that can bypass antivirus programs. Attackers often use encryption to hide detection. Therefore, use of static & dynamic approaches is key to effective malware analysis.

Index Terms- Malware, Software, cloud, encryption, freeware, shareware.

I. Introduction

With increase in the user base of Internet the number of malwares is increasing very rapidly regardless of the antivirus/antimalware software. It a massive challenge for the antivirus solutions to detect the malware as attackers develop new kind of techniques to evade from the detection. Typically the anti-virus software uses signature or feed based detection techniques which is incompetent in the present scenario. Malwares are also capable to create their own variants which results in change of signatures/hashes through which it can easily evade antivirus detection.

II. Types of Malware Analysis

1) Static Malware analysis - Static analysis is the process of analyzing the code or structure of a program to identify its behavior. The program itself is not executed during this process. It is more efficient & cost effective than dynamic analysis.

SNo	Name	Functionality
1	Virustotal.com	A cloud based application to analyze programs and hash based detection
2	PEiD	To check packed/obfuscated binary programs
3	Md5deep	To calculate MD5, SHA-1, SHA-256 of the files

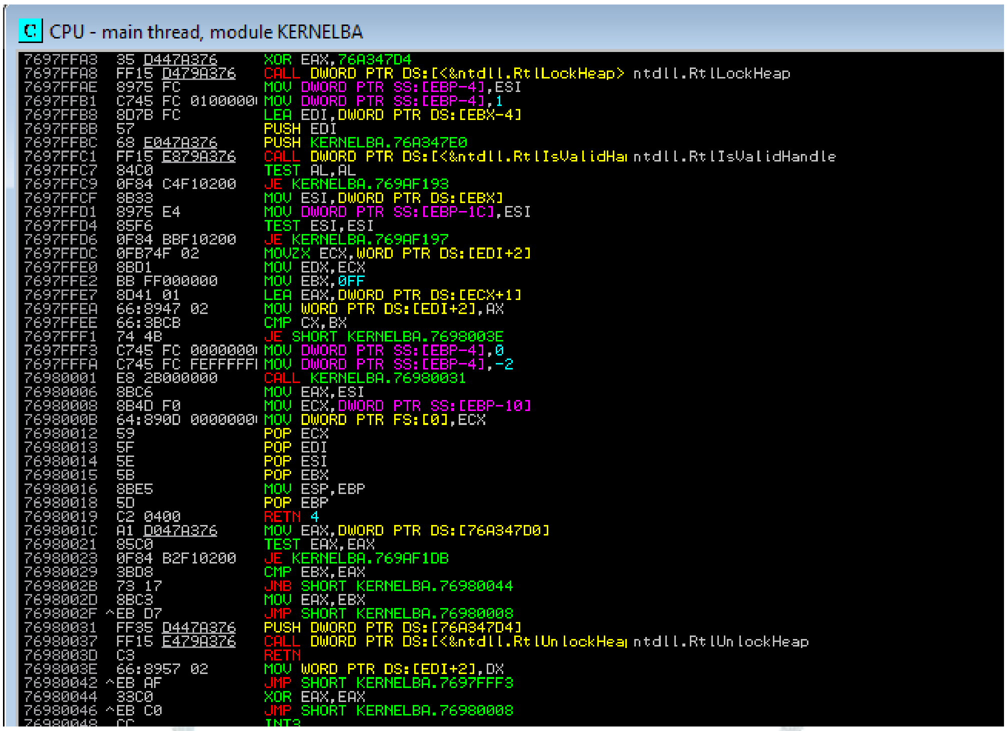
Table 1 – Static malware analysis tools

2) Dynamic Malware analysis – In Dynamic malware analysis the sample file or program is executed in a controlled environment and activity/behavior is monitored to detect malicious intent. This technique requires more sophisticated skills and it requires an isolated setup environment.

SNo	Name	Functionality
1	Hybrid-analysis.com	A cloud based application to dynamically analyze programs
2	IDA Pro	A debugger to dynamically execute executables, to debug code in assembly
3	Immunity Debugger	A debugger to dynamically execute executables, to create breakpoints & to debug code in assembly

