
# Master of Information Security

MIS4203 – Independent Studies in Information Security

Index Number – 16770217 | Reg. Number – 2016MIS021

## Study Number – 07 - Digital Forensic – II

January 19, 2019

University of Colombo School of Computing

Table of Contents

Problem

Perform a forensics analysis of the memory image “is7.elf” and gather the following forensic artifacts;
Memory image “is7.elf”: Sha1 hash value: “f66dc5e898d3edf1013c86d706813071147f6ae6”
Forensics Analysis

Hash Verification:

```
[AngryBird:is7 Dilanka$ shasum 1 is7.elf
 shasum: 1:
 f66dc5e898d3edf1013c86d706813071147f6ae6  is7.elf
 AngryBird:is7 Dilanka$
```

Used tools:

1. Volatility
2. https://packetstormsecurity.com
3. https://www.virustotal.com
4. AVG Antivirus Software

- System Information
  - Operating System name and version

    Command : Imageinfo

    For a high level summary of the memory sample you're analyzing, use the imageinfo command. Most often this command is used to identify the operating system, service pack, and hardware architecture (32 or 64 bit)

```
[AngryBird:is7 Dilanka$ vol.py -f is7.elf imageinfo
 Volatility Foundation Volatility Framework 2.5
 INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : OSXPmemELF (Unnamed AS)
                     AS Layer3 : FileAddressSpace (/Documents/MIS/shared_between_vms/mini_projects/19-Jan-2019/is7/is7.elf)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82972c28L
          Number of Processors : 1
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0x82973c00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2019-01-18 12:02:09 UTC+0000
     Image local date and time : 2019-01-18 17:32:09 +0530
[AngryBird:is7 Dilanka$
```

Using suggested profiles:

```
[AngryBird:is7 Dilanka$ vol.py -f is7.elf --profile=Win7SP0x86 kdbgscan
Volatility Foundation Volatility Framework 2.5
**************************************************
Instantiating KDBG using: Kernel AS Win7SP0x86 (6.1.7600 32bit)
Offset (V)                    : 0x82972c28
Offset (P)                    : 0x2972c28
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win7SP1x86
Version64                     : 0x82972c00 (Major: 15, Minor: 7600)
Service Pack (CmNtCSDVersion) : 0
Build string (NtBuildLab)     : 7600.17795.x86fre.win7_gdr.15031
PsActiveProcessHead           : 0x8298aea8 (55 processes)
PsLoadedModuleList            : 0x82992810 (143 modules)
KernelBase                    : 0x8284a000 (Matches MZ: True)
Major (OptionalHeader)        : 6
Minor (OptionalHeader)        : 1
KPCR                          : 0x82973c00 (CPU 0)

**************************************************
Instantiating KDBG using: Kernel AS Win7SP0x86 (6.1.7600 32bit)
Offset (V)                    : 0x82972c28
Offset (P)                    : 0x2972c28
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win7SP0x86
Version64                     : 0x82972c00 (Major: 15, Minor: 7600)
Service Pack (CmNtCSDVersion) : 0
Build string (NtBuildLab)     : 7600.17795.x86fre.win7_gdr.15031
PsActiveProcessHead           : 0x8298aea8 (55 processes)
PsLoadedModuleList            : 0x82992810 (143 modules)
KernelBase                    : 0x8284a000 (Matches MZ: True)
Major (OptionalHeader)        : 6
Minor (OptionalHeader)        : 1
KPCR                          : 0x82973c00 (CPU 0)
```

```
[AngryBird:is7 Dilanka$ vol.py -f is7.elf --profile=Win7SP1x86 kdbgscan
Volatility Foundation Volatility Framework 2.5
**************************************************
Instantiating KDBG using: Kernel AS Win7SP1x86 (6.1.7601 32bit)
Offset (V)                    : 0x82972c28
Offset (P)                    : 0x2972c28
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win7SP1x86
Version64                     : 0x82972c00 (Major: 15, Minor: 7600)
Service Pack (CmNtCSDVersion) : 0
Build string (NtBuildLab)     : 7600.17795.x86fre.win7_gdr.15031
PsActiveProcessHead           : 0x8298aea8 (55 processes)
PsLoadedModuleList            : 0x82992810 (143 modules)
KernelBase                    : 0x8284a000 (Matches MZ: True)
Major (OptionalHeader)        : 6
Minor (OptionalHeader)        : 1
KPCR                          : 0x82973c00 (CPU 0)

**************************************************
Instantiating KDBG using: Kernel AS Win7SP1x86 (6.1.7601 32bit)
Offset (V)                    : 0x82972c28
Offset (P)                    : 0x2972c28
KDBG owner tag check          : True
Profile suggestion (KDBGHeader): Win7SP0x86
Version64                     : 0x82972c00 (Major: 15, Minor: 7600)
Service Pack (CmNtCSDVersion) : 0
Build string (NtBuildLab)     : 7600.17795.x86fre.win7_gdr.15031
PsActiveProcessHead           : 0x8298aea8 (55 processes)
PsLoadedModuleList            : 0x82992810 (143 modules)
KernelBase                    : 0x8284a000 (Matches MZ: True)
Major (OptionalHeader)        : 6
Minor (OptionalHeader)        : 1
KPCR                          : 0x82973c00 (CPU 0)
```

- User information

  By scanning registry hives using hivelist command. We can list down all the hives with ntuser.dat file related paths, then identify user account.

  User account is mis-win7

  Using profile : Win7SP0x86

```
[AngryBird:is7 Dilanka$ vol.py -f is7.elf --profile=Win7SP0x86 hivelist
Volatility Foundation Volatility Framework 2.5
Virtual    Physical   Name
---------- ---------- ----
0x89e16788 0x27b73788 \SystemRoot\System32\Config\SECURITY
0x89e95008 0x26e76008 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x89ecc9d0 0x260c29d0 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x8a6379d0 0x2bfb79d0 \Device\HarddiskVolume1\Boot\BCD
0x8a7f6008 0x2c148008 \SystemRoot\System32\Config\SOFTWARE
0x9c094008 0x7641a008 \??\C:\Users\mis-win7\ntuser.dat
0x9cd9a008 0x1c05f008 \??\C:\Users\mis-win7\AppData\Local\Microsoft\Windows\UsrClass.dat
0xa4b5b9d0 0x259729d0 \??\C:\System Volume Information\Syscache.hve
0x8960c800 0x2d643800 [no name]
0x8961a2c8 0x2d68f2c8 \REGISTRY\MACHINE\SYSTEM
0x896428d8 0x2d5b98d8 \REGISTRY\MACHINE\HARDWARE
0x896d19d0 0x033279d0 \SystemRoot\System32\Config\DEFAULT
0x89e043b0 0x271c53b0 \SystemRoot\System32\Config\SAM
```

Using profile: Win7SP1x86

```
[AngryBird:is7 Dilanka$ vol.py -f is7.elf --profile=Win7SP1x86 hivelist
Volatility Foundation Volatility Framework 2.5
Virtual    Physical   Name
---------- ---------- ----
0x89e16788 0x27b73788 \SystemRoot\System32\Config\SECURITY
0x89e95008 0x26e76008 \??\C:\Windows\ServiceProfiles\LocalService\NTUSER.DAT
0x89ecc9d0 0x260c29d0 \??\C:\Windows\ServiceProfiles\NetworkService\NTUSER.DAT
0x8a6379d0 0x2bfb79d0 \Device\HarddiskVolume1\Boot\BCD
0x8a7f6008 0x2c148008 \SystemRoot\System32\Config\SOFTWARE
0x9c094008 0x7641a008 \??\C:\Users\mis-win7\ntuser.dat
0x9cd9a008 0x1c05f008 \??\C:\Users\mis-win7\AppData\Local\Microsoft\Windows\UsrClass.dat
0xa4b5b9d0 0x259729d0 \??\C:\System Volume Information\Syscache.hve
0x8960c800 0x2d643800 [no name]
0x8961a2c8 0x2d68f2c8 \REGISTRY\MACHINE\SYSTEM
0x896428d8 0x2d5b98d8 \REGISTRY\MACHINE\HARDWARE
0x896d19d0 0x033279d0 \SystemRoot\System32\Config\DEFAULT
0x89e043b0 0x271c53b0 \SystemRoot\System32\Config\SAM
```

- Start and End time

  Start time can be consider as system process start time.

```
Volatility Foundation Volatility Framework 2.5
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x8483c968 System                    4      0     82      569 ------      0 2019-01-17 09:16:33 UTC+0000
0x85822428 smss.exe                272      4      2       29 ------      0 2019-01-17 09:16:33 UTC+0000
0x85eebd40 smss.exe                340    272      0 --------      0      0 2019-01-17 09:16:39 UTC+0000   2019-01-17 09:16:43 UTC+0000
```

Since this is memory dump and taken from the running computer, image created time can be considered as end time.

```
AngryBird:is7 Dilanka$ vol.py -f is7.elf imageinfo
Volatility Foundation Volatility Framework 2.5
INFO    : volatility.debug    : Determining profile based on KDBG search...
          Suggested Profile(s) : Win7SP0x86, Win7SP1x86
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : OSXPmemELF (Unnamed AS)
                     AS Layer3 : FileAddressSpace (/Documents/MIS/shared_between_vms/mini_projects/19-Jan-2019/is7/is7.elf)
                      PAE type : PAE
                           DTB : 0x185000L
                          KDBG : 0x82972c28L
          Number of Processors : 1
     Image Type (Service Pack) : 0
                KPCR for CPU 0 : 0x82973c00L
             KUSER_SHARED_DATA : 0xffdf0000L
           Image date and time : 2019-01-18 12:02:09 UTC+0000
     Image local date and time : 2019-01-18 17:32:09 +0530
AngryBird:is7 Dilanka$
```

