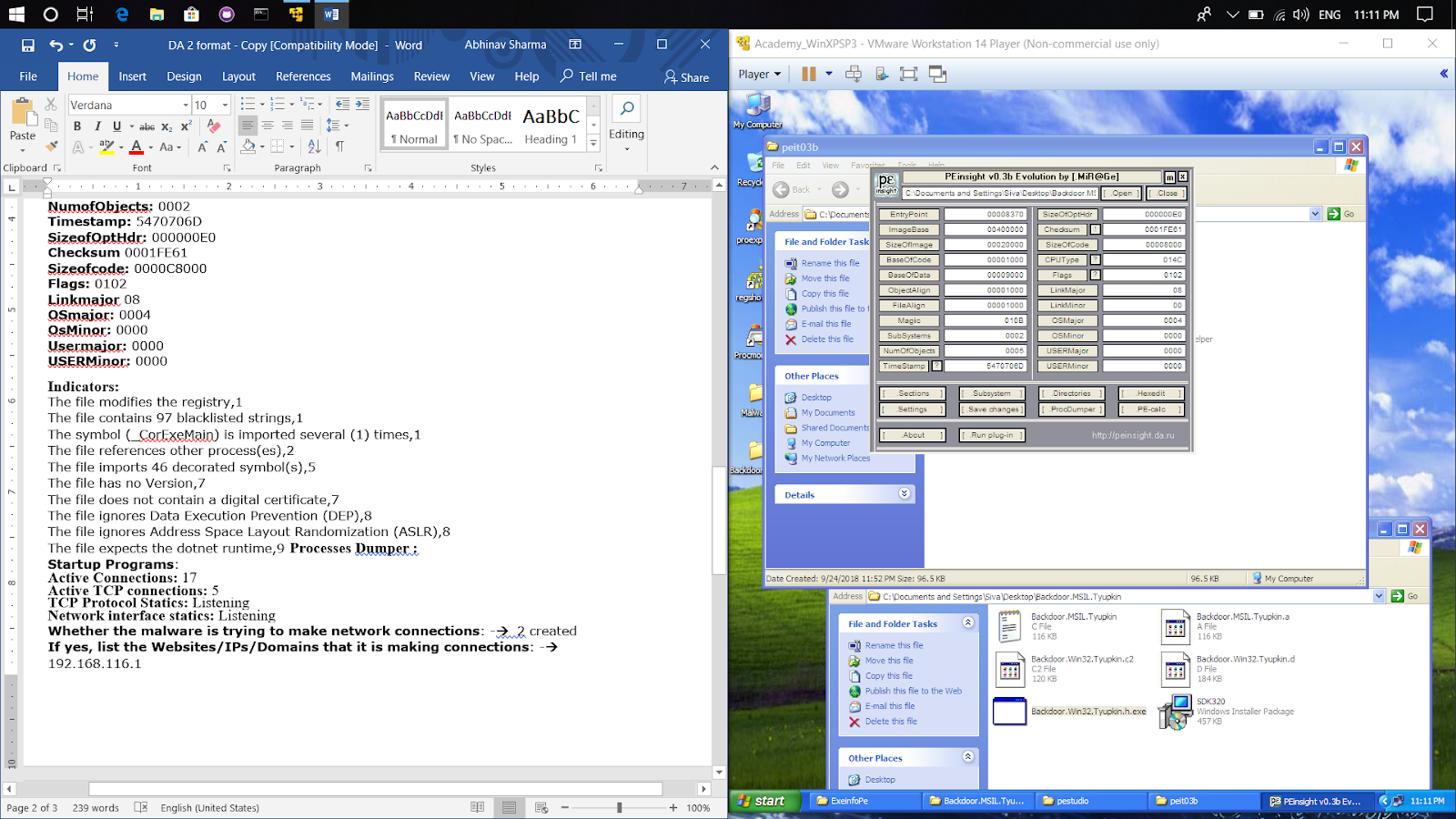
**Malware Analysis Report**

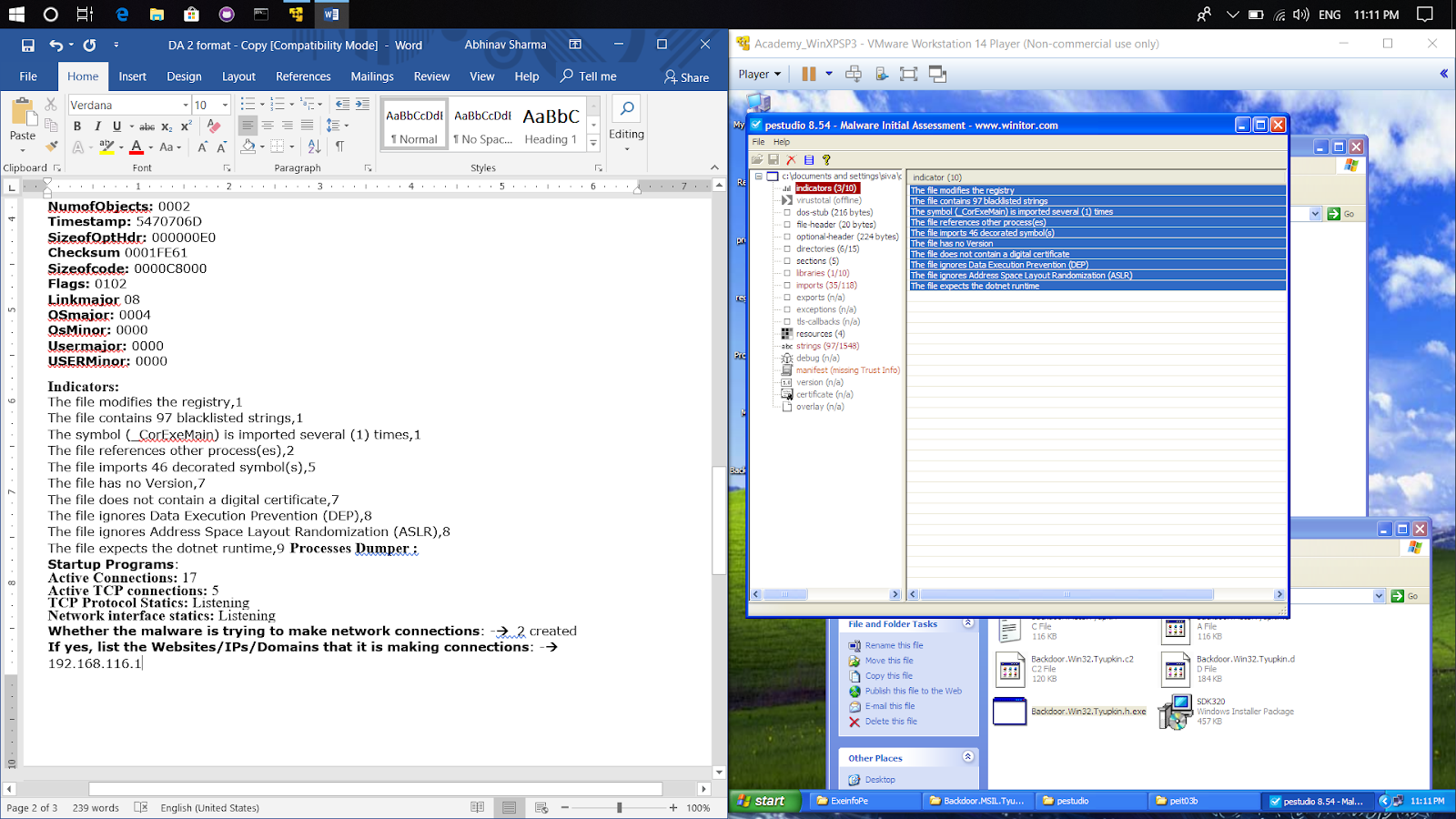
Type of Malware: Backdoor.Win32.Tyupkin

**Static Malware Analysis Report:**

1. **MD5 HASH& SHA HASH** : 🡪 250B77DFBB1B666E95B3BCDA082DE287 and 5A699A8F64046D3D7FB5014D0242C159A04B8EED
2. **File Size** : 🡪 120.00 KB (122880 bytes)
3. **File Info** 🡪 No Match found.
4. **File Type** 🡪 Portable Executable 32 .NET Assembly
5. **PE Size** : 🡪 120.00 KB (122880 bytes)
6. **Company Name** : 🡪 Kaspersky Labs
7. **Legal Copyright :** 🡪 NIL
8. **File Name :** 🡪Backdoor.Win32.Tyupkin.h
9. **UPX Utility** 🡪 NIL
10. **Entropy value** 🡪 5.7157
11. **Entropy Percentage** 🡪 71%
12. **Entry Point 🡪** 00008370
13. **File Offset 🡪** 00008370
14. **Linker Info 🡪** 8.00
15. **File Size** 🡪 0001E000h
16. **First byte 🡪** FF,25,C8,91,40,00,CC,CC,CC,CC
17. **Subsystem 🡪** Windows GUI
18. **Overlay** 🡪 NO   00000000
19. **Version Info 🡪** No File version info found
20. **Zero Byte Test🡪** 30.2824%
21. **Image base:** 00400000
22. **Size of Image:** 00020000
23. **Base of code:** 00001000
24. **Base of Data:** 00009000
25. **Object Align:** 00001000
26. **Magic:** 010B
27. **Num of Objects:** 0002
28. **Timestamp:** 5470706D
29. **Size of OptHdr:** 000000E0
30. **Checksum**: 0001FE61
31. **Size of code:** 0000C8000
32. **Flags:** 0102
33. **Link major** 08
34. **OS major:** 0004
35. **OS Minor:** 0000
36. **User major:** 0000
37. **USER Minor:** 0000
38. **Processes Dumper :**



1. **Indicators:**

****

.

