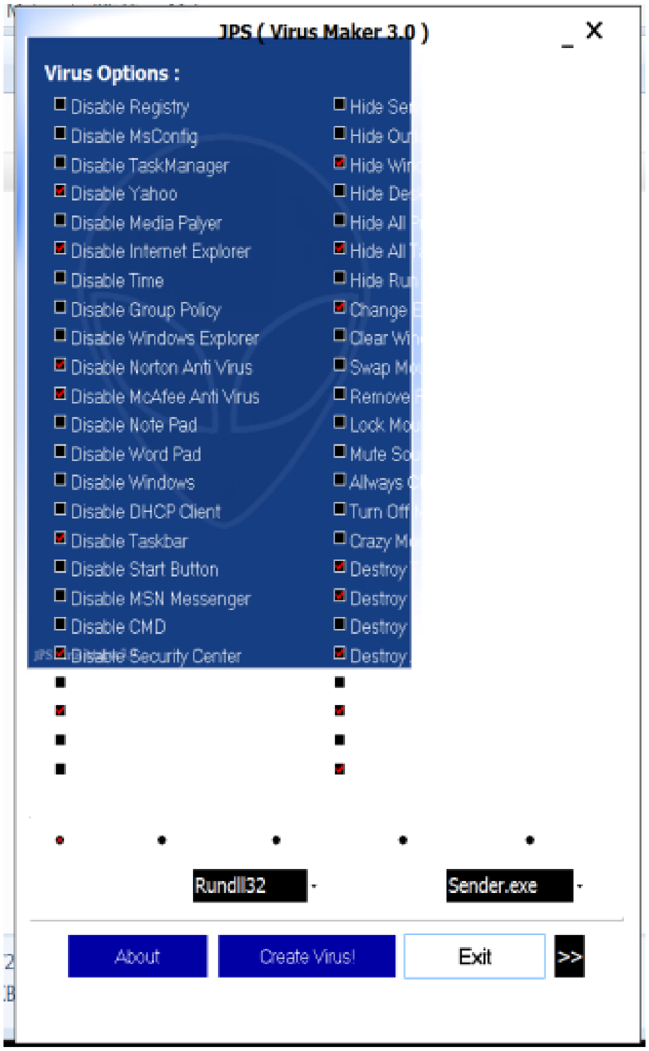
Malware Threats
Lab Assignments (Module 7)

Name: Sachin Saj T K
Roll NO: CB.EN.P2CEN18012
Date of Submission: 18/06/2019

Creating a Virus Using the JPS Virus Maker Tool

1. Checking what all features wanted, for the virus to perform



JPS (Virus Maker 3.0)

Virus Options :

☐ Disable Registry
☐ Disable MsConfig
☐ Disable TaskManager
☒ Disable Yahoo
☐ Disable Media Palyer
☒ Disable Internet Explorer
☐ Disable Time
☐ Disable Group Policy
☐ Disable Windows Explorer
☒ Disable Norton Anti Virus
☒ Disable McAfee Anti Virus
☐ Disable Note Pad
☐ Disable Word Pad
☐ Disable Windows
☐ Disable DHCP Client
☒ Disable Taskbar
☐ Disable Start Button
☐ Disable MSN Messenger
☐ Disable CMD
☒ Disable Security Center

☐ Hide Se
☐ Hide Ou
☒ Hide Wi
☐ Hide De
☐ Hide All
☒ Hide All
☐ Hide Ru
☒ Change
☐ Clear Wi
☐ Swap M
☐ Remove
☐ Lock Mo
☐ Mute So
☐ Always
☐ Turn Off
☐ Crazy M
☒ Destroy
☒ Destroy
☐ Destroy
☒ Destroy