Processes

- Processes List

  With profile: Win7SP1x86

```
AngryBird:is7 Dilanka$ vol.py -f is7.elf --profile=Win7SP1x86 pslist
Volatility Foundation Volatility Framework 2.5
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x8483c968 System                    4      0     82      569 ------      0 2019-01-17 09:16:33 UTC+0000
0x85822428 smss.exe                272      4      2       29 ------      0 2019-01-17 09:16:33 UTC+0000
0x85eebd40 smss.exe                340    272      0 --------      0      0 2019-01-17 09:16:39 UTC+0000   2019-01-17 09:16:43 UTC+0000
0x85ee9d40 csrss.exe               348    340      9      416      0      0 2019-01-17 09:16:41 UTC+0000
0x85f35c08 smss.exe                376    272      0 --------      1      0 2019-01-17 09:16:43 UTC+0000   2019-01-17 09:16:44 UTC+0000
0x848a4750 wininit.exe             384    340      3       76      0      0 2019-01-17 09:16:43 UTC+0000
0x85fc2d40 csrss.exe               392    376      9      449      1      0 2019-01-17 09:16:43 UTC+0000
0x85f52d40 winlogon.exe            432    376      5      116      1      0 2019-01-17 09:16:44 UTC+0000
0x85f7f9d8 services.exe            480    384      8      195      0      0 2019-01-17 09:16:45 UTC+0000
0x85f8f030 lsass.exe               488    384      7      713      0      0 2019-01-17 09:16:45 UTC+0000
0x85e79180 lsm.exe                 496    384     10      153      0      0 2019-01-17 09:16:46 UTC+0000
0x848ddaf8 svchost.exe             608    480     11      357      0      0 2019-01-17 09:16:47 UTC+0000
0x8612ed40 VBoxService.ex          668    480     12      106      0      0 2019-01-17 09:16:47 UTC+0000
0x86142480 svchost.exe             732    480      6      249      0      0 2019-01-17 09:16:49 UTC+0000
0x8615bbd0 svchost.exe             768    480     23      590      0      0 2019-01-17 09:16:50 UTC+0000
0x861a4030 svchost.exe             892    480     29      600      0      0 2019-01-17 09:16:51 UTC+0000
0x861b2988 svchost.exe             932    480     46     1192      0      0 2019-01-17 09:16:51 UTC+0000
0x861d7af8 svchost.exe            1072    480     18      449      0      0 2019-01-17 09:16:54 UTC+0000
0x86206908 svchost.exe            1176    480     20      628      0      0 2019-01-17 09:16:55 UTC+0000
0x8623a030 spoolsv.exe            1272    480     13      288      0      0 2019-01-17 09:16:55 UTC+0000
0x8623e498 svchost.exe            1300    480     20      336      0      0 2019-01-17 09:16:55 UTC+0000
0x85de5150 svchost.exe            1432    480     19      257      0      0 2019-01-17 09:16:58 UTC+0000
0x85e78030 userinit.exe            492    432      0 --------      1      0 2019-01-17 09:17:24 UTC+0000   2019-01-17 09:17:47 UTC+0000
0x85e775d8 dwm.exe                 624    892      5       98      1      0 2019-01-17 09:17:24 UTC+0000
0x8639ebb8 explorer.exe            928    492     68     1418      1      0 2019-01-17 09:17:24 UTC+0000
0x863d0d40 taskhost.exe           1404    480     15      228      1      0 2019-01-17 09:17:24 UTC+0000
0x8641f030 VBoxTray.exe           1884    928      9      119      1      0 2019-01-17 09:17:24 UTC+0000
0x85ec8458 SearchIndexer.         1320    480     13      659      0      0 2019-01-17 09:17:30 UTC+0000
0x86461198 svchost.exe            2068    480      9      352      0      0 2019-01-17 09:17:32 UTC+0000
0x85e53538 chrome.exe              944    928     36     1258      1      0 2019-01-18 11:09:59 UTC+0000
0x84d0f460 chrome.exe             1696    944      7      122      1      0 2019-01-18 11:09:59 UTC+0000
0x86415d40 chrome.exe             2840    944      3       87      1      0 2019-01-18 11:10:00 UTC+0000
0x84e9aab8 chrome.exe             3432    944      9      225      1      0 2019-01-18 11:10:08 UTC+0000
0x84de8030 chrome.exe             3256    944     16      258      1      0 2019-01-18 11:20:31 UTC+0000
0x8621e4e8 chrome.exe             1540    944     13      175      1      0 2019-01-18 11:20:40 UTC+0000
0x84ee4870 chrome.exe             1020    944     15      197      1      0 2019-01-18 11:21:28 UTC+0000
0x84ff7a48 WinRAR.exe             2000    928      3      129      1      0 2019-01-18 11:22:52 UTC+0000
0x84d91740 noixre.exe             3100   3568      0 --------      1      0 2019-01-18 11:35:23 UTC+0000   2019-01-18 11:35:24 UTC+0000
0x84988030 taskmgr.exe            2252    928      7      133      1      0 2019-01-18 11:35:31 UTC+0000
0x84f1aba0 ExeBinder.exe          2448    928      0 --------      1      0 2019-01-18 11:36:59 UTC+0000   2019-01-18 11:36:59 UTC+0000
0x84de6d40 svchost.exe            2772   2448      6      116      1      0 2019-01-18 11:36:59 UTC+0000
0x84f5d658 taskhost.exe           1672    480      7      208      1      0 2019-01-18 11:37:24 UTC+0000
0x85010618 svchost.exe            2708    480      2       23      0      0 2019-01-18 11:39:06 UTC+0000
0x8502bd40 sysdati.exe            2556    480      5       75      0      0 2019-01-18 11:39:56 UTC+0000
0x85048568 chrome.exe             3244    944     15      222      1      0 2019-01-18 12:00:21 UTC+0000
0x84f90be8 chrome.exe             2976    944     15      188      1      0 2019-01-18 12:00:34 UTC+0000
0x84fbc030 SearchProtocol         2196   1320      6      313      0      0 2019-01-18 12:00:35 UTC+0000
0x84bdfc88 SearchFilterHo         3092   1320      4       95      0      0 2019-01-18 12:00:35 UTC+0000
0x85014850 audiodg.exe            2480    768      6      128      0      0 2019-01-18 12:00:57 UTC+0000
0x84e1a030 mmcrack.exe            1588    928      0 --------      1      0 2019-01-18 12:01:03 UTC+0000   2019-01-18 12:01:09 UTC+0000
0x85057d40 csrstub.exe            4076   1588      1       10      1      0 2019-01-18 12:01:09 UTC+0000
0x84de8658 conhost.exe            1340    392      1       33      1      0 2019-01-18 12:01:09 UTC+0000
0x8501ad40 ntvdm.exe              1508   4076      4       59      1      0 2019-01-18 12:01:09 UTC+0000
0x8502b030 conhost.exe            3856    392      2       51      1      0 2019-01-18 12:01:09 UTC+0000
0x85009a48 WINI.EXE               3660   1508      7      130      1      0 2019-01-18 12:01:11 UTC+0000
AngryBird:is7 Dilanka$
```