1. **Dos Header values:**

DOS Header

Magic number: 0x5a4d (MZ)

Bytes in last page: 144

Pages in file: 3

Relocations: 0

Size of header in paragraphs: 4

Minimum extra paragraphs: 0

Maximum extra paragraphs: 65535

Initial (relative) SS value: 0

Initial SP value: 0xb8

Initial IP value: 0

Initial (relative) CS value: 0

Address of relocation table: 0x40

Overlay number: 0

OEM identifier: 0

OEM information: 0

PE header offset: 0x118

1. **Coff(Common Object file format) Header values:**

COFF/File header

Machine: 0x14c IMAGE\_FILE\_MACHINE\_I386

Number of sections: 5

Date/time stamp: 1416654957 (Sat, 22 Nov 2014 11:15:57 UTC)

Symbol Table offset: 0

Number of symbols: 0

Size of optional header: 0xe0

Characteristics: 0x102

Characteristics names

IMAGE\_FILE\_EXECUTABLE\_IMAGE

IMAGE\_FILE\_32BIT\_MACHINE

1. **Optional Header values:**

Optional/Image header

Magic number: 0x10b (PE32)

Linker major version: 8

Linker minor version: 0

Size of .text section: 0x8000

Size of .data section: 0x15000

Size of .bss section: 0

Entry point: 0x8370

Address of .text section: 0x1000

Address of .data section: 0x9000

Image Base: 0x400000

Alignment of sections: 0x1000

Alignment factor: 0x1000

Major version of required OS: 4

Minor version of required OS: 0

Major version of image: 0

Minor version of image: 0

Major version of subsystem: 4

Minor version of subsystem: 0

Size of image: 0x20000

Size of headers: 0x1000

Checksum: 0x1fe61

Subsystem required: 0x2 (IMAGE\_SUBSYSTEM\_WINDOWS\_GUI)

DLL characteristics: 0

DLL characteristics names

Size of stack to reserve: 0x100000

Size of stack to commit: 0x1000

Size of heap space to reserve: 0x100000

Size of heap space to commit: 0x1000

1. **All PE section values:**

Sections

Section

Name: .text

Virtual Address: 0x1000

Physical Address: 0x7967

Size: 0x8000 (32768 bytes)

Pointer to Data: 0x1000

Relocations: 0

Characteristics: 0x60000020

Characteristic Names

IMAGE\_SCN\_CNT\_CODE

IMAGE\_SCN\_MEM\_EXECUTE

IMAGE\_SCN\_MEM\_READ

Section

Name: .rdata

Virtual Address: 0x9000

Physical Address: 0x1100e

Size: 0x12000 (73728 bytes)

Pointer to Data: 0x9000

Relocations: 0

Characteristics: 0x40000040

Characteristic Names

IMAGE\_SCN\_CNT\_INITIALIZED\_DATA

IMAGE\_SCN\_MEM\_READ

Section

Name: .data

Virtual Address: 0x1b000

Physical Address: 0x243c

Size: 0x1000 (4096 bytes)

Pointer To Data: 0x1b000

Relocations: 0

Characteristics: 0xc0000040

Characteristic Names

IMAGE\_SCN\_CNT\_INITIALIZED\_DATA

IMAGE\_SCN\_MEM\_READ

IMAGE\_SCN\_MEM\_WRITE

Section

Name: .rsrc

Virtual Address: 0x1e000

Physical Address: 0x6a0

Size: 0x1000 (4096 bytes)

Pointer To Data: 0x1c000

Relocations: 0

Characteristics: 0x40000040

Characteristic Names

IMAGE\_SCN\_CNT\_INITIALIZED\_DATA

IMAGE\_SCN\_MEM\_READ

Section

Name: .reloc

Virtual Address: 0x1f000

Physical Address: 0x6d2

Size: 0x1000 (4096 bytes)