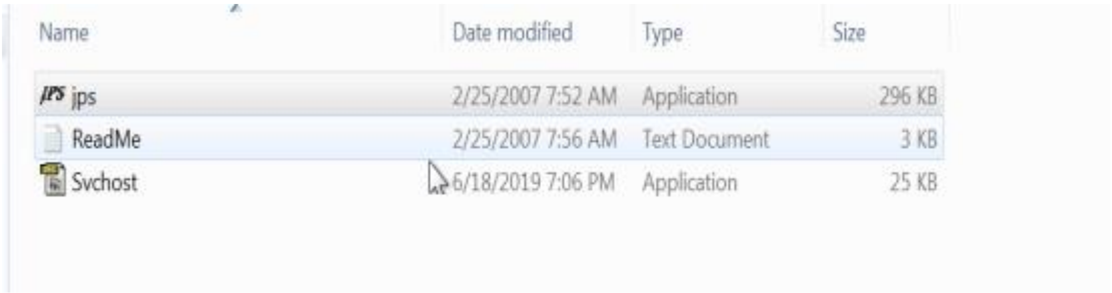
☐ ☐
☒ ☒
☐ ☐
☐ ☒

● ○ ○ ○ ○

Rundll32

Sender.exe

2. Virus is created



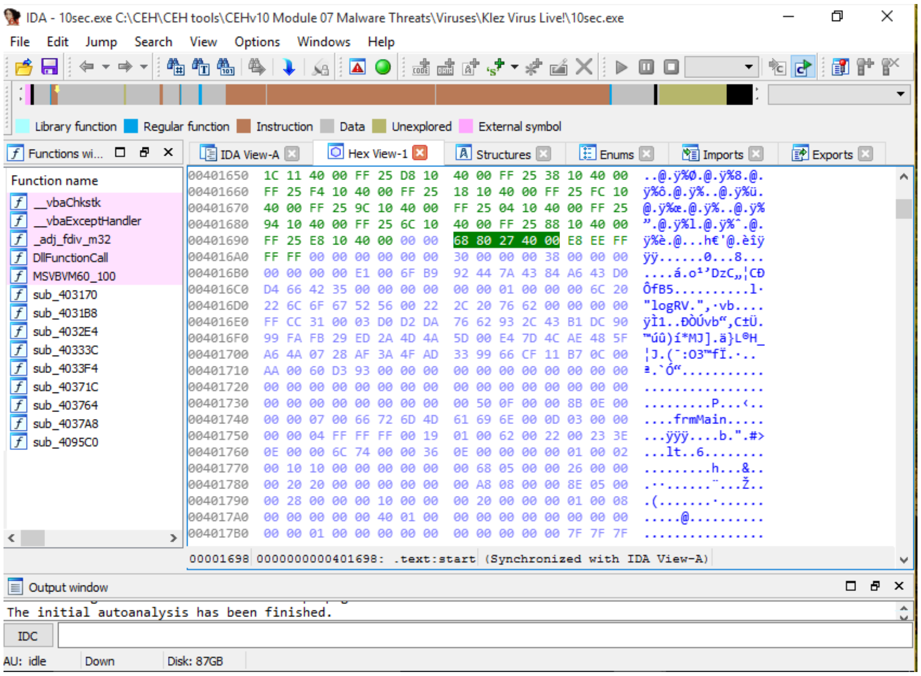
Name	Date modified	Type	Size
jps	2/25/2007 7:52 AM	Application	296 KB
ReadMe	2/25/2007 7:56 AM	Text Document	3 KB
Svchost	6/18/2019 7:06 PM	Application	25 KB

Lab Analysis

Tool/Utility	**Information**
JPS Virus Maker Tool	**To make Virus options are used:** • Disable Yahoo • Disable Internet Explorer • Disable Norton Antivirus • Disable McAfree Antivirus • Disable Taskbar • Disable Security Restore • Disable Control panel • Hide Windows Clock • Hide All Tasks in Task,mgr • Destroy Audio Services • Terminate Windows • Auto Setup

Virus Analysis Using IDA Pro

1. Hex View-A



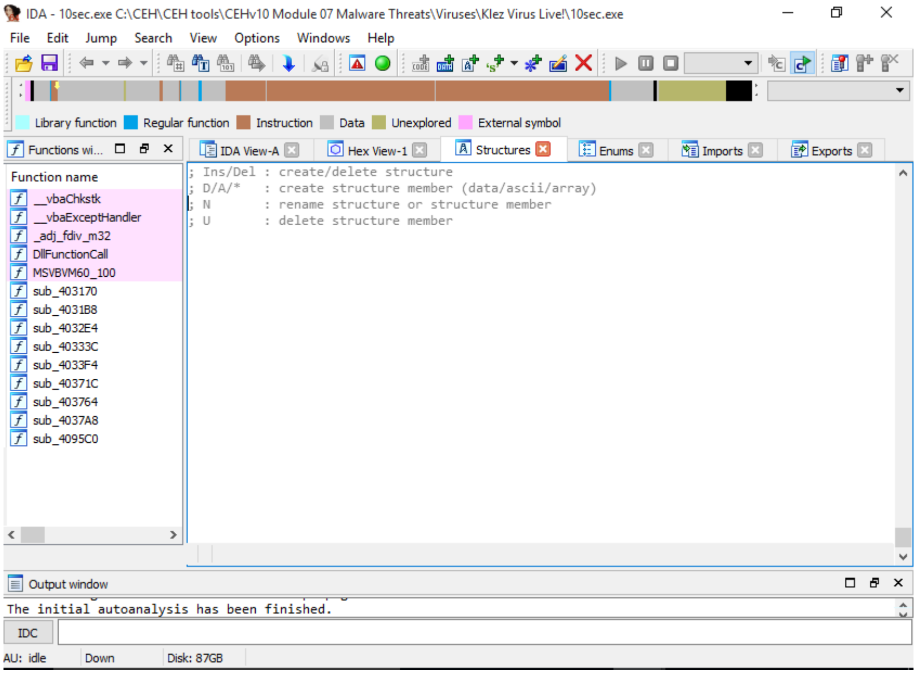
IDA - 10sec.exe C:\CEH\CEH tools\CEHv10 Module 07 Malware Threats\Viruses\Klez Virus Live!\10sec.exe