With profile: Win7SP0x86

```
AngryBird:is7 Dilanka$ vol.py -f is7.elf --profile=Win7SP0x86 pslist
Volatility Foundation Volatility Framework 2.5
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x8483c968 System                    4      0     82      569 ------      0 2019-01-17 09:16:33 UTC+0000
0x85822428 smss.exe                272      4      2       29 ------      0 2019-01-17 09:16:33 UTC+0000
0x85eebd40 smss.exe                340    272      0 --------      0      0 2019-01-17 09:16:39 UTC+0000   2019-01-17 09:16:43 UTC+0000
0x85ee9d40 csrss.exe               348    340      9      416      0      0 2019-01-17 09:16:41 UTC+0000
0x85f35c08 smss.exe                376    272      0 --------      1      0 2019-01-17 09:16:43 UTC+0000   2019-01-17 09:16:44 UTC+0000
0x848a4750 wininit.exe             384    340      3       76      0      0 2019-01-17 09:16:43 UTC+0000
0x85fc2d40 csrss.exe               392    376      9      449      1      0 2019-01-17 09:16:43 UTC+0000
0x85f52d40 winlogon.exe            432    376      5      116      1      0 2019-01-17 09:16:44 UTC+0000
0x85f7f9d8 services.exe            480    384      8      195      0      0 2019-01-17 09:16:45 UTC+0000
0x85f8f030 lsass.exe               488    384      7      713      0      0 2019-01-17 09:16:45 UTC+0000
0x85e79180 lsm.exe                 496    384     10      153      0      0 2019-01-17 09:16:46 UTC+0000
0x848ddaf8 svchost.exe             608    480     11      357      0      0 2019-01-17 09:16:47 UTC+0000
0x8612ed40 VBoxService.ex          668    480     12      106      0      0 2019-01-17 09:16:47 UTC+0000
0x86142480 svchost.exe             732    480      6      249      0      0 2019-01-17 09:16:49 UTC+0000
0x8615bbd0 svchost.exe             768    480     23      590      0      0 2019-01-17 09:16:50 UTC+0000
0x861a4030 svchost.exe             892    480     29      600      0      0 2019-01-17 09:16:51 UTC+0000
0x861b2988 svchost.exe             932    480     46     1192      0      0 2019-01-17 09:16:51 UTC+0000
0x861d7af8 svchost.exe            1072    480     18      449      0      0 2019-01-17 09:16:54 UTC+0000
0x86206908 svchost.exe            1176    480     20      628      0      0 2019-01-17 09:16:55 UTC+0000
0x8623a030 spoolsv.exe            1272    480     13      288      0      0 2019-01-17 09:16:55 UTC+0000
0x8623e498 svchost.exe            1300    480     20      336      0      0 2019-01-17 09:16:55 UTC+0000
0x85de5150 svchost.exe            1432    480     19      257      0      0 2019-01-17 09:16:58 UTC+0000
0x85e78030 userinit.exe            492    432      0 --------      1      0 2019-01-17 09:17:24 UTC+0000   2019-01-17 09:17:47 UTC+0000
0x85e775d8 dwm.exe                 624    892      5       98      1      0 2019-01-17 09:17:24 UTC+0000
0x8639ebb8 explorer.exe            928    492     68     1418      1      0 2019-01-17 09:17:24 UTC+0000
0x863d0d40 taskhost.exe           1404    480     15      228      1      0 2019-01-17 09:17:24 UTC+0000
0x8641f030 VBoxTray.exe           1884    928      9      119      1      0 2019-01-17 09:17:24 UTC+0000
0x85ec8458 SearchIndexer.         1320    480     13      659      0      0 2019-01-17 09:17:30 UTC+0000
0x86461198 svchost.exe            2068    480      9      352      0      0 2019-01-17 09:17:32 UTC+0000
0x85e53538 chrome.exe              944    928     36     1258      1      0 2019-01-18 11:09:59 UTC+0000
0x84d0f460 chrome.exe             1696    944      7      122      1      0 2019-01-18 11:09:59 UTC+0000
0x86415d40 chrome.exe             2840    944      3       87      1      0 2019-01-18 11:10:00 UTC+0000
0x84e9aab8 chrome.exe             3432    944      9      225      1      0 2019-01-18 11:10:08 UTC+0000
0x84de8030 chrome.exe             3256    944     16      258      1      0 2019-01-18 11:20:31 UTC+0000
0x8621e4e8 chrome.exe             1540    944     13      175      1      0 2019-01-18 11:20:40 UTC+0000
0x84ee4870 chrome.exe             1020    944     15      197      1      0 2019-01-18 11:21:28 UTC+0000
0x84ff7a48 WinRAR.exe             2000    928      3      129      1      0 2019-01-18 11:22:52 UTC+0000
0x84d91740 noixre.exe             3100   3568      0 --------      1      0 2019-01-18 11:35:23 UTC+0000   2019-01-18 11:35:24 UTC+0000
0x84988030 taskmgr.exe            2252    928      7      133      1      0 2019-01-18 11:35:31 UTC+0000
0x84f1aba0 ExeBinder.exe          2448    928      0 --------      1      0 2019-01-18 11:36:59 UTC+0000   2019-01-18 11:36:59 UTC+0000
0x84de6d40 svchost.exe            2772   2448      6      116      1      0 2019-01-18 11:36:59 UTC+0000
0x84f5d658 taskhost.exe           1672    480      7      208      1      0 2019-01-18 11:37:24 UTC+0000
0x85010618 svchost.exe            2708    480      2       23      0      0 2019-01-18 11:39:06 UTC+0000
0x8502bd40 sysdati.exe            2556    480      5       75      0      0 2019-01-18 11:39:56 UTC+0000
0x85048568 chrome.exe             3244    944     15      222      1      0 2019-01-18 12:00:21 UTC+0000
0x84f90be8 chrome.exe             2976    944     15      188      1      0 2019-01-18 12:00:34 UTC+0000
0x84fbc030 SearchProtocol         2196   1320      6      313      0      0 2019-01-18 12:00:35 UTC+0000
0x84bdfc88 SearchFilterHo         3092   1320      4       95      0      0 2019-01-18 12:00:35 UTC+0000
0x85014850 audiodg.exe            2480    768      6      128      0      0 2019-01-18 12:00:57 UTC+0000
0x84e1a030 mmcrack.exe            1588    928      0 --------      1      0 2019-01-18 12:01:03 UTC+0000   2019-01-18 12:01:09 UTC+0000
0x85057d40 csrstub.exe            4076   1588      1       10      1      0 2019-01-18 12:01:09 UTC+0000
0x84de8658 conhost.exe            1340    392      1       33      1      0 2019-01-18 12:01:09 UTC+0000
0x8501ad40 ntvdm.exe              1508   4076      4       59      1      0 2019-01-18 12:01:09 UTC+0000
0x8502b030 conhost.exe            3856    392      2       51      1      0 2019-01-18 12:01:09 UTC+0000
0x85009a48 WINI.EXE               3660   1508      7      130      1      0 2019-01-18 12:01:11 UTC+0000
AngryBird:is7 Dilanka$
```

- Processes tree

  With profile: Win7SP0x86

```
[AngryBird:is7 Dilanka$ vol.py -f is7.elf --profile=Win7SP0x86 pstree
Volatility Foundation Volatility Framework 2.5
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x8483c968:System                                      4      0     82    569 2019-01-17 09:16:33 UTC+0000
. 0x85822428:smss.exe                                 272      4      2     29 2019-01-17 09:16:33 UTC+0000
.. 0x85eebd40:smss.exe                                340    272      0 ------ 2019-01-17 09:16:39 UTC+0000
... 0x848a4750:wininit.exe                            384    340      3     76 2019-01-17 09:16:43 UTC+0000
.... 0x85f7f9d8:services.exe                          480    384      8    195 2019-01-17 09:16:45 UTC+0000
..... 0x8615bbd0:svchost.exe                          768    480     23    590 2019-01-17 09:16:50 UTC+0000
...... 0x85014850:audiodg.exe                        2480    768      6    128 2019-01-18 12:00:57 UTC+0000
..... 0x86206908:svchost.exe                         1176    480     20    628 2019-01-17 09:16:55 UTC+0000
..... 0x8623e498:svchost.exe                         1300    480     20    336 2019-01-17 09:16:55 UTC+0000
..... 0x85de5150:svchost.exe                         1432    480     19    257 2019-01-17 09:16:58 UTC+0000
..... 0x8612ed40:VBoxService.ex                       668    480     12    106 2019-01-17 09:16:47 UTC+0000
..... 0x861d7af8:svchost.exe                         1072    480     18    449 2019-01-17 09:16:54 UTC+0000
..... 0x861b2988:svchost.exe                          932    480     46   1192 2019-01-17 09:16:51 UTC+0000
..... 0x85ec8458:SearchIndexer.                      1320    480     13    659 2019-01-17 09:17:30 UTC+0000
...... 0x84fbc030:SearchProtocol                     2196   1320      6    313 2019-01-18 12:00:35 UTC+0000
...... 0x84bdfc88:SearchFilterHo                     3092   1320      4     95 2019-01-18 12:00:35 UTC+0000
..... 0x84f5d658:taskhost.exe                        1672    480      7    208 2019-01-18 11:37:24 UTC+0000
..... 0x85010618:svchost.exe                         2708    480      2     23 2019-01-18 11:39:06 UTC+0000
..... 0x848ddaf8:svchost.exe                          608    480     11    357 2019-01-17 09:16:47 UTC+0000
..... 0x8623a030:spoolsv.exe                         1272    480     13    288 2019-01-17 09:16:55 UTC+0000
..... 0x86142480:svchost.exe                          732    480      6    249 2019-01-17 09:16:49 UTC+0000
..... 0x8502bd40:sysdati.exe                         2556    480      5     75 2019-01-18 11:39:56 UTC+0000
..... 0x863d0d40:taskhost.exe                        1404    480     15    228 2019-01-17 09:17:24 UTC+0000
..... 0x86461198:svchost.exe                         2068    480      9    352 2019-01-17 09:17:32 UTC+0000
..... 0x861a4030:svchost.exe                          892    480     29    600 2019-01-17 09:16:51 UTC+0000
...... 0x85e775d8:dwm.exe                             624    892      5     98 2019-01-17 09:17:24 UTC+0000
.... 0x85f8f030:lsass.exe                             488    384      7    713 2019-01-17 09:16:45 UTC+0000
.... 0x85e79180:lsm.exe                               496    384     10    153 2019-01-17 09:16:46 UTC+0000
... 0x85ee9d40:csrss.exe                              348    340      9    416 2019-01-17 09:16:41 UTC+0000
 0x85f35c08:smss.exe                                  376    272      0 ------ 2019-01-17 09:16:43 UTC+0000
... 0x85fc2d40:csrss.exe                              392    376      9    449 2019-01-17 09:16:43 UTC+0000
.... 0x84de8658:conhost.exe                          1340    392      1     33 2019-01-18 12:01:09 UTC+0000
.... 0x8502b030:conhost.exe                          3856    392      2     51 2019-01-18 12:01:09 UTC+0000
... 0x85f52d40:winlogon.exe                           432    376      5    116 2019-01-17 09:16:44 UTC+0000
.... 0x85e78030:userinit.exe                          492    432      0 ------ 2019-01-17 09:17:24 UTC+0000
..... 0x8639ebb8:explorer.exe                         928    492     68   1418 2019-01-17 09:17:24 UTC+0000
...... 0x8641f030:VBoxTray.exe                       1884    928      9    119 2019-01-17 09:17:24 UTC+0000
...... 0x85e53538:chrome.exe                          944    928     36   1258 2019-01-18 11:09:59 UTC+0000
....... 0x8621e4e8:chrome.exe                        1540    944     13    175 2019-01-18 11:20:40 UTC+0000
....... 0x84f90be8:chrome.exe                        2976    944     15    188 2019-01-18 12:00:34 UTC+0000
....... 0x85048568:chrome.exe                        3244    944     15    222 2019-01-18 12:00:21 UTC+0000
....... 0x84ee4870:chrome.exe                        1020    944     15    197 2019-01-18 11:21:28 UTC+0000
....... 0x86415d40:chrome.exe                        2840    944      3     87 2019-01-18 11:10:00 UTC+0000
....... 0x84de8030:chrome.exe                        3256    944     16    258 2019-01-18 11:20:31 UTC+0000
....... 0x84e9aab8:chrome.exe                        3432    944      9    225 2019-01-18 11:10:08 UTC+0000
....... 0x84d0f460:chrome.exe                        1696    944      7    122 2019-01-18 11:09:59 UTC+0000
...... 0x84988030:taskmgr.exe                        2252    928      7    133 2019-01-18 11:35:31 UTC+0000
...... 0x84e1a030:mmcrack.exe                        1588    928      0 ------ 2019-01-18 12:01:03 UTC+0000
....... 0x85057d40:csrstub.exe                       4076   1588      1     10 2019-01-18 12:01:09 UTC+0000
........ 0x8501ad40:ntvdm.exe                        1508   4076      4     59 2019-01-18 12:01:09 UTC+0000
......... 0x85009a48:WINI.EXE                        3660   1508      7    130 2019-01-18 12:01:11 UTC+0000
...... 0x84ff7a48:WinRAR.exe                         2000    928      3    129 2019-01-18 11:22:52 UTC+0000
...... 0x84f1aba0:ExeBinder.exe                      2448    928      0 ------ 2019-01-18 11:36:59 UTC+0000
....... 0x84de6d40:svchost.exe                       2772   2448      6    116 2019-01-18 11:36:59 UTC+0000
 0x84d91740:noixre.exe                               3100   3568      0 ------ 2019-01-18 11:35:23 UTC+0000
AngryBird:is7 Dilanka$
```