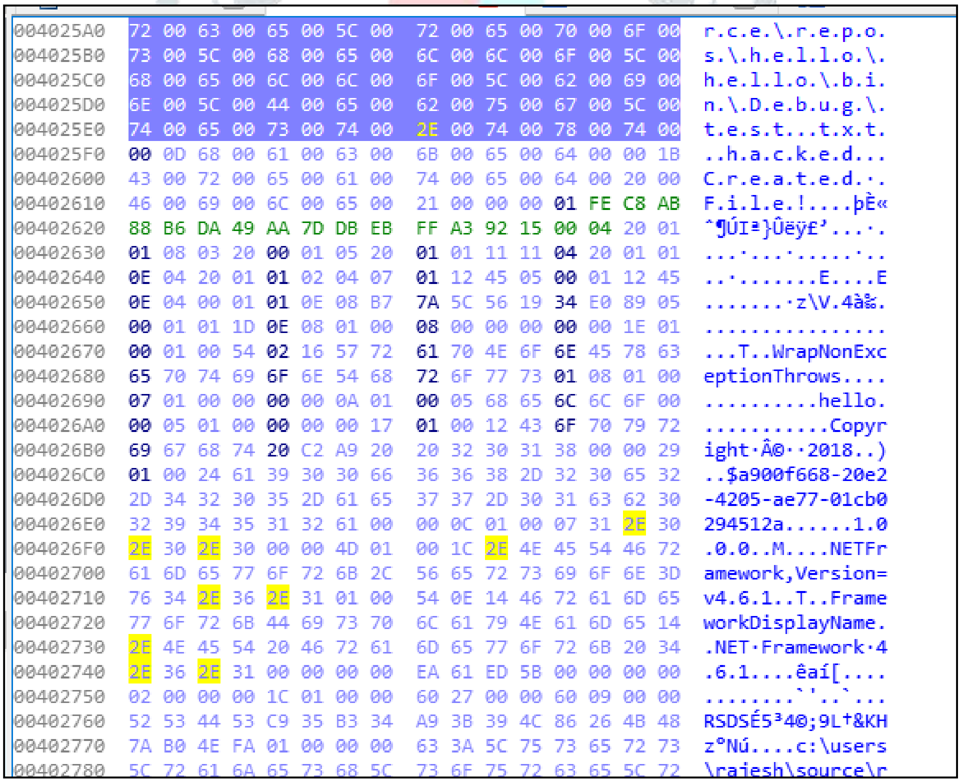
Table 2 – Dynamic malware analysis tools