Function name
- __vbaChkstk
- __vbaExceptHandler
- _adj_fdiv_m32
- DllFunctionCall
- MSVBVM60_100
- sub_403170
- sub_4031B8
- sub_4032E4
- sub_40333C
- sub_4033F4
- sub_40371C
- sub_403764
- sub_4037A8
- sub_4095C0

```
00401650  1C 11 40 00 FF 25 D8 10  40 00 FF 25 38 10 40 00  ..@.ÿ%Ø.@.ÿ%8.@.
00401660  FF 25 F4 10 40 00 FF 25  18 10 40 00 FF 25 FC 10  ÿ%ô.@.ÿ%..@.ÿ%ü.
00401670  40 00 FF 25 9C 10 40 00  FF 25 04 10 40 00 FF 25  @.ÿ%œ.@.ÿ%..@.ÿ%
00401680  94 10 40 00 FF 25 6C 10  40 00 FF 25 88 10 40 00  ”.@.ÿ%l.@.ÿ%ˆ.@.
00401690  FF 25 E8 10 40 00 00 00  68 80 27 40 00 E8 EE FF  ÿ%è.@...h€'@.èîÿ
004016A0  FF FF 00 00 00 00 00 00  30 00 00 00 38 00 00 00  ÿÿ......0...8...
004016B0  00 00 00 00 E1 00 6F B9  92 44 7A 43 84 A6 43 D0  ....á.o¹’DzC„¦CÐ
004016C0  D4 66 42 35 00 00 00 00  00 00 01 00 00 00 6C 20  ÔfB5..........l·
004016D0  22 6C 6F 67 52 56 00 22  2C 20 76 62 00 00 00 00  "logRV.",·vb....
004016E0  FF CC 31 00 03 D0 D2 DA  76 62 93 2C 43 B1 DC 90  ÿÌ1..ÐÒÚvb“,C±Ü.
004016F0  99 FA FB 29 ED 2A 4D 4A  5D 00 E4 7D 4C AE 48 5F  ™úû)í*MJ].ä}L®H_
00401700  A6 4A 07 28 AF 3A 4F AD  33 99 66 CF 11 B7 0C 00  ¦J.(¯:O3™fÏ.·..
00401710  AA 00 60 D3 93 00 00 00  00 00 00 00 00 00 00 00  ª.`Ó“...........
00401720  00 00 00 00 00 00 00 00  00 00 00 00 00 00 00 00  ................
00401730  00 00 00 00 00 00 00 00  00 50 0F 00 00 8B 0E 00  .........P...‹..
00401740  00 00 07 00 66 72 6D 4D  61 69 6E 00 0D 03 00 00  ....frmMain.....
00401750  00 00 04 FF FF FF 00 19  01 00 62 00 22 00 23 3E  ...ÿÿÿ....b.".#>
00401760  0E 00 00 6C 74 00 00 36  0E 00 00 00 00 01 00 02  ...lt..6........
00401770  00 10 10 00 00 00 00 00  00 68 05 00 00 26 00 00  .........h...&..
00401780  00 20 20 00 00 00 00 00  00 A8 08 00 00 8E 05 00  .··......¨...Ž..
00401790  00 28 00 00 00 10 00 00  00 20 00 00 00 01 00 08  .(.......·......
004017A0  00 00 00 00 00 40 01 00  00 00 00 00 00 00 00 00  .....@..........
004017B0  00 00 01 00 00 00 00 00  00 00 00 00 00 7F 7F 7F  ................
00001698 0000000000401698: .text:start (Synchronized with IDA View-A)
```

```
The initial autoanalysis has been finished.
```