With profile: Win7SP1x86

```
[AngryBird:is7 Dilanka$ vol.py -f is7.elf --profile=Win7SP1x86 pstree
Volatility Foundation Volatility Framework 2.5
Name                                                 Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x8483c968:System                                     4      0     82    569 2019-01-17 09:16:33 UTC+0000
. 0x85822428:smss.exe                                272      4      2     29 2019-01-17 09:16:33 UTC+0000
.. 0x85eebd40:smss.exe                               340    272      0 ------ 2019-01-17 09:16:39 UTC+0000
... 0x848a4750:wininit.exe                           384    340      3     76 2019-01-17 09:16:43 UTC+0000
.... 0x85f7f9d8:services.exe                         480    384      8    195 2019-01-17 09:16:45 UTC+0000
..... 0x8615bbd0:svchost.exe                         768    480     23    590 2019-01-17 09:16:50 UTC+0000
...... 0x85014850:audiodg.exe                       2480    768      6    128 2019-01-18 12:00:57 UTC+0000
..... 0x86206908:svchost.exe                        1176    480     20    628 2019-01-17 09:16:55 UTC+0000
..... 0x8623e498:svchost.exe                        1300    480     20    336 2019-01-17 09:16:55 UTC+0000
..... 0x85de5150:svchost.exe                        1432    480     19    257 2019-01-17 09:16:58 UTC+0000
..... 0x8612ed40:VBoxService.ex                      668    480     12    106 2019-01-17 09:16:47 UTC+0000
..... 0x861d7af8:svchost.exe                        1072    480     18    449 2019-01-17 09:16:54 UTC+0000
..... 0x861b2988:svchost.exe                         932    480     46   1192 2019-01-17 09:16:51 UTC+0000
..... 0x85ec8458:SearchIndexer.                     1320    480     13    659 2019-01-17 09:17:30 UTC+0000
...... 0x84fbc030:SearchProtocol                    2196   1320      6    313 2019-01-18 12:00:35 UTC+0000
...... 0x84bdfc88:SearchFilterHo                    3092   1320      4     95 2019-01-18 12:00:35 UTC+0000
..... 0x84f5d658:taskhost.exe                       1672    480      7    208 2019-01-18 11:37:24 UTC+0000
..... 0x85010618:svchost.exe                        2708    480      2     23 2019-01-18 11:39:06 UTC+0000
..... 0x848ddaf8:svchost.exe                         608    480     11    357 2019-01-17 09:16:47 UTC+0000
..... 0x8623a030:spoolsv.exe                        1272    480     13    288 2019-01-17 09:16:55 UTC+0000
..... 0x86142480:svchost.exe                         732    480      6    249 2019-01-17 09:16:49 UTC+0000
..... 0x8502bd40:sysdati.exe                        2556    480      5     75 2019-01-18 11:39:56 UTC+0000
..... 0x863d0d40:taskhost.exe                       1404    480     15    228 2019-01-17 09:17:24 UTC+0000
..... 0x86461198:svchost.exe                        2068    480      9    352 2019-01-17 09:17:32 UTC+0000
..... 0x861a4030:svchost.exe                         892    480     29    600 2019-01-17 09:16:51 UTC+0000
...... 0x85e775d8:dwm.exe                            624    892      5     98 2019-01-17 09:17:24 UTC+0000
.... 0x85f8f030:lsass.exe                            488    384      7    713 2019-01-17 09:16:45 UTC+0000
.... 0x85e79180:lsm.exe                              496    384     10    153 2019-01-17 09:16:46 UTC+0000
... 0x85ee9d40:csrss.exe                             348    340      9    416 2019-01-17 09:16:41 UTC+0000
.. 0x85f35c08:smss.exe                               376    272      0 ------ 2019-01-17 09:16:43 UTC+0000
... 0x85fc2d40:csrss.exe                             392    376      9    449 2019-01-17 09:16:43 UTC+0000
.... 0x84de8658:conhost.exe                         1340    392      1     33 2019-01-18 12:01:09 UTC+0000
.... 0x8502b030:conhost.exe                         3856    392      2     51 2019-01-18 12:01:09 UTC+0000
... 0x85f52d40:winlogon.exe                          432    376      5    116 2019-01-17 09:16:44 UTC+0000
.... 0x85e78030:userinit.exe                         492    432      0 ------ 2019-01-17 09:17:24 UTC+0000
..... 0x8639ebb8:explorer.exe                        928    492     68   1418 2019-01-17 09:17:24 UTC+0000
...... 0x8641f030:VBoxTray.exe                      1884    928      9    119 2019-01-17 09:17:24 UTC+0000
...... 0x85e53538:chrome.exe                         944    928     36   1258 2019-01-18 11:09:59 UTC+0000
....... 0x8621e4e8:chrome.exe                       1540    944     13    175 2019-01-18 11:20:40 UTC+0000
....... 0x84f90be8:chrome.exe                       2976    944     15    188 2019-01-18 12:00:34 UTC+0000
....... 0x85048568:chrome.exe                       3244    944     15    222 2019-01-18 12:00:21 UTC+0000
....... 0x84ee4870:chrome.exe                       1020    944     15    197 2019-01-18 11:21:28 UTC+0000
....... 0x86415d40:chrome.exe                       2840    944      3     87 2019-01-18 11:10:00 UTC+0000
....... 0x84de8030:chrome.exe                       3256    944     16    258 2019-01-18 11:20:31 UTC+0000
....... 0x84e9aab8:chrome.exe                       3432    944      9    225 2019-01-18 11:10:08 UTC+0000
....... 0x84d0f460:chrome.exe                       1696    944      7    122 2019-01-18 11:09:59 UTC+0000
...... 0x84988030:taskmgr.exe                       2252    928      7    133 2019-01-18 11:35:31 UTC+0000
...... 0x84e1a030:mmcrack.exe                       1588    928      0 ------ 2019-01-18 12:01:03 UTC+0000
....... 0x85057d40:csrstub.exe                      4076   1588      1     10 2019-01-18 12:01:09 UTC+0000
........ 0x8501ad40:ntvdm.exe                       1508   4076      4     59 2019-01-18 12:01:09 UTC+0000
......... 0x85009a48:WINI.EXE                       3660   1508      7    130 2019-01-18 12:01:11 UTC+0000
...... 0x84ff7a48:WinRAR.exe                        2000    928      3    129 2019-01-18 11:22:52 UTC+0000
...... 0x84f1aba0:ExeBinder.exe                     2448    928      0 ------ 2019-01-18 11:36:59 UTC+0000
....... 0x84de6d40:svchost.exe                      2772   2448      6    116 2019-01-18 11:36:59 UTC+0000
 0x84d91740:noixre.exe                              3100   3568      0 ------ 2019-01-18 11:35:23 UTC+0000
AngryBird:is7 Dilanka$
```

- Processes start and end time

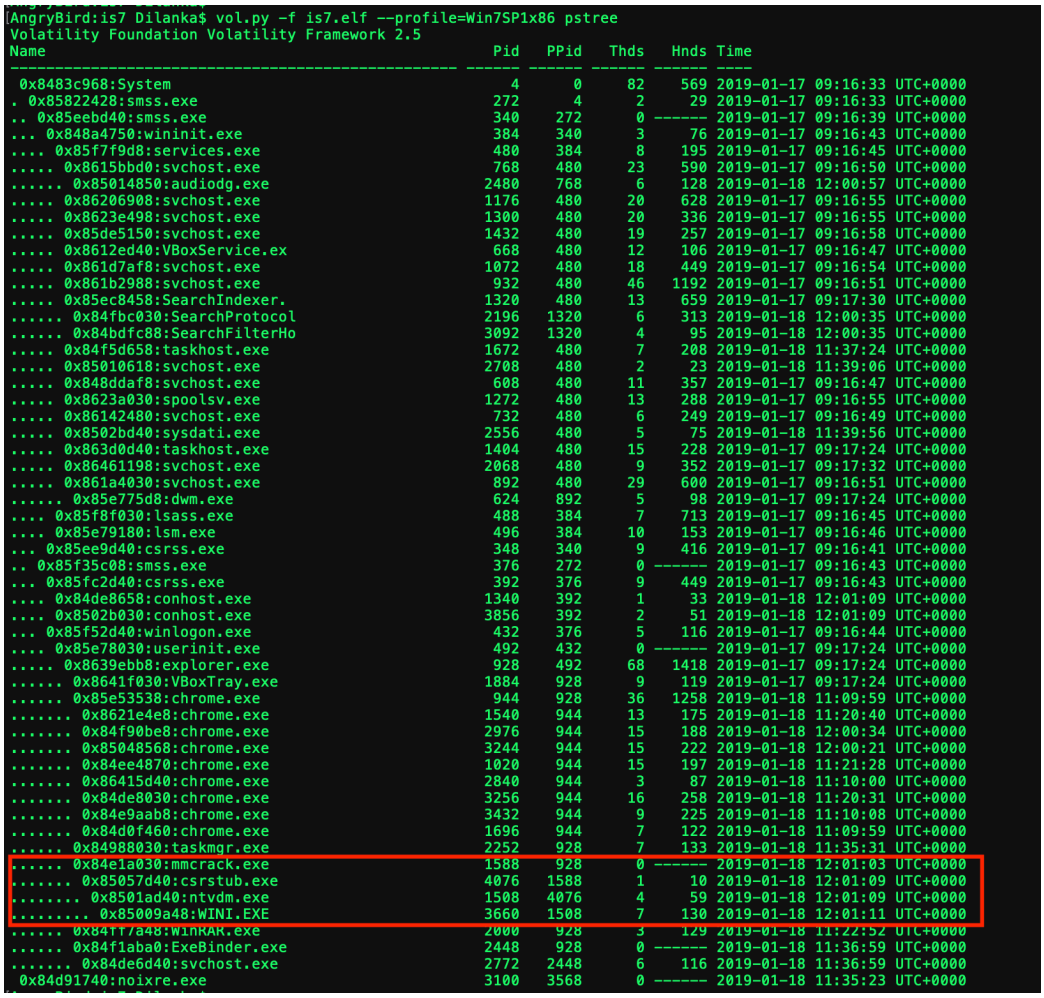
  For both profiles: most processes don't have end time according to the pslist command generated report. So here are the processes have start and end time.