Pointer To Data: 0x1d000

Relocations: 0

Characteristics: 0x42000040

Characteristic Names

IMAGE\_SCN\_CNT\_INITIALIZED\_DATA

IMAGE\_SCN\_MEM\_DISCARDABLE

IMAGE\_SCN\_MEM\_READ

1. **Imported function values:**

Imported functions

Library

Name: MSVCR80.dll

Functions

Function

Name: srand

Function

Name: rand

Function

Name: printf

Function

Name: \_strdup

Function

Name: exit

Function

Name: wcstombs

Function

Name: mbstowcs

Function

Name: remove

Function

Name: wprintf

Function

Name: \_cexit

Function

Name: \_amsg\_exit

Function

Name: \_\_FrameUnwindFilter

Function

Name: \_time64

Function

Name: \_localtime64

Function

Name: \_invalid\_parameter\_noinfo

Function

Name: \_\_CxxUnregisterExceptionObject

Function

Name: \_\_CxxQueryExceptionSize

Name: ?endl@std@@YAAAV?$basic\_ostream@DU?$char\_traits@D@std@@@1@AAV21@@Z

Function

Name: ?cout@std@@3V?$basic\_ostream@DU?$char\_traits@D@std@@@1@A

Function

Name: ?\_Unlock@?$basic\_streambuf@DU?$char\_traits@D@std@@@std@@QAEXXZ

Function

Name: ?sputc@?$basic\_streambuf@DU?$char\_traits@D@std@@@std@@QAEHD@Z

Function

Name: ?close@?$basic\_ofstream@DU?$char\_traits@D@std@@@std@@QAEXXZ

Function

Name: ??0?$basic\_ofstream@DU?$char\_traits@D@std@@@std@@QAE@PBDHH@Z

Function

Name: ??0?$basic\_ifstream@DU?$char\_traits@D@std@@@std@@QAE@PBDHH@Z

Function

Name: ?flush@?$basic\_ostream@DU?$char\_traits@D@std@@@std@@QAEAAV12@XZ

Function

Name: ??6?$basic\_ostream@DU?$char\_traits@D@std@@@std@@QAEAAV01@J@Z

Function

Name: ??\_D?$basic\_ofstream@DU?$char\_traits@D@std@@@std@@QAEXXZ

Function

Name: ??\_D?$basic\_ifstream@DU?$char\_traits@D@std@@@std@@QAEXXZ

Function

Name: ??0?$basic\_string@DU?$char\_traits@D@std@@V?$allocator@D@2@@std@@QAE@ABV01@@Z

Function

Name: ??0?$basic\_string@DU?$char\_traits@D@std@@V?$allocator@D@2@@std@@QAE@PBD@Z

Function

Name: ?fill@?$basic\_ios@DU?$char\_traits@D@std@@@std@@QBEDXZ

Function

Name: ??6?$basic\_ostream@DU?$char\_traits@D@std@@@std@@QAEAAV01@K@Z

Function

Name: ?\_Lock@?$basic\_streambuf@DU?$char\_traits@D@std@@@std@@QAEXXZ

Function

Name: ?tie@?$basic\_ios@DU?$char\_traits@D@std@@@std@@QBEPAV?$basic\_ostream@DU?$char\_traits@D@std@@@2@XZ

Function

Name: ?\_Osfx@?$basic\_ostream@DU?$char\_traits@D@std@@@std@@QAEXXZ

Function

Name: ?sputn@?$basic\_streambuf@DU?$char\_traits@D@std@@@std@@QAEHPBDH@Z

Function

Name: ?uncaught\_exception@std@@YA\_NXZ

Function

Name: ??6?$basic\_ostream@DU?$char\_traits@D@std@@@std@@QAEAAV01@I@Z

Function

Name: ??6?$basic\_ostream@DU?$char\_traits@D@std@@@std@@QAEAAV01@H@Z

Function

Name: ??6?$basic\_ostream@DU?$char\_traits@D@std@@@std@@QAEAAV01@G@Z

Function

Name: ??6?$basic\_ostream@DU?$char\_traits@D@std@@@std@@QAEAAV01@P6AAAV01@AAV01@@Z@Z

Function

Name: ?rdbuf@?$basic\_ios@DU?$char\_traits@D@std@@@std@@QBEPAV?$basic\_streambuf@DU?$char\_traits@D@std@@@2@XZ

Function

Name: ?setstate@?$basic\_ios@DU?$char\_traits@D@std@@@std@@QAEXH\_N@Z

Function

Name: ?c\_str@?$basic\_string@DU?$char\_traits@D@std@@V?$allocator@D@2@@std@@QBEPBDXZ

Function

Name: ??1?$basic\_string@DU?$char\_traits@D@std@@V?$allocator@D@2@@std@@QAE@XZ

Library

Name: KERNEL32.dll

Functions

Function

Name: TerminateProcess

Function

Name: GetCurrentProcess

Function

Name: UnhandledExceptionFilter

Function

Name: SetUnhandledExceptionFilter

Function

Name: IsDebuggerPresent

Function

Name: GetSystemTimeAsFileTime

Function

Name: GetCurrentProcessId

Function

Name: GetCurrentThreadId

Function

1. **Exported function values:**  export directory not found
2. **Disassemble Entry point:**

8370: ff 25 c8 91 40 00 jmp dword [0x4091c8]

8376: cc int3

8377: cc int3

8378: cc int3

8379: cc int3

837a: cc int3

837b: cc int3

837c: cc int3

837d: cc int3

837e: cc int3

837f: cc int3

8380: 03 30 add esi, [eax]

8382: 01 00 add [eax], eax

8384: 0d 00 00 00 00 or eax, 0x0

8389: 00 00 add [eax], al

838b: 00 fe add dh, bh

838d: 06 push es

838e: 4c dec esp

838f: 00 00 add [eax], al

8391: 06 push es

8392: 28 2f sub [edi], ch

8394: 00 00 add [eax], al

8396: 06 push es

8397: 26 2a 00 sub al, [es:eax]

839a: 00 00 add [eax], al

839c: 00 00 add [eax], al

839e: 00 00 add [eax], al

83a0: 03 30 add esi, [eax]

83a2: 01 00 add [eax], eax

83a4: 0d 00 00 00 00 or eax, 0x0

83a9: 00 00 add [eax], al

83ab: 00 fe add dh, bh

83ad: 06 push es

83ae: 4e dec esi

83af: 00 00 add [eax], al

83b1: 06 push es

83b2: 28 2f sub [edi], ch

83b4: 00 00 add [eax], al

83b6: 06 push es

83b7: 26 2a 00 sub al, [es:eax]