2. Structure



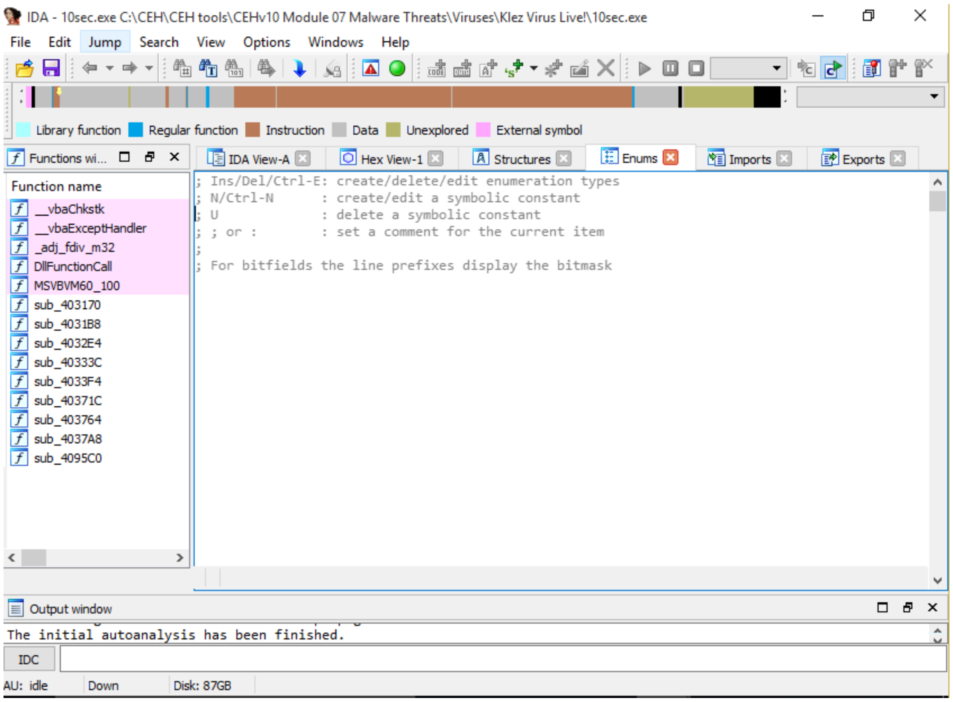
IDA - 10sec.exe C:\CEH\CEH tools\CEHv10 Module 07 Malware Threats\Viruses\Klez Virus Live!\10sec.exe

Function name
- __vbaChkstk
- __vbaExceptHandler
- _adj_fdiv_m32
- DllFunctionCall
- MSVBVM60_100
- sub_403170
- sub_4031B8
- sub_4032E4
- sub_40333C
- sub_4033F4
- sub_40371C
- sub_403764
- sub_4037A8
- sub_4095C0

```
; Ins/Del : create/delete structure
; D/A/*   : create structure member (data/ascii/array)
; N       : rename structure or structure member
; U       : delete structure member
```

```
The initial autoanalysis has been finished.
```

3. Enums



```
; Ins/Del/Ctrl-E: create/delete/edit enumeration types
; N/Ctrl-N      : create/edit a symbolic constant
; U             : delete a symbolic constant
; ; or :        : set a comment for the current item
;
; For bitfields the line prefixes display the bitmask
```

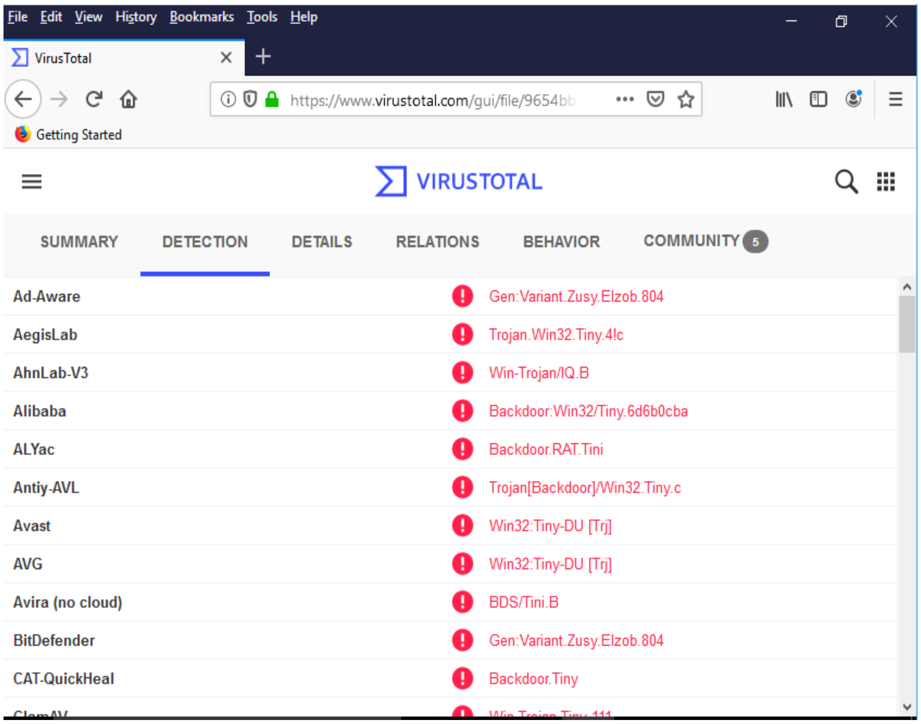
```
The initial autoanalysis has been finished.
```