  Note: Extracted all the processes to text editor and filtered.

```
AngryBird:is7 Dilanka$ vol.py -f is7.elf --profile=Win7SP1x86 pslist
Volatility Foundation Volatility Framework 2.5
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x85eebd40 smss.exe                340    272      0 --------      0      0 2019-01-17 09:16:39 UTC+0000   2019-01-17 09:16:43 UTC+0000

0x85f35c08 smss.exe                376    272      0 --------      1      0 2019-01-17 09:16:43 UTC+0000   2019-01-17 09:16:44 UTC+0000
0x85e78030 userinit.exe            492    432      0 --------      1      0 2019-01-17 09:17:24 UTC+0000   2019-01-17 09:17:47 UTC+0000
0x84d91740 noixre.exe             3100   3568      0 --------      1      0 2019-01-18 11:35:23 UTC+0000   2019-01-18 11:35:24 UTC+0000
0x84f1aba0 ExeBinder.exe          2448    928      0 --------      1      0 2019-01-18 11:36:59 UTC+0000   2019-01-18 11:36:59 UTC+0000
0x84e1a030 mmcrack.exe            1588    928      0 --------      1      0 2019-01-18 12:01:03 UTC+0000   2019-01-18 12:01:09 UTC+0000

AngryBird:is7 Dilanka$
AngryBird:is7 Dilanka$ vol.py -f is7.elf --profile=Win7SP0x86 pslist
Volatility Foundation Volatility Framework 2.5
Offset(V)  Name                    PID   PPID   Thds     Hnds   Sess  Wow64 Start                          Exit
---------- -------------------- ------ ------ ------ -------- ------ ------ ------------------------------ ------------------------------
0x85eebd40 smss.exe                340    272      0 --------      0      0 2019-01-17 09:16:39 UTC+0000   2019-01-17 09:16:43 UTC+0000
0x85f35c08 smss.exe                376    272      0 --------      1      0 2019-01-17 09:16:43 UTC+0000   2019-01-17 09:16:44 UTC+0000
0x85e78030 userinit.exe            492    432      0 --------      1      0 2019-01-17 09:17:24 UTC+0000   2019-01-17 09:17:47 UTC+0000
0x84f1aba0 ExeBinder.exe          2448    928      0 --------      1      0 2019-01-18 11:36:59 UTC+0000   2019-01-18 11:36:59 UTC+0000
0x84e1a030 mmcrack.exe            1588    928      0 --------      1      0 2019-01-18 12:01:03 UTC+0000   2019-01-18 12:01:09 UTC+0000

AngryBird:is7 Dilanka$
AngryBird:is7 Dilanka$ vol.py -f is7.elf --profile=Win7SP0x86 pstree
```

- Malicious activities
    - Which processes was most likely responsible for the exploit?

      According to the process tree, suspect the below highlighted process and sub processes after that. So suspected activity starting point is mmcrack.exe. So I suspect that user opened the crack file which may carry the malware or trojan object.



```
[AngryBird:is7 Dilanka$ vol.py -f is7.elf --profile=Win7SP1x86 pstree
Volatility Foundation Volatility Framework 2.5
Name                                                  Pid   PPid   Thds   Hnds Time
-------------------------------------------------- ------ ------ ------ ------ ----
 0x8483c968:System                                      4      0     82    569 2019-01-17 09:16:33 UTC+0000
. 0x85822428:smss.exe                                 272      4      2     29 2019-01-17 09:16:33 UTC+0000
.. 0x85eebd40:smss.exe                                340    272      0 ------ 2019-01-17 09:16:39 UTC+0000
... 0x848a4750:wininit.exe                            384    340      3     76 2019-01-17 09:16:43 UTC+0000
.... 0x85f7f9d8:services.exe                          480    384      8    195 2019-01-17 09:16:45 UTC+0000
..... 0x8615bbd0:svchost.exe                          768    480     23    590 2019-01-17 09:16:50 UTC+0000
...... 0x85014850:audiodg.exe                        2480    768      6    128 2019-01-18 12:00:57 UTC+0000
..... 0x86206908:svchost.exe                         1176    480     20    628 2019-01-17 09:16:55 UTC+0000
..... 0x8623e498:svchost.exe                         1300    480     20    336 2019-01-17 09:16:55 UTC+0000
..... 0x85de5150:svchost.exe                         1432    480     19    257 2019-01-17 09:16:58 UTC+0000
..... 0x8612ed40:VBoxService.ex                       668    480     12    106 2019-01-17 09:16:47 UTC+0000
..... 0x861d7af8:svchost.exe                         1072    480     18    449 2019-01-17 09:16:54 UTC+0000
..... 0x861b2988:svchost.exe                          932    480     46   1192 2019-01-17 09:16:51 UTC+0000
..... 0x85ec8458:SearchIndexer.                      1320    480     13    659 2019-01-17 09:17:30 UTC+0000
...... 0x84fbc030:SearchProtocol                     2196   1320      6    313 2019-01-18 12:00:35 UTC+0000
...... 0x84bdfc88:SearchFilterHo                     3092   1320      4     95 2019-01-18 12:00:35 UTC+0000
..... 0x84f5d658:taskhost.exe                        1672    480      7    208 2019-01-18 11:37:24 UTC+0000
..... 0x85010618:svchost.exe                         2708    480      2     23 2019-01-18 11:39:06 UTC+0000
..... 0x848ddaf8:svchost.exe                          608    480     11    357 2019-01-17 09:16:47 UTC+0000
..... 0x8623a030:spoolsv.exe                         1272    480     13    288 2019-01-17 09:16:55 UTC+0000
..... 0x86142480:svchost.exe                          732    480      6    249 2019-01-17 09:16:49 UTC+0000
..... 0x8502bd40:sysdati.exe                         2556    480      5     75 2019-01-18 11:39:56 UTC+0000
..... 0x863d0d40:taskhost.exe                        1404    480     15    228 2019-01-17 09:17:24 UTC+0000
..... 0x86461198:svchost.exe                         2068    480      9    352 2019-01-17 09:17:32 UTC+0000
..... 0x861a4030:svchost.exe                          892    480     29    600 2019-01-17 09:16:51 UTC+0000
...... 0x85e775d8:dwm.exe                             624    892      5     98 2019-01-17 09:17:24 UTC+0000
.... 0x85f8f030:lsass.exe                             488    384      7    713 2019-01-17 09:16:45 UTC+0000
.... 0x85e79180:lsm.exe                               496    384     10    153 2019-01-17 09:16:46 UTC+0000
... 0x85ee9d40:csrss.exe                              348    340      9    416 2019-01-17 09:16:41 UTC+0000
.. 0x85f35c08:smss.exe                                376    272      0 ------ 2019-01-17 09:16:43 UTC+0000
... 0x85fc2d40:csrss.exe                              392    376      9    449 2019-01-17 09:16:43 UTC+0000
.... 0x84de8658:conhost.exe                          1340    392      1     33 2019-01-18 12:01:09 UTC+0000
.... 0x8502b030:conhost.exe                          3856    392      2     51 2019-01-18 12:01:09 UTC+0000
... 0x85f52d40:winlogon.exe                           432    376      5    116 2019-01-17 09:16:44 UTC+0000
.... 0x85e78030:userinit.exe                          492    432      0 ------ 2019-01-17 09:17:24 UTC+0000
..... 0x8639ebb8:explorer.exe                         928    492     68   1418 2019-01-17 09:17:24 UTC+0000
...... 0x8641f030:VBoxTray.exe                       1884    928      9    119 2019-01-17 09:17:24 UTC+0000
...... 0x85e53538:chrome.exe                          944    928     36   1258 2019-01-18 11:09:59 UTC+0000
....... 0x8621e4e8:chrome.exe                        1540    944     13    175 2019-01-18 11:20:40 UTC+0000
....... 0x84f90be8:chrome.exe                        2976    944     15    188 2019-01-18 12:00:34 UTC+0000
....... 0x85048568:chrome.exe                        3244    944     15    222 2019-01-18 12:00:21 UTC+0000
....... 0x84ee4870:chrome.exe                        1020    944     15    197 2019-01-18 11:21:28 UTC+0000
....... 0x86415d40:chrome.exe                        2840    944      3     87 2019-01-18 11:10:00 UTC+0000
....... 0x84de8030:chrome.exe                        3256    944     16    258 2019-01-18 11:20:31 UTC+0000
....... 0x84e9aab8:chrome.exe                        3432    944      9    225 2019-01-18 11:10:08 UTC+0000
....... 0x84d0f460:chrome.exe                        1696    944      7    122 2019-01-18 11:09:59 UTC+0000
...... 0x84988030:taskmgr.exe                        2252    928      7    133 2019-01-18 11:35:31 UTC+0000
...... 0x84e1a030:mmcrack.exe                        1588    928      0 ------ 2019-01-18 12:01:03 UTC+0000
....... 0x85057d40:csrstub.exe                       4076   1588      1     10 2019-01-18 12:01:09 UTC+0000
........ 0x8501ad40:ntvdm.exe                        1508   4076      4     59 2019-01-18 12:01:09 UTC+0000
........ 0x85009a48:WINI.EXE                         3660   1508      7    130 2019-01-18 12:01:11 UTC+0000
...... 0x84ff7a48:WinRAR.exe                         2000    928      3    129 2019-01-18 11:22:52 UTC+0000
...... 0x84f1aba0:ExeBinder.exe                      2448    928      0 ------ 2019-01-18 11:36:59 UTC+0000
....... 0x84de6d40:svchost.exe                       2772   2448      6    116 2019-01-18 11:36:59 UTC+0000
 0x84d91740:noixre.exe                               3100   3568      0 ------ 2019-01-18 11:35:23 UTC+0000
```

    - List the network connections that were open on the victim's machine during infection.