83ba: 00 00 add [eax], al

83bc: 00 00 add [eax], al

83be: 00 00 add [eax], al

83c0: 03 30 add esi, [eax]

83c2: 01 00 add [eax], eax

83c4: 0d 00 00 00 00 or eax, 0x0

83c9: 00 00 add [eax], al

83cb: 00 fe add dh, bh

83cd: 06 push es

83ce: 50 push eax

83cf: 00 00 add [eax], al

83d1: 06 push es

83d7: 26 2a 00 sub al, [es:eax]

83da: 00 00 add [eax], al

83dc: 00 00 add [eax], al

83de: 00 00 add [eax], al

83e0: 03 30 add esi, [eax]

83e2: 01 00 add [eax], eax

83e4: 0d 00 00 00 00 or eax, 0x0

83e9: 00 00 add [eax], al

83eb: 00 fe add dh, bh

83ed: 06 push es

83ee: 52 push edx

83ef: 00 00 add [eax], al

83f1: 06 push es

83f2: 28 2f sub [edi], ch

83f4: 00 00 add [eax], al

83f6: 06 push es

83f7: 26 2a 00 sub al, [es:eax]

83fa: 00 00 add [eax], al

83fc: 00 00 add [eax], al

83fe: 00 00 add [eax], al

8400: 03 30 add esi, [eax]

8402: 01 00 add [eax], eax

8404: 0d 00 00 00 00 or eax, 0x0

8409: 00 00 add [eax], al

840b: 00 fe add dh, bh

840d: 06 push es

840e: 54 push esp

840f: 00 00 add [eax], al

8411: 06 push es

8412: 28 2f sub [edi], ch

8414: 00 00 add [eax], al

8416: 06 push es

8417: 26 2a 00 sub al, [es:eax]

841a: 00 00 add [eax], al

841c: 00 00 add [eax], al

841e: 00 00 add [eax], al

8420: 03 30 add esi, [eax]

8422: 01 00 add [eax], eax

8424: 0d 00 00 00 00 or eax, 0x0

8429: 00 00 add [eax], al

842b: 00 fe add dh, bh

842d: 06 push es

842e: 56 push esi

842f: 00 00 add [eax], al

8431: 06 push es

8432: 28 2f sub [edi], ch

8434: 00 00 add [eax], al

8436: 06 push es

8437: 26 2a 00 sub al, [es:eax]

843a: 00 00 add [eax], al

843c: 00 00 add [eax], al

843e: 00 00 add [eax], al

8440: 03 30 add esi, [eax]

8442: 01 00 add [eax], eax

8444: 0d 00 00 00 00 or eax, 0x0

1. **Version of file :🡪** License GPLv2+: GNU GPL version 2 or later <https://www.gnu.org/licenses/gpl-2.0.txt>.
2. **DOS Header Hash: :🡪**

headers

   header

       header\_name: IMAGE\_DOS\_HEADER

       md5: b21fca0037445b4971f2b051b7373900

       sha1: a569e380281584df54b422fbb745a8df7806c0b1

sha256: f215799b1140fdff628fa97b01e22a52cbc1b98946b67f0efe844fe3653b978c

       ssdeep: 3:/hlaMtrl/JlltjCgf/DrTl:/2Mzjt/DrTl

section

   section\_name

   md5: b21fca0037445b4971f2b051b7373900

   sha1: a569e380281584df54b422fbb745a8df7806c0b1

   sha256:f215799b1140fdff628fa97b01e22a52cbc1b98946b67f0efe844fe3653b978

   ssdeep: 3:/hlaMtrl/JlltjCgf/DrTl:/2Mzjt/DrTl

1. **COff Header Hash: :🡪**

headers

header

header\_name: IMAGE\_COFF\_HEADER

md5: 060cb8648c7b0dd9b1a95563690737e5

sha1: 227fd0eb97c092c27279b51196a65ab7598df702

sha256: 9cf62aea496b75ce92c7045ac4e95b82758d73660e23dbe61472c07c502799db

ssdeep: 3:hIVbt/Nkn:hTn

1. **Optional Header Hash: :🡪**

Headers

   header

       header\_name: IMAGE\_OPTIONAL\_HEADER

       md5: f0389cd2a58a8709dd0d1997f2118127

       sha1: 8ef419ce6286cad67e655bc31f9b5a36d5f1f427

       sha256: a205301643586d25e09c0f1e792738134327c5e1eeb305951561ae3ba29397cc

       ssdeep: 3:7vlh//VmPlltvl6all/hlll/tv/glPt1l9tllH:7vL6h1mlN

section

    section\_name

    md5: f0389cd2a58a8709dd0d1997f2118127

    sha1: 8ef419ce6286cad67e655bc31f9b5a36d5f1f427

    sha256: a205301643586d25e09c0f1e792738134327c5e1eeb305951561ae3ba29397cc

    ssdeep: 3:7vlh//VmPlltvl6all/hlll/tv/glPt1l9tllH:7vL6h1mlN

1. **File entropy : 🡪** 5.715688 (normal)
2. **Fpu anti-disassemble:🡪** no
3. **Imagebase : :🡪** normal
4. **Entrypoint :🡪** normal
5. **DOS Stub :🡪** normal
6. **TLS Callback function :🡪** NIL
7. **TLS Directory :🡪** NIL
8. **Timestamp :🡪** normal
9. **Section count :🡪** 5
10. **Sections :🡪** .text,.rdata,.data,.rsrc,.reloc
11. Details about the section:



1. Name all the section names and their status (Normal or Suspicious)

.text: normal

.rdata: normal

.data: normal

.rsrc: normal

.reloc: normal

1. **Packer in file: :🡪** NIL
2. **Resource Statics : 🡪**

Total Structs: 27

Total Resource Directory: 8

Total Directory Entry: 11

Total Data String: 4

Total Data Entry: 4

1. **Security features in PEFILE :** 🡪

ASLR: no

DEP/NX: no

SEH: yes

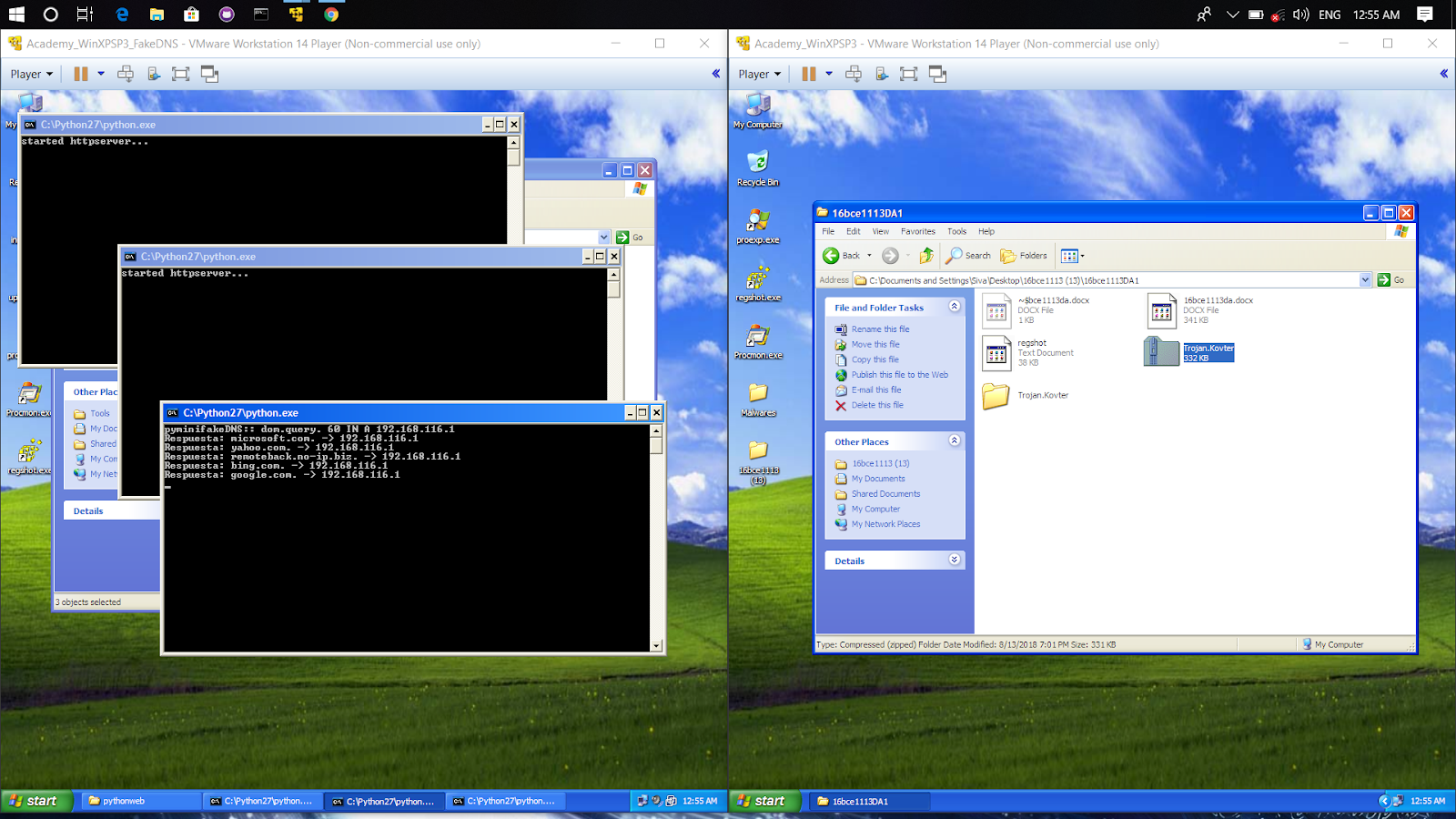
Stack cookies (EXPERIMENTAL): yes

1. **Suspicious file/ Normal file :**🡪 Normal
2. **show network-related strings (IPs, hostnames etc) :** 🡪NIL