III. ANALYSIS USING DIFFERENT TOOLS



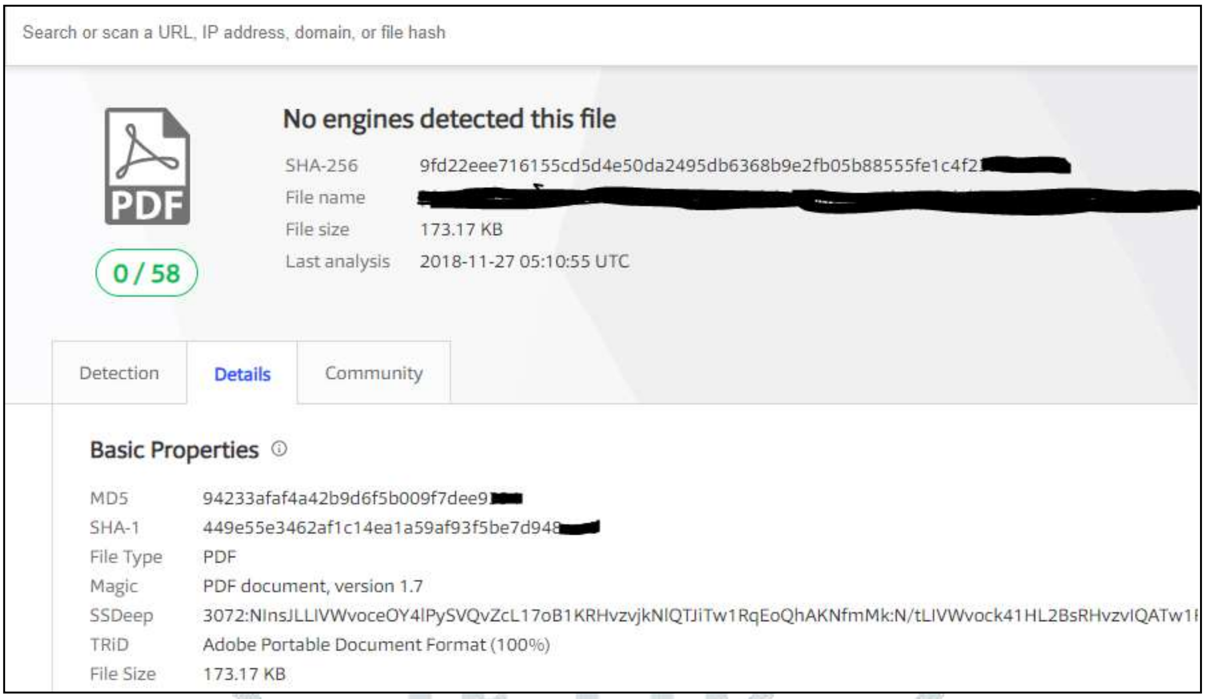
```
7697FFA3   35 D447A376       XOR EAX,76A347D4
7697FFA8   FF15 D479A376     CALL DWORD PTR DS:[<&ntdll.RtlLockHeap> ntdll.RtlLockHeap
7697FFAE   8975 FC           MOV DWORD PTR SS:[EBP-4],ESI
7697FFB1   C745 FC 0100000l  MOV DWORD PTR SS:[EBP-4],1
7697FFB8   8D7B FC           LEA EDI,DWORD PTR DS:[EBX-4]
7697FFBB   57                PUSH EDI
7697FFBC   68 E047A376       PUSH KERNELBA.76A347E0
7697FFC1   FF15 E879A376     CALL DWORD PTR DS:[<&ntdll.RtlIsValidHa ntdll.RtlIsValidHandle
7697FFC7   84C0              TEST AL,AL
7697FFC9   0F84 C4F10200     JE KERNELBA.769AF193
7697FFCF   8B33              MOV ESI,DWORD PTR DS:[EBX]
7697FFD1   8975 E4           MOV DWORD PTR SS:[EBP-1C],ESI
7697FFD4   85F6              TEST ESI,ESI
7697FFD6   0F84 BBF10200     JE KERNELBA.769AF197
7697FFDC   0FB74F 02         MOVZX ECX,WORD PTR DS:[EDI+2]
7697FFE0   8BD1              MOV EDX,ECX
7697FFE2   BB FF000000       MOV EBX,0FF
7697FFE7   8D41 01           LEA EAX,DWORD PTR DS:[ECX+1]
7697FFEA   66:8947 02        MOV WORD PTR DS:[EDI+2],AX
7697FFEE   66:3BCB           CMP CX,BX
7697FFF1   74 4B             JE SHORT KERNELBA.7698003E
7697FFF3   C745 FC 0000000l  MOV DWORD PTR SS:[EBP-4],0
7697FFFA   C745 FC FEFFFFFl  MOV DWORD PTR SS:[EBP-4],-2
76980001   E8 2B000000       CALL KERNELBA.76980031
76980006   8BC6              MOV EAX,ESI
76980008   8B4D F0           MOV ECX,DWORD PTR SS:[EBP-10]
7698000B   64:890D 0000000l  MOV DWORD PTR FS:[0],ECX
76980012   59                POP ECX
76980013   5F                POP EDI
76980014   5E                POP ESI
76980015   5B                POP EBX
76980016   8BE5              MOV ESP,EBP
76980018   5D                POP EBP
76980019   C2 0400           RETN 4
7698001C   A1 D047A376       MOV EAX,DWORD PTR DS:[76A347D0]
76980021   85C0              TEST EAX,EAX
76980023   0F84 B2F10200     JE KERNELBA.769AF1DB
76980029   3BD8              CMP EBX,EAX
7698002B   73 17             JNB SHORT KERNELBA.76980044
7698002D   8BC3              MOV EAX,EBX
7698002F ^EB D7              JMP SHORT KERNELBA.76980008
76980031   FF35 D447A376     PUSH DWORD PTR DS:[76A347D4]
76980037   FF15 E479A376     CALL DWORD PTR DS:[<&ntdll.RtlUnlockHea ntdll.RtlUnlockHeap
7698003D   C3                RETN
7698003E   66:8957 02        MOV WORD PTR DS:[EDI+2],DX
76980042 ^EB AF              JMP SHORT KERNELBA.7697FFF3
76980044   33C0              XOR EAX,EAX
76980046 ^EB C0              JMP SHORT KERNELBA.76980008
76980048   CC                INT3
```