      We can take all connection using netscan command. Here is the screenshot of list connection. It is too big for the screenshot, so attached the total connections as a file with evidence.

```
AngryBird:is7 Dilanka$ vol.py -f is7.elf --profile=Win7SP1x86 netscan
Volatility Foundation Volatility Framework 2.5
Offset(P)          Proto    Local Address                  Foreign Address      State            Pid      Owner          Created
0x4bf7968          UDPv4    0.0.0.0:58020                  *:*                                   1072     svchost.exe    2019-01-18 11:09:22 UTC+0000
0x7e254648         UDPv4    0.0.0.0:5355                   *:*                                   1176     svchost.exe    2019-01-18 11:09:23 UTC+0000
0x7e26aac8         UDPv4    0.0.0.0:0                      *:*                                   2068     svchost.exe    2019-01-17 09:17:32 UTC+0000
0x7e26aac8         UDPv6    :::0                           *:*                                   2068     svchost.exe    2019-01-17 09:17:32 UTC+0000
0x7e292ab0         UDPv6    ::1:58017                      *:*                                   1432     svchost.exe    2019-01-18 11:09:21 UTC+0000
0x7e2f5968         UDPv4    0.0.0.0:0                      *:*                                   2068     svchost.exe    2019-01-17 09:17:42 UTC+0000
0x7e2f5968         UDPv6    :::0                           *:*                                   2068     svchost.exe    2019-01-17 09:17:42 UTC+0000
0x7e2fa8e0         UDPv4    0.0.0.0:3540                   *:*                                   2068     svchost.exe    2019-01-17 09:17:42 UTC+0000
0x7e2fa8e0         UDPv6    :::3540                        *:*                                   2068     svchost.exe    2019-01-17 09:17:42 UTC+0000
0x7e405c28         UDPv6    fe80::2151:a5e2:7627:756c:58016 *:*                                  1432     svchost.exe    2019-01-18 11:09:21 UTC+0000
0x7e40ad80         UDPv6    ::1:1900                       *:*                                   1432     svchost.exe    2019-01-18 11:09:21 UTC+0000
0x7e443f50         UDPv4    0.0.0.0:4500                   *:*                                   932      svchost.exe    2019-01-17 09:16:58 UTC+0000
0x7e443f50         UDPv6    :::4500                        *:*                                   932      svchost.exe    2019-01-17 09:16:58 UTC+0000
0x7e49a008         UDPv4    0.0.0.0:0                      *:*                                   928      explorer.exe   2019-01-18 12:01:19 UTC+0000
0x7e49a008         UDPv6    :::0                           *:*                                   928      explorer.exe   2019-01-18 12:01:19 UTC+0000
0x7e5051e0         UDPv4    0.0.0.0:54916                  *:*                                   1432     svchost.exe    2019-01-17 09:17:02 UTC+0000
0x7e5051e0         UDPv6    :::54916                       *:*                                   1432     svchost.exe    2019-01-17 09:17:02 UTC+0000
0x7e505e38         UDPv4    0.0.0.0:54915                  *:*                                   1432     svchost.exe    2019-01-17 09:17:02 UTC+0000
0x7e53a3a0         UDPv4    0.0.0.0:14440                  *:*                                   928      explorer.exe   2019-01-18 11:35:39 UTC+0000
0x7e5637d0         UDPv4    0.0.0.0:3702                   *:*                                   1432     svchost.exe    2019-01-18 11:09:26 UTC+0000
0x7e5637d0         UDPv6    :::3702                        *:*                                   1432     svchost.exe    2019-01-18 11:09:26 UTC+0000
0x7e5d9098         UDPv4    10.0.2.15:1900                 *:*                                   1432     svchost.exe    2019-01-18 11:09:21 UTC+0000
0x7e5f1528         UDPv4    0.0.0.0:3702                   *:*                                   1432     svchost.exe    2019-01-18 11:09:26 UTC+0000
0x7e5f78d0         UDPv4    0.0.0.0:3702                   *:*                                   1432     svchost.exe    2019-01-18 11:09:26 UTC+0000
0x7e774e88         UDPv4    0.0.0.0:3702                   *:*                                   1432     svchost.exe    2019-01-18 11:09:26 UTC+0000
0x7e774e88         UDPv6    :::3702                        *:*                                   1432     svchost.exe    2019-01-18 11:09:26 UTC+0000
0x7e80f838         UDPv4    0.0.0.0:500                    *:*                                   932      svchost.exe    2019-01-17 09:16:58 UTC+0000
0x7e80f838         UDPv6    :::500                         *:*                                   932      svchost.exe    2019-01-17 09:16:58 UTC+0000
0x7e80fcc8         UDPv4    0.0.0.0:500                    *:*                                   932      svchost.exe    2019-01-17 09:16:58 UTC+0000
0x7e810830         UDPv4    0.0.0.0:0                      *:*                                   932      svchost.exe    2019-01-17 09:16:58 UTC+0000
0x7e810d80         UDPv4    0.0.0.0:4500                   *:*                                   932      svchost.exe    2019-01-17 09:16:58 UTC+0000
0x7e81de38         UDPv4    0.0.0.0:0                      *:*                                   932      svchost.exe    2019-01-17 09:16:58 UTC+0000
0x7e81de38         UDPv6    :::0                           *:*                                   932      svchost.exe    2019-01-17 09:16:58 UTC+0000
0x7ebd2c08         UDPv4    0.0.0.0:0                      *:*                                   1176     svchost.exe    2019-01-18 11:09:23 UTC+0000
0x7ebd2c08         UDPv6    :::0                           *:*                                   1176     svchost.exe    2019-01-18 11:09:23 UTC+0000
0x7e41b2a8         TCPv4    0.0.0.0:49154                  0.0.0.0:0            LISTENING        932      svchost.exe
```

- Are there any connections initiated by the suspicious process?

  Sub process of suspicious process initiated the connection to all other available computers in network. This may be worm/virus/trojon.

```
0x7fe4d998         UDPv6    :::0                           *:*                                   2068     svchost.exe
0x7f8297c0         TCPv4    10.0.2.15:139                  0.0.0.0:0            LISTENING        4        System
0x7f985120         TCPv4    0.0.0.0:16629                  0.0.0.0:0            LISTENING        928      explorer.exe
0x7f9a54f8         TCPv4    0.0.0.0:12133                  0.0.0.0:0            LISTENING        928      explorer.exe
0x7f9a54f8         TCPv6    :::12133                       :::0                 LISTENING        928      explorer.exe
0x7faed258         TCPv4    0.0.0.0:12346                  0.0.0.0:0            LISTENING        3660     WINI.EXE
0x7fe76610         TCPv4    0.0.0.0:12345                  0.0.0.0:0            LISTENING        3660     WINI.EXE
0x7f8dccd8         TCPv4    10.0.2.15:50556                198.84.60.200:443    CLOSE_WAIT       944      chrome.exe
0x7f8f8bd0         TCPv4    10.0.2.15:50533                198.84.60.198:443    CLOSE_WAIT       944      chrome.exe
0x7f9035f8         TCPv4    10.0.2.15:50557                198.84.60.200:443    CLOSE_WAIT       944      chrome.exe
0x7f911df8         TCPv4    10.0.2.15:50552                198.84.60.198:443    CLOSE_WAIT       944      chrome.exe
0x7f922df8         TCPv4    10.0.2.15:50544                93.184.220.66:443    ESTABLISHED      944      chrome.exe
0x7f970df8         TCPv4    10.0.2.15:49790                172.217.160.35:443   CLOSE_WAIT       944      chrome.exe
0x7f99cdf8         TCPv4    10.0.2.15:50530                74.125.68.102:443    ESTABLISHED      944      chrome.exe
0x7f9b3008         TCPv4    -:0                            -:0                  CLOSED           2556     svsdati.exe
```

- At what time(s) exactly this incident happened? (Timestamp)

  mmcrack.exe file opened at 2019-01-18 12:01:03 UTC+0000 and exited at 2019-01-18 12:01:09 UTC+0000 then subprocess started the malicious activity at 2019-01-18 12:01:11 UTC+0000

```
..... 0x84988030:taskmgr.exe                  2252    928      7    133 2019-01-18 11:35:31 UTC+0000
..... 0x84e1a030:mmcrack.exe                  1588    928      0 ------ 2019-01-18 12:01:03 UTC+0000
..... 0x85057d40:csrstub.exe                  4076   1588      1     10 2019-01-18 12:01:09 UTC+0000
..... 0x8501ad40:ntvdm.exe                    1508   4076      4     59 2019-01-18 12:01:09 UTC+0000
..... 0x85009a48:WINI.EXE                     3660   1508      7    130 2019-01-18 12:01:11 UTC+0000
..... 0x84ff7a48:WinRAR.exe                   2000    928      3    129 2019-01-18 11:22:52 UTC+0000
..... 0x84f1aba0:ExeBinder.exe                2448    928      0 ------ 2019-01-18 11:36:59 UTC+0000
..... 0x84de6d40:svchost.exe                  2772   2448      6    116 2019-01-18 11:36:59 UTC+0000
 0x84d91740:noixre.exe                        3100   3568      0 ------ 2019-01-18 11:35:23 UTC+0000
[AngryBird:is7 Dilanka$
```