**Dynamic Malware Analysis Report**

Run the Malware and fill the following points

1. **Any new Processes created** : NIL
2. **If yes, how many Processes are newly created?** : NIL
3. **Names of the processes** 🡪 NIL
4. **Proc explorer running or closed ->** running
5. **Any new changes in the number of processes** 🡪 NIL
6. **Whether the malware is trying to make network connections**: yes

****

1. **If yes, list the Websites/IPs/Domains that it is making connections**:

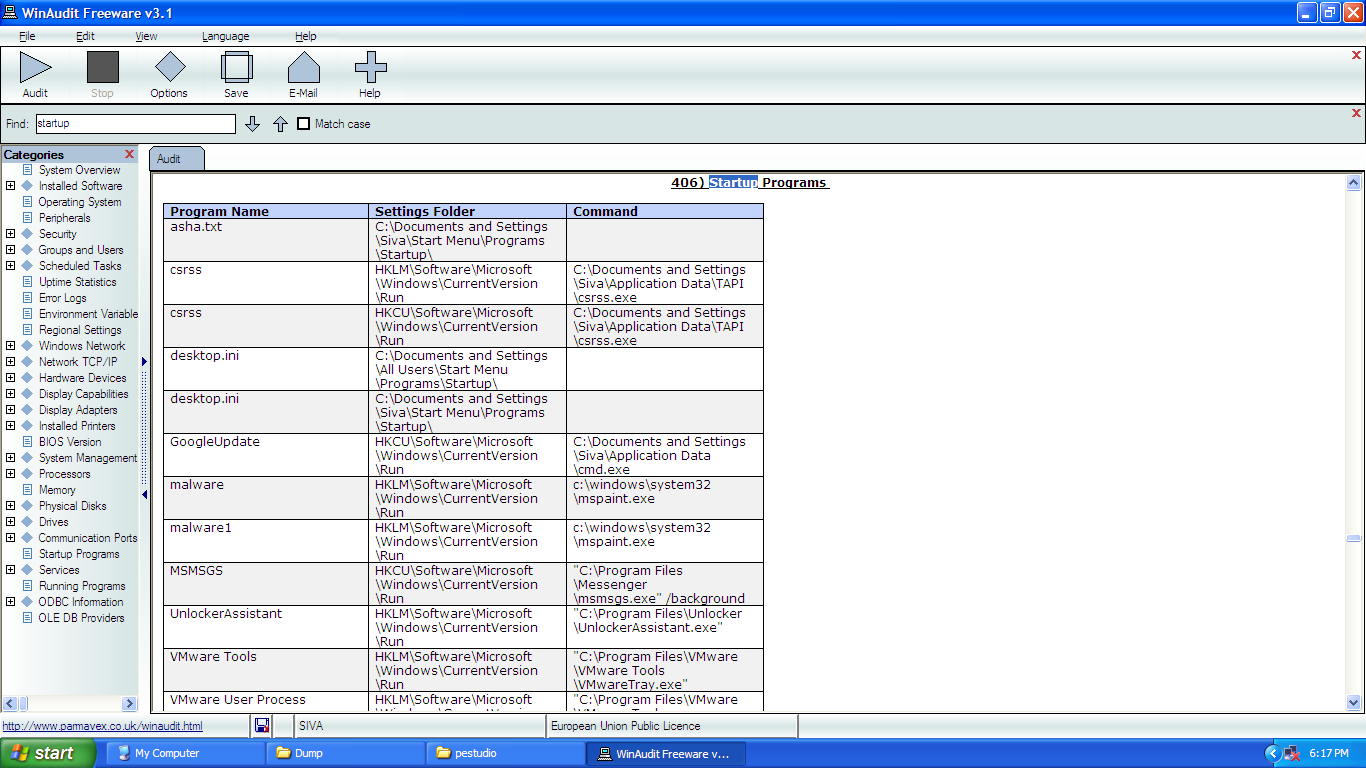
www.microsoft.com ->192.168.116.1

remoteback.no-ip.biz. ->192.168.116.1

cabin.su->192.168.116.1

mjed10.no-ip.info.->192.168.116.1

1. **Total number of connections the malware is making:** 25
2. Startup Programs:

****

1. Number of Active Connections: 17
2. Number of Active TCP connections: 5
3. TCP Protocol Statics: Listening
4. Network interface statics: Listening
5. During execution of the malware, bold and italicize the appropriate behavior from the following

a.Self-deletes 1

b.Self-deletes and getting created in another folder. 1

C:\WINDOWS\Prefetch\ROOTKIT.EXE-06DD46A3.pf

c. Replicates in some folders NIL

d. Replicates in all folders NIL

e. Propagates NIL

1. Changes file name 10

HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: 1F F6 D6 10 DB B9 87 F4 B1 A6 9B DB 4E 51 F5 98 E9 EE 1E E5 90 0E BF 00 FB 3F 2E 0C 82 B6 16 92 3D BC 4B 1C 61 47 4E D2 FA 2A F2 B5 E1 97 57 11 87 3D B1 11 B7 8D B8 BC 35 F4 D3 FD 7B A2 69 1F 16 A7 B2 0B D5 21 9A A9 7B A6 A0 A6 60 C8 FE 17