Lab Analysis

Tool/Utility	**Information Collected/Objective Achieved**
IDA Pro	**File name**: 10sec.exe
	Output: • Hex View-A • View Structures • View Enums

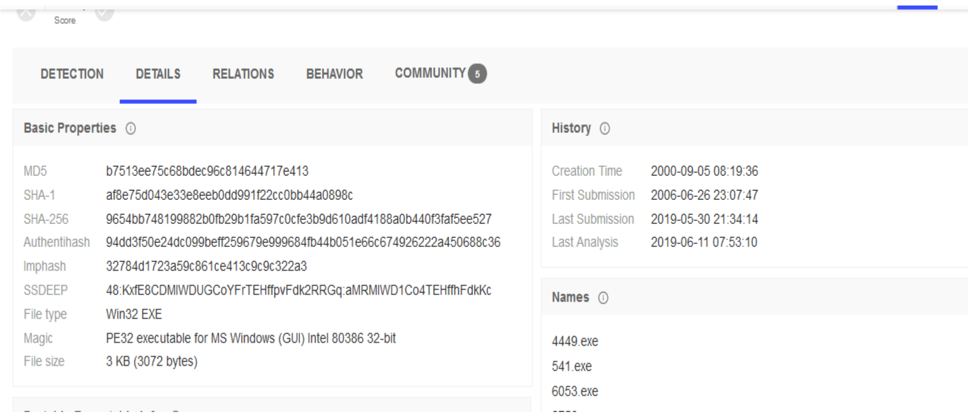
Virus Analysis Using Virus Total

1. Virus total, scanned!



Ad-Aware	Gen:Variant.Zusy.Elzob.804
AegisLab	Trojan.Win32.Tiny.4!c
AhnLab-V3	Win-Trojan/IQ.B
Alibaba	Backdoor:Win32/Tiny.6d6b0cba
ALYac	Backdoor.RAT.Tini
Antiy-AVL	Trojan[Backdoor]/Win32.Tiny.c
Avast	Win32:Tiny-DU [Trj]
AVG	Win32:Tiny-DU [Trj]
Avira (no cloud)	BDS/Tini.B
BitDefender	Gen:Variant.Zusy.Elzob.804
CAT-QuickHeal	Backdoor.Tiny
ClamAV	Win.Trojan.Tiny-111

2. Details



Basic Properties

MD5	b7513ee75c68bdec96c814644717e413
SHA-1	af8e75d043e33e8eeb0dd991f22cc0bb44a0898c
SHA-256	9654bb748199882b0fb29b1fa597c0cfe3b9d610adf4188a0b440f3faf5ee527
Authentihash	94dd3f50e24dc099beff259679e999684fb44b051e66c674926222a450688c36
Imphash	32784d1723a59c861ce413c9c9c322a3
SSDEEP	48:KxfE8CDMlWDUGCoYFrTEHffpvFdk2RRGq:aMRMlWD1Co4TEHffhFdkKc
File type	Win32 EXE
Magic	PE32 executable for MS Windows (GUI) Intel 80386 32-bit
File size	3 KB (3072 bytes)

History

Creation Time	2000-09-05 08:19:36
First Submission	2006-06-26 23:07:47
Last Submission	2019-05-30 21:34:14
Last Analysis	2019-06-11 07:53:10