- What are the local sockets this process tried open in the machine?

```
0x7f985120         TCPv4    0.0.0.0:16629                  0.0.0.0:0            LISTENING        928      explorer.exe
0x7f9a54f8         TCPv4    0.0.0.0:12133                  0.0.0.0:0            LISTENING        928      explorer.exe
0x7f9a54f8         TCPv6    :::12133                       :::0                 LISTENING        928      explorer.exe
0x7faed258         TCPv4    0.0.0.0:12346                  0.0.0.0:0            LISTENING        3660     WINI.EXE
0x7fe76610         TCPv4    0.0.0.0:12345                  0.0.0.0:0            LISTENING        3660     WINI.EXE
0x7f8dccd8         TCPv4    10.0.2.15:50556                198.84.60.200:443    CLOSE_WAIT       944      chrome.exe
0x7f8f8bd0         TCPv4    10.0.2.15:50533                198.84.60.198:443    CLOSE_WAIT       944      chrome.exe
0x7f9035f8         TCPv4    10.0.2.15:50557                198.84.60.200:443    CLOSE_WAIT       944      chrome.exe
0x7f911df8         TCPv4    10.0.2.15:50552                198.84.60.198:443    CLOSE_WAIT       944      chrome.exe
0x7f922df8         TCPv4    10.0.2.15:50544                93.184.220.66:443    ESTABLISHED      944      chrome.exe
```

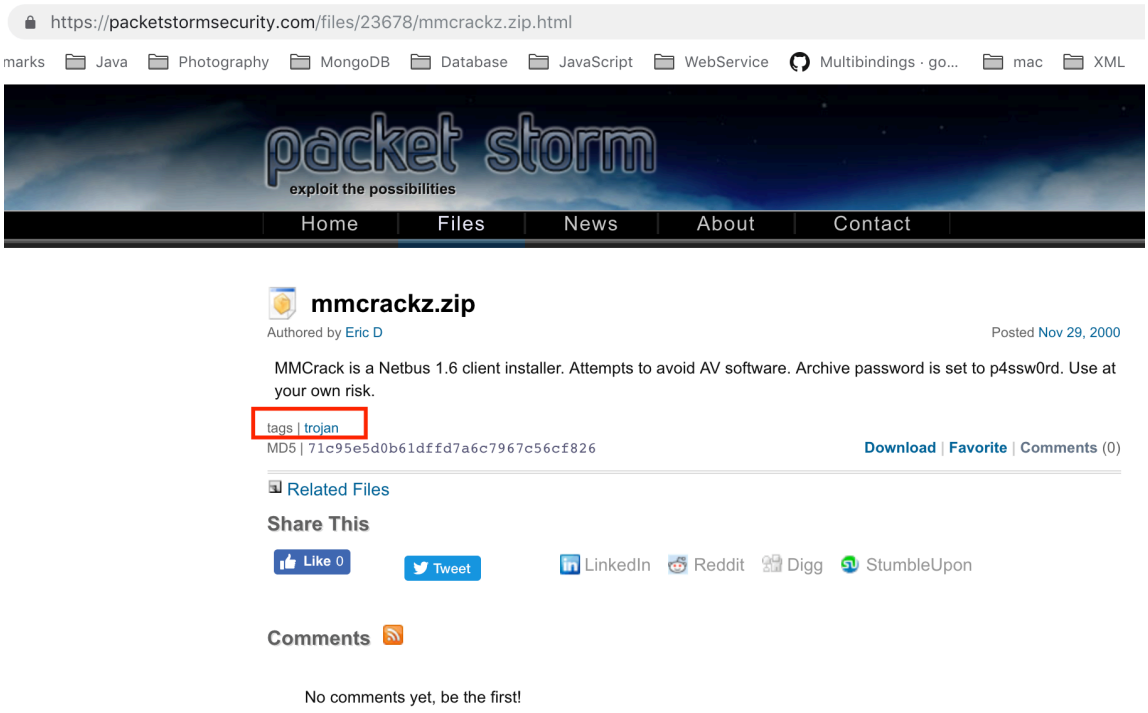
- What can you conclude about the identified sockets?

  TCPv4  0.0.0.0:12346

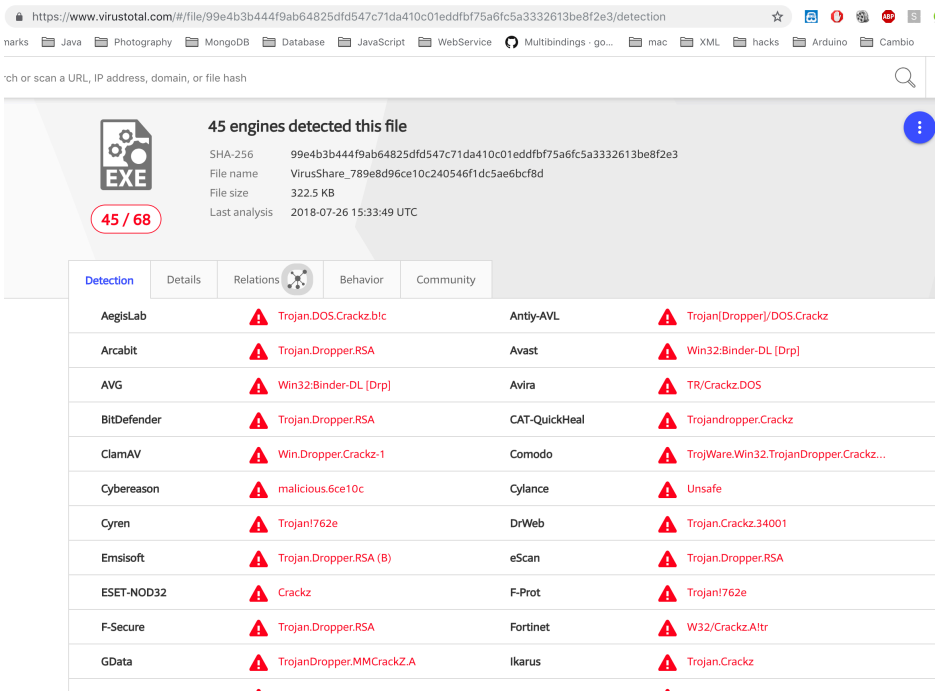
  TCPv4  0.0.0.0:12345

These ports are not the common ports that applications using. So, can be considered they are using by the malicious activity since it is open by the malicious process's subprocess.

So, I searched for the suspected crack file and the exe file in virus databases. Found this

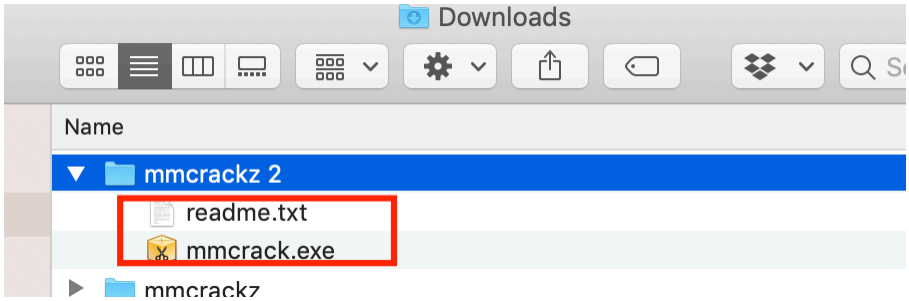



Using Virus total:

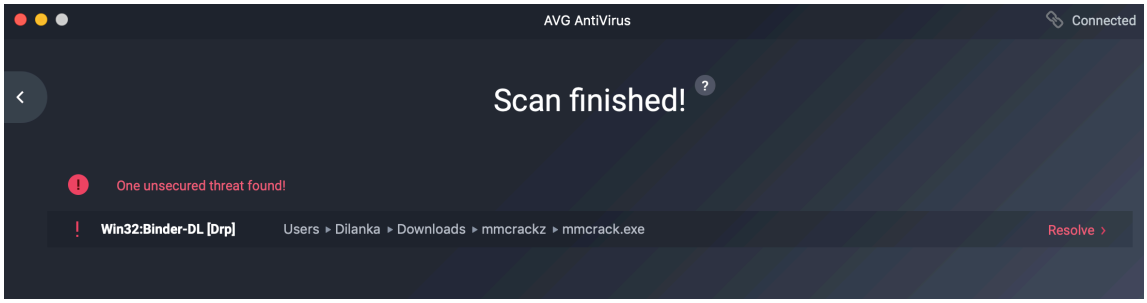


It is listed as trojan which attempt to avoid antivirus software.

I downloaded crack file and tried to scan using antivirus.