Image 1 – Dynamic malware analysis using Immunity Debugger



```
004025A0  72 00 63 00 65 00 5C 00  72 00 65 00 70 00 6F 00  r.c.e.\.r.e.p.o.
004025B0  73 00 5C 00 68 00 65 00  6C 00 6C 00 6F 00 5C 00  s.\.h.e.l.l.o.\.
004025C0  68 00 65 00 6C 00 6C 00  6F 00 5C 00 62 00 69 00  h.e.l.l.o.\.b.i.
004025D0  6E 00 5C 00 44 00 65 00  62 00 75 00 67 00 5C 00  n.\.D.e.b.u.g.\.
004025E0  74 00 65 00 73 00 74 00  2E 00 74 00 78 00 74 00  t.e.s.t...t.x.t.
004025F0  00 0D 68 00 61 00 63 00  6B 00 65 00 64 00 00 1B  ..h.a.c.k.e.d...
00402600  43 00 72 00 65 00 61 00  74 00 65 00 64 00 20 00  C.r.e.a.t.e.d.·.
00402610  46 00 69 00 6C 00 65 00  21 00 00 00 01 FE C8 AB  F.i.l.e.!....þÈ«
00402620  88 B6 DA 49 AA 7D DB EB  FF A3 92 15 00 04 20 01  ˆ¶ÚIª}Ûëÿ£’....·.
00402630  01 08 03 20 00 01 05 20  01 01 11 11 04 20 01 01  ...·...·.....·..
00402640  0E 04 20 01 01 02 04 07  01 12 45 05 00 01 12 45  ..·.......E....E
00402650  0E 04 00 01 01 0E 08 B7  7A 5C 56 19 34 E0 89 05  .......·z\V.4à‰.
00402660  00 01 01 1D 0E 08 01 00  08 00 00 00 00 00 1E 01  ................
00402670  00 01 00 54 02 16 57 72  61 70 4E 6F 6E 45 78 63  ...T..WrapNonExc
00402680  65 70 74 69 6F 6E 54 68  72 6F 77 73 01 08 01 00  eptionThrows....
00402690  07 01 00 00 00 00 0A 01  00 05 68 65 6C 6C 6F 00  ..........hello.
004026A0  00 05 01 00 00 00 00 17  01 00 12 43 6F 70 79 72  ...........Copyr
004026B0  69 67 68 74 20 C2 A9 20  20 32 30 31 38 00 00 29  ight·Â©··2018..)
004026C0  01 00 24 61 39 30 30 66  36 36 38 2D 32 30 65 32  ..$a900f668-20e2
004026D0  2D 34 32 30 35 2D 61 65  37 37 2D 30 31 63 62 30  -4205-ae77-01cb0
004026E0  32 39 34 35 31 32 61 00  00 0C 01 00 07 31 2E 30  294512a......1.0
004026F0  2E 30 2E 30 00 00 4D 01  00 1C 2E 4E 45 54 46 72  .0.0..M....NETFr
00402700  61 6D 65 77 6F 72 6B 2C  56 65 72 73 69 6F 6E 3D  amework,Version=
00402710  76 34 2E 36 2E 31 01 00  54 0E 14 46 72 61 6D 65  v4.6.1..T..Frame
00402720  77 6F 72 6B 44 69 73 70  6C 61 79 4E 61 6D 65 14  workDisplayName.
00402730  2E 4E 45 54 20 46 72 61  6D 65 77 6F 72 6B 20 34  .NET·Framework·4
00402740  2E 36 2E 31 00 00 00 00  EA 61 ED 5B 00 00 00 00  .6.1....êaí[....
00402750  02 00 00 00 1C 01 00 00  60 27 00 00 60 09 00 00  ........`'..`...
00402760  52 53 44 53 C9 35 B3 34  A9 3B 39 4C 86 26 4B 48  RSDSÉ5³4©;9L†&KH
00402770  7A B0 4E FA 01 00 00 00  63 3A 5C 75 73 65 72 73  z°Nú....c:\users
00402780  5C 72 61 6A 65 73 68 5C  73 6F 75 72 63 65 5C 72  \rajesh\source\r
```

Image 2 – Dynamic malware analysis using IDA Pro



No engines detected this file

SHA-256 9fd22eee716155cd5d4e50da2495db6368b9e2fb05b88555fe1c4f2[redacted]
File name [redacted]
File size 173.17 KB
Last analysis 2018-11-27 05:10:55 UTC

Basic Properties

MD5 94233afaf4a42b9d6f5b009f7dee9[redacted]
SHA-1 449e55e3462af1c14ea1a59af93f5be7d948[redacted]
File Type PDF
Magic PDF document, version 1.7
SSDeep 3072:NInsJLLIVWvoceOY4lPySVQvZcL17oB1KRHvzvjkNlQTJiTw1RqEoQhAKNfmMk:N/tLIVWvock41HL2BsRHvzvlQATw1
TRiD Adobe Portable Document Format (100%)
File Size 173.17 KB

Image 3 – Dynamic malware analysis using VirusTotal

REFERENCES

[1] Victor Marak.2013Windows Malware Analysis Essentials
[2] Christopher C. Elisan.2015.Advanced Malware Analysis