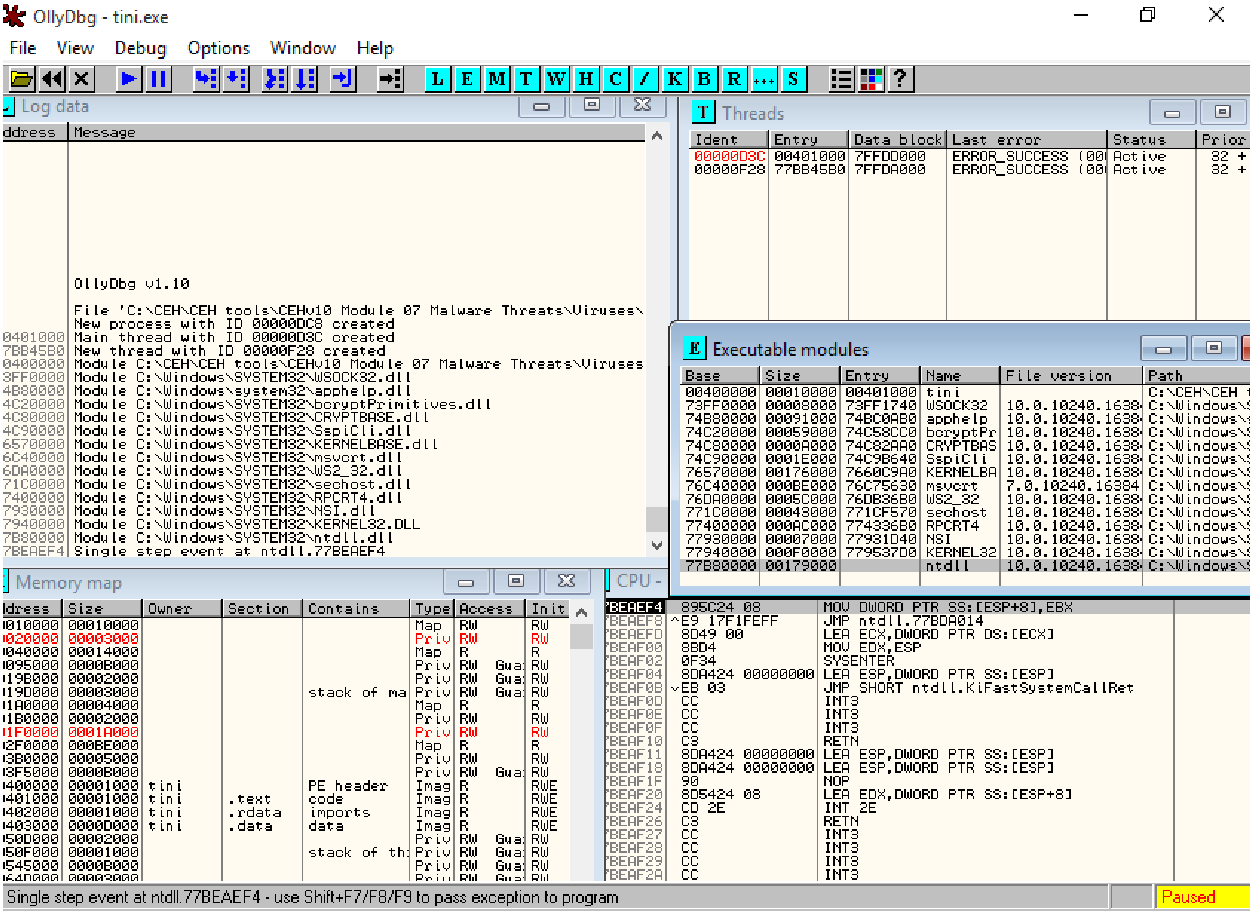
Names

4449.exe
541.exe
6053.exe

Lab Analysis

Tool/Utility	Information Collected/Objective Achieved
Virus Total	**Scan Report Shows:** • **SHA256**:9654bb748199882b0fb29b1fa597c0cfe3b9d610asf4188a0b440f3faf5ee527 • **SHA1:** af8e75d043e33e8eeb0dd991f22cc0bb44a0898c • **MD5:** b7513ee75c68bdec96c814644717e413 • **File size:** 3 KB • **File name**: tini • **File Type**: Win32 • **Analysis date:**2019-06-11 07:53:10