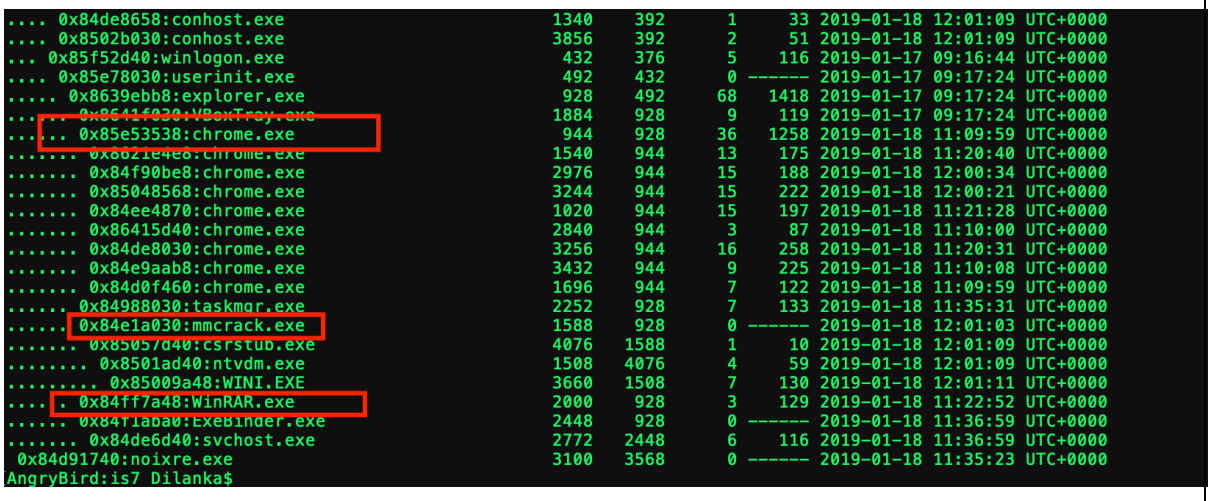



Scanning result:

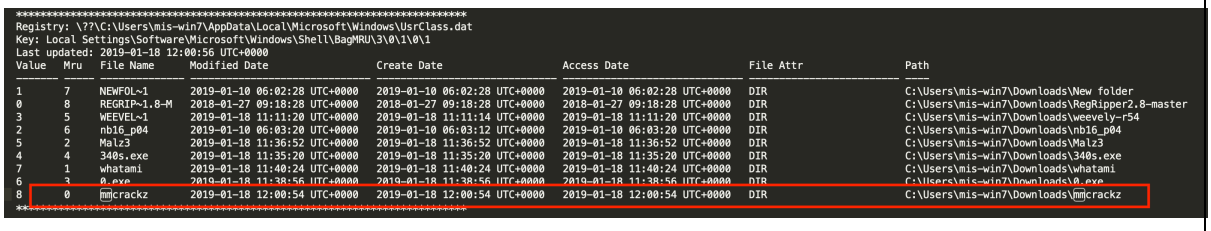



Conclusion:

User has downloaded mmcrack.zip file from the internet and extracted using WinRAR as I can see WinRAR process in the process list.




Exploring shellbags logs:



After that user has executed the mmcrack.exe file to open it and which cause of the start of other subprocess and infection.

- Provide event happened after the exploits (Timeline)

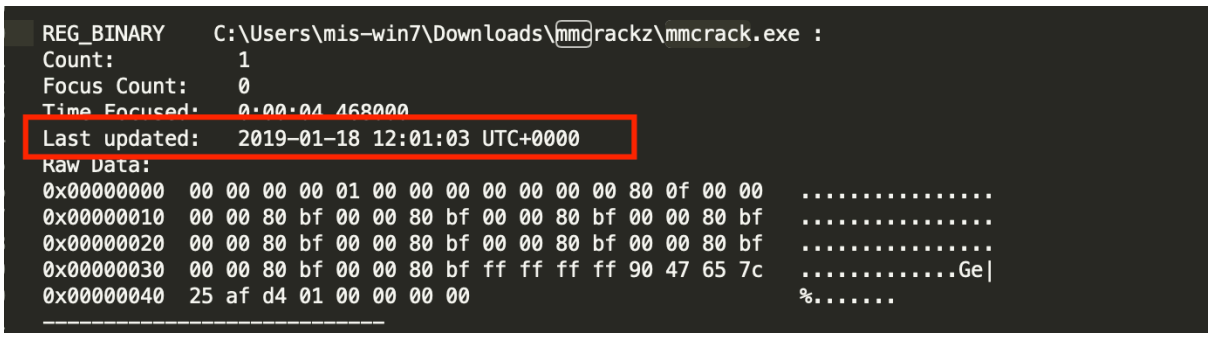
mftparser can be used to scans for potential Master File Table (MFT) entries in memory (using "FILE" and "BAAD" signatures) and prints out information for certain attributes,currently: $FILE_NAME ($FN), $STANDARD_INFORMATION ($SI), $FN and $SI attributes from the $ATTRIBUTE_LIST, $OBJECT_ID(default output only) and resident $DATA.

| | | | |
|---|---|---|---|
| 53 | 2019-01-18 12:01:22 UTC+0000 | [_HBASE_BLOCK TimeStamp] | \SystemRoot\System32\Config\SOFTWARE |
| 54 | 2019-01-18 12:01:19 UTC+0000 | [NETWORK CONNECTION] | 0.0.0.0:0 -> *:* |
| 55 | 2019-01-18 12:01:19 UTC+0000 | [NETWORK CONNECTION] | :::0 -> *:* |
| 56 | 2019-01-18 12:01:15 UTC+0000 | [_HBASE_BLOCK TimeStamp] | \REGISTRY\MACHINE\SYSTEM |
| 57 | 2019-01-18 12:01:13 UTC+0000 | [Handle (Key)] | MACHINE\CONTROLSET001\SERVICES\SHAREDACCESS\EPOCH |
| 58 | 2019-01-18 12:01:13 UTC+0000 | [Handle (Key)] | MACHINE\CONTROLSET001\SERVICES\SHAREDACCESS\EPOCH |
| 59 | 2019-01-18 12:01:13 UTC+0000 | [Handle (Key)] | MACHINE\CONTROLSET001\SERVICES\SHAREDACCESS\EPOCH |
| 60 | 2019-01-18 12:01:13 UTC+0000 | [Handle (Key)] | MACHINE\CONTROLSET001\SERVICES\SHAREDACCESS\EPOCH |
| 61 | 2019-01-18 12:01:13 UTC+0000 | [Handle (Key)] | MACHINE\CONTROLSET001\SERVICES\SHAREDACCESS\EPOCH |
| 62 | 2019-01-18 12:01:13 UTC+0000 | [Handle (Key)] | MACHINE\CONTROLSET001\SERVICES\SHAREDACCESS\EPOCH |
| 63 | 2019-01-18 12:01:11 UTC+0000 | [Handle (Key)] | USER |
| 64 | 2019-01-18 12:01:11 UTC+0000 | [DLL LOADTIME (dll)] | apphelp.dll |
| 65 | 2019-01-18 12:01:11 UTC+0000 | [Handle (Key)] | USER |
| 66 | 2019-01-18 12:01:11 UTC+0000 | [Handle (Key)] | USER |
| 67 | 2019-01-18 12:01:11 UTC+0000 | [Handle (Key)] | USER |
| 68 | 2019-01-18 12:01:11 UTC+0000 | [Handle (Key)] | USER |
| 69 | 2019-01-18 12:01:11 UTC+0000 | [Handle (Key)] | USER |
| 70 | 2019-01-18 12:01:11 UTC+0000 | [Handle (Key)] | USER |
| 71 | 2019-01-18 12:01:11 UTC+0000 | [Handle (Key)] | USER |
| 72 | 2019-01-18 12:01:11 UTC+0000 | [Handle (Key)] | USER |
| 73 | 2019-01-18 12:01:11 UTC+0000 | [DLL LOADTIME (dll)] | DEVOBJ.dll |
| 74 | 2019-01-18 12:01:11 UTC+0000 | [DLL LOADTIME (dll)] | SETUPAPI.dll |
| 75 | 2019-01-18 12:01:11 UTC+0000 | [DLL LOADTIME (dll)] | comctl32.dll |
| 76 | 2019-01-18 12:01:11 UTC+0000 | [Handle (Key)] | USER |
| 77 | 2019-01-18 12:01:11 UTC+0000 | [Handle (Key)] | USER |
| 78 | 2019-01-18 12:01:11 UTC+0000 | [Handle (Key)] | USER |
| 79 | 2019-01-18 12:01:11 UTC+0000 | [Handle (Key)] | USER |
| 80 | 2019-01-18 12:01:11 UTC+0000 | [Handle (Key)] | USER |
| 81 | 2019-01-18 12:01:11 UTC+0000 | [Handle (Key)] | USER |
| 82 | 2019-01-18 12:01:11 UTC+0000 | [Handle (Key)] | USER |
| 83 | 2019-01-18 12:01:11 UTC+0000 | [Handle (Key)] | USER |
| 84 | 2019-01-18 12:01:11 UTC+0000 | [PROCESS] | WINI.EXE |
| 85 | 2019-01-18 12:01:11 UTC+0000 | [Handle (Key)] | USER |
| 86 | 2019-01-18 12:01:11 UTC+0000 | [DLL LOADTIME (dll)] | DEVOBJ.dll |

- Registry changes

Listed down all the registries and find if there changes related to the malicious file.

vol.py -f is7.elf --profile=Win7SP1x86 userassist




Approach

1. With the artefact provided and as it is memory dump, decided to choose appropriate tools which help to analyse and examine memory dump.
2. Initially started the analysis with the tool called Volatility.
3. Able to find information related to the infrastructure related information with the analysis by the Volatility.
    a. System/OS information
    b. Hardware compatibility
    c. Processes list of the computer when taking the memory dump
    d. Processes tree of the computer when taking the memory dump
4. Once analyse the process tree, identified suspicious processes and suspected that it is malicious activity such as Virus/Worm.
5. Then tried to find it via common virus databases.
    a. https://packetstormsecurity.com
    b. https://www.virustotal.com
6. Founded the it is trojan process that uses to open victims computer port to anywhere.

Conclusion

Victim user has downloaded mmcrack.zip file via chrome browser and extracted to the computer and executed the mmcrack.exe file. Which caused to open WINI.exe malicious process to be started and it has opened some ports to attacker.

********** End **********