HKLM\SOFTWARE\Microsoft\Cryptography\RNG\Seed: FC 5D 4F 4B 28 5F 9A F3 EF 18 06 96 E1 D1 21 7D 9A F3 07 52 85 77 4F 1A 97 8F 79 0E F9 85 45 17 1F 4C AB 53 21 7B 73 40 8F DE 29 3A EF 99 74 2F 27 A5 24 A2 45 6B B5 46 55 AC 24 8F 8F 7D 92 21 7E 0D CB 15 AC C5 9B 88 4E B5 3B 7E 00 B1 2A 65

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Directory: "C:\Documents and Settings\Siva\Local Settings\Temporary Internet Files\Content.IE5"

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\Directory: "C:\WINDOWS\system32\config\systemprofile\Local Settings\Temporary Internet Files\Content.IE5"

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path1\CachePath: "C:\Documents and Settings\Siva\Local Settings\Temporary Internet Files\Content.IE5\Cache1"

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path1\CachePath: "C:\WINDOWS\system32\config\systemprofile\Local Settings\Temporary Internet Files\Content.IE5\Cache1"

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path2\CachePath: "C:\Documents and Settings\Siva\Local Settings\Temporary Internet Files\Content.IE5\Cache2"

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path2\CachePath: "C:\WINDOWS\system32\config\systemprofile\Local Settings\Temporary Internet Files\Content.IE5\Cache2"

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path3\CachePath: "C:\Documents and Settings\Siva\Local Settings\Temporary Internet Files\Content.IE5\Cache3"

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path3\CachePath: "C:\WINDOWS\system32\config\systemprofile\Local Settings\Temporary Internet Files\Content.IE5\Cache3"

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path4\CachePath: "C:\Documents and Settings\Siva\Local Settings\Temporary Internet Files\Content.IE5\Cache4"

HKLM\SOFTWARE\Microsoft\Windows\CurrentVersion\Internet Settings\Cache\Paths\path4\CachePath: "C:\WINDOWS\system32\config\systemprofile\Local Settings\Temporary Internet Files\Content.IE5\Cache4"

HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings: 3C 00 00 00 02 00 00 00 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

HKU\.DEFAULT\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings: 3C 00 00 00 03 00 00 00 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

HKU\S-1-5-21-1202660629-926492609-839522115-1005\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR\_EHACNGU: 07 00 00 00 DD 00 00 00 10 05 F9 35 6F 67 D4 01

HKU\S-1-5-21-1202660629-926492609-839522115-1005\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR\_EHACNGU: 07 00 00 00 DE 00 00 00 00 58 A2 4E 6F 67 D4 01

HKU\S-1-5-21-1202660629-926492609-839522115-1005\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR\_HVFPHG: 07 00 00 00 5F 00 00 00 30 34 7E 39 6F 67 D4 01

HKU\S-1-5-21-1202660629-926492609-839522115-1005\Software\Microsoft\Windows\CurrentVersion\Explorer\UserAssist\{75048700-EF1F-11D0-9888-006097DEACF9}\Count\HRZR\_HVFPHG: 07 00 00 00 60 00 00 00 10 2C 9B 4E 6F 67 D4 01

HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings: 3C 00 00 00 02 00 00 00 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

HKU\S-1-5-18\Software\Microsoft\Windows\CurrentVersion\Internet Settings\Connections\SavedLegacySettings: 3C 00 00 00 03 00 00 00 09 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00

* 1. Changes the icons based on the extension 8

C:\Documents and Settings\Siva\NTUSER.DAT.LOG

C:\WINDOWS\Prefetch\CMD.EXE-087B4001.pf

C:\WINDOWS\system32\config\default.LOG

C:\WINDOWS\system32\config\software.LOG

C:\WINDOWS\system32\config\system.LOG

C:\WINDOWS\system32\config\systemprofile\Cookies\index.dat

C:\WINDOWS\system32\config\systemprofile\Local Settings\History\History.IE5\index.dat

C:\WINDOWS\system32\config\systemprofile\Local Settings\Temporary Internet Files\Content.IE5\index.dat

* 1. Getting added in the startup programs ( could be got from startup programs)
     1. Press Ctrl+Alt+Del → NIL
  2. Getting added in autorun programs NIL
  3. Establishes Network connections
     1. To a single server Yes

1. To multiple servers No
2. **Type of the Malware**: Virus

1. **Regshot Output :**

* **Keys Added:47**
* **Keys deleted:NIL**
* **Values added:199**
* **Values Modified:33**
* **Values Deleted:2**
* **Files Added:55**
* **Files Deleted:5**
* **Files Modified:13**
* **Folders added:13**
* **Total Changes:367**

1. **List some unique behavior of the malware** : 🡪

1. Access and infection

2. Control and theft

3. A unique digit combination key based on random numbers is freshly generated for every session.

4. Making connection to other sites

5. Cloning itself in other folders

1. **Suggest some removal procedures apart from VM Snapshots** : 🡪
2. Delete temporary files
3. Download malware scanners
4. Use forced removal methods like ‘rm –rf ‘filename’ ’ to delete the infected files
5. Enter the system into safe mode