Virus Analysis Using OllyDbg



```
ddress |Message

       |OllyDbg v1.10

       |File 'C:\CEH\CEH tools\CEHv10 Module 07 Malware Threats\Viruses\
       |New process with ID 00000DC8 created
0401000|Main thread with ID 00000D3C created
7BB45B0|New thread with ID 00000F28 created
0400000|Module C:\CEH\CEH tools\CEHv10 Module 07 Malware Threats\Viruses
3FF0000|Module C:\Windows\SYSTEM32\WSOCK32.dll
4B80000|Module C:\Windows\system32\apphelp.dll
4C20000|Module C:\Windows\SYSTEM32\bcryptPrimitives.dll
4C80000|Module C:\Windows\SYSTEM32\CRYPTBASE.dll
4C90000|Module C:\Windows\SYSTEM32\SspiCli.dll
6570000|Module C:\Windows\SYSTEM32\KERNELBASE.dll
6C40000|Module C:\Windows\SYSTEM32\msvcrt.dll
6DA0000|Module C:\Windows\SYSTEM32\WS2_32.dll
71C0000|Module C:\Windows\SYSTEM32\sechost.dll
7400000|Module C:\Windows\SYSTEM32\RPCRT4.dll
7930000|Module C:\Windows\SYSTEM32\NSI.dll
7940000|Module C:\Windows\SYSTEM32\KERNEL32.DLL
7B80000|Module C:\Windows\SYSTEM32\ntdll.dll
7BEAEF4|Single step event at ntdll.77BEAEF4
```

```
Ident    Entry    Data block Last error        Status  Prior
00000D3C 00401000 7FFDD000   ERROR_SUCCESS (00 Active   32 +
00000F28 77BB45B0 7FFDA000   ERROR_SUCCESS (00 Active   32 +
```

```
Base     Size     Entry    Name     File version    Path
00400000 00010000 00401000 tini                     C:\CEH\CEH t
73FF0000 00008000 73FF1740 WSOCK32  10.0.10240.1638 C:\Windows\
74B80000 00091000 74BC0AB0 apphelp  10.0.10240.1638 C:\Windows\
74C20000 00059000 74C58CC0 bcryptPr 10.0.10240.1638 C:\Windows\
74C80000 0000A000 74C82AA0 CRYPTBAS 10.0.10240.1638 C:\Windows\
74C90000 0001E000 74C9B640 SspiCli  10.0.10240.1638 C:\Windows\
76570000 00176000 7660C9A0 KERNELBA 10.0.10240.1638 C:\Windows\
76C40000 000BE000 76C75630 msvcrt   7.0.10240.16384 C:\Windows\
76DA0000 0005C000 76DB36B0 WS2_32   10.0.10240.1638 C:\Windows\
771C0000 00043000 771CF570 sechost  10.0.10240.1638 C:\Windows\
77400000 000AC000 774336B0 RPCRT4   10.0.10240.1638 C:\Windows\
77930000 00007000 77931D40 NSI      10.0.10240.1638 C:\Windows\
77940000 000F0000 779537D0 KERNEL32 10.0.10240.1638 C:\Windows\
77B80000 00179000          ntdll    10.0.10240.1638 C:\Windows\
```

```
ldress  Size     Owner Section Contains    Type Access   Init
010000  00010000                           Map  RW       RW
020000  00003000                           Priv RW       RW
040000  00014000                           Map  R        R
095000  0000B000                           Priv RW  Gua: RW
19B000  00002000                           Priv RW  Gua: RW
19D000  00003000               stack of ma Priv RW  Gua: RW
1A0000  00004000                           Map  R        R
1B0000  00002000                           Priv RW       RW
1F0000  0001A000                           Priv RW       RW
2F0000  000BE000                           Map  R        R
3B0000  00005000                           Priv RW       RW
3F5000  0000B000                           Priv RW  Gua: RW
400000  00001000 tini          PE header   Imag R        RWE
401000  00001000 tini  .text   code        Imag R        RWE
402000  00001000 tini  .rdata  imports     Imag R        RWE
403000  0000D000 tini  .data   data        Imag R        RWE
50D000  00002000                           Priv RW  Gua: RW
50F000  00001000               stack of th:Priv RW  Gua: RW
545000  0000B000                           Priv RW  Gua: RW
64D000  00003000                           Priv RW  Gua: RW
```

```
7BEAEF4  895C24 08         MOV DWORD PTR SS:[ESP+8],EBX
7BEAEF8 ^E9 17F1FEFF       JMP ntdll.77BDA014
7BEAEFD  8D49 00           LEA ECX,DWORD PTR DS:[ECX]
7BEAF00  8BD4              MOV EDX,ESP
7BEAF02  0F34              SYSENTER
7BEAF04  8DA424 00000000   LEA ESP,DWORD PTR SS:[ESP]
7BEAF0B vEB 03             JMP SHORT ntdll.KiFastSystemCallRet
7BEAF0D  CC                INT3
7BEAF0E  CC                INT3
7BEAF0F  CC                INT3
7BEAF10  C3                RETN
7BEAF11  8DA424 00000000   LEA ESP,DWORD PTR SS:[ESP]
7BEAF18  8DA424 00000000   LEA ESP,DWORD PTR SS:[ESP]
7BEAF1F  90                NOP
7BEAF20  8D5424 08         LEA EDX,DWORD PTR SS:[ESP+8]
7BEAF24  CD 2E             INT 2E
7BEAF26  C3                RETN
7BEAF27  CC                INT3
7BEAF28  CC                INT3
7BEAF29  CC                INT3
7BEAF2A  CC                INT3
```

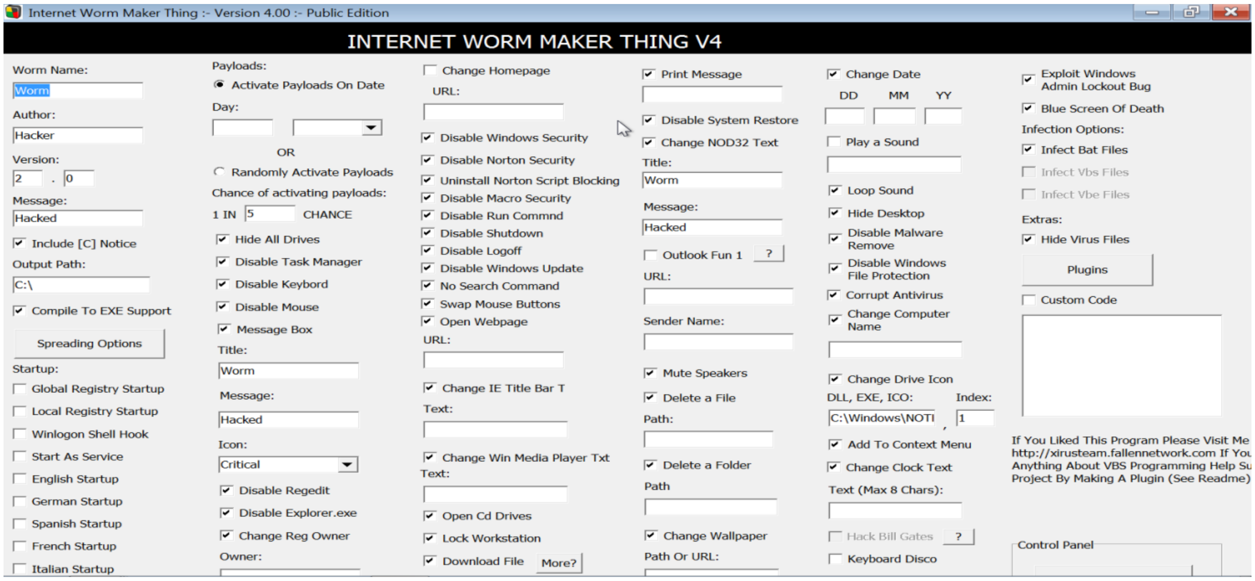
Single step event at ntdll.77BEAEF4 - use Shift+F7/F8/F9 to pass exception to program

Paused

Lab Analysis

Tool/Utility	Information Collected/Objective Achieved
OllyDbg	**Result:** • CPU-main thread • Log data • Executable modules • Memory Map • Threads

Creating a Worm Using Internet Worm Maker Thing



Internet Worm Maker Thing :- Version 4.00 :- Public Edition

INTERNET WORM MAKER THING V4

Worm Name: Worm
Author: Hacker
Version: 2 . 0
Message: Hacked
☑ Include [C] Notice
Output Path: C:\
☑ Compile To EXE Support
Startup:
□ Global Registry Startup
□ Local Registry Startup
□ Winlogon Shell Hook
□ Start As Service
□ English Startup
□ German Startup
□ Spanish Startup
□ French Startup
□ Italian Startup

Payloads:
● Activate Payloads On Date
Day:
OR
○ Randomly Activate Payloads
Chance of activating payloads:
1 IN 5 CHANCE
☑ Hide All Drives
☑ Disable Task Manager
☑ Disable Keybord
☑ Disable Mouse
☑ Message Box
Title: Worm
Message: Hacked
Icon: Critical
☑ Disable Regedit
☑ Disable Explorer.exe
☑ Change Reg Owner
Owner:

□ Change Homepage
URL:
☑ Disable Windows Security
☑ Disable Norton Security
☑ Uninstall Norton Script Blocking
☑ Disable Macro Security
☑ Disable Run Commnd
☑ Disable Shutdown
☑ Disable Logoff
☑ Disable Windows Update
☑ No Search Command
☑ Swap Mouse Buttons
☑ Open Webpage
URL:
☑ Change IE Title Bar T
Text:
☑ Change Win Media Player Txt
Text:
☑ Open Cd Drives
☑ Lock Workstation
☑ Download File

☑ Print Message
☑ Disable System Restore
☑ Change NOD32 Text
Title: Worm
Message: Hacked
□ Outlook Fun 1
URL:
Sender Name:
☑ Mute Speakers
☑ Delete a File
Path:
☑ Delete a Folder
Path
☑ Change Wallpaper
Path Or URL:

☑ Change Date
DD MM YY
□ Play a Sound
☑ Loop Sound
☑ Hide Desktop
☑ Disable Malware Remove
☑ Disable Windows File Protection
☑ Corrupt Antivirus
☑ Change Computer Name
☑ Change Drive Icon
DLL, EXE, ICO: C:\Windows\NOTI , Index: 1
☑ Add To Context Menu
☑ Change Clock Text
Text (Max 8 Chars):
□ Hack Bill Gates
□ Keyboard Disco

☑ Exploit Windows Admin Lockout Bug
☑ Blue Screen Of Death
Infection Options:
☑ Infect Bat Files
□ Infect Vbs Files
□ Infect Vbe Files
Extras:
☑ Hide Virus Files
□ Custom Code

If You Liked This Program Please Visit Me http://xirusteam.fallennetwork.com If You Anything About VBS Programming Help Su Project By Making A Plugin (See Readme)

Lab Analysis

Tool/Utility	Information Collected/Objective Achieved
Internet Worm Maker Thing	**To make Worm option are used:** • Hide all driver • Disables Task Manager • Disable Keyboard • Disable mouse • Message box • Disable Regedit • Disable Explorer.exe • Change Reg owner • Change HomePage • Disable Windows security • Disable Norton security • Disable Run command • Disable Shutdown