(Georgia)

DFIRCON APT Malware & Memory Challenge

Malware Analysis

გამოყენებული ხელსაწყოები: Strings/Volatility/Virustotal
სისტემა სადაც ვირუსი გაანალიზდა: linux
დაინფიცირებული მანქანა:WinXPSP2x86

მაშ ასე გადავიდეთ მემორი ფაილის ანალიზზე და შევამოწმოთ დაინფიცირებული მანქანა:

```
Determining profile based on KDBG search...

          Suggested Profile(s) : WinXPSP2x86, WinXPSP3x86 (Instantiated with WinXPSP2x86)
                     AS Layer1 : IA32PagedMemoryPae (Kernel AS)
                     AS Layer2 : FileAddressSpace (/home/ch3k1/Desktop/sans/APT.img)
                      PAE type : PAE
                           DTB : 0x319000L
                          KDBG : 0x80545b60
          Number of Processors : 1
     Image Type (Service Pack) : 3
                KPCR for CPU 0 : 0xffdff000
             KUSER_SHARED_DATA : 0xffdf0000
           Image date and time : 2009-05-05 19:28:57 UTC+0000
     Image local date and time : 2009-05-05 15:28:57 -0400
```

სურათზე უყურებთ დაინფიცირებულ მანქანას, სადაც მოხდა მემორი ფაილის მოხსნა

მემორი ფაილი შეგიძლიათ გადმოწეროთ სანსის ბლოგიდან, ასევე სანსის ბლოგზე შეგიძლიათ უპასუხოდ სანსის მიერ შედგენინ კითხვებს პასუხების სწორად გაცემის შემთხვევაში დაგიფინანსებენ კურსებს, მეტი ინფორმაციისთვის ეწვიეთ სანსის ფორენსიკის ბლოგს *https://www.surveymonkey.com/s/JQ9QFHP*

შევამოწმოთ ქონექშენები :

```
Offset(P)  Local Address             Remote Address            Pid
---------- ------------------------- ------------------------- ---
0x0205ece0 192.168.157.10:1050       222.128.1.2:443           1672
0x020611f8 192.168.157.10:1053       218.85.133.23:89          796
0x032c01f8 192.168.157.10:1053       218.85.133.23:89          796
0x0337dce0 192.168.157.10:1050       222.128.1.2:443           1672
0x08a4ace0 192.168.157.10:1050       222.128.1.2:443           1672
0x18200ce0 192.168.157.10:1050       222.128.1.2:443           1672
```

ip: 222.128.1.2 კომუნიკაციის პორტი 443
პროცესის Pid არის 1672

შევამოწმოთ პროცესები:

```
 0x823c8830:System                                  4      0     55    254 1970-01-01 00:00:00 UTC+0000
. 0x8230aad8:smss.exe                             564      4      3     19 2009-04-16 16:10:01 UTC+0000
.. 0x81f63020:winlogon.exe                        660    564     16    502 2009-04-16 16:10:06 UTC+0000
... 0x81f22020:services.exe                       704    660     15    254 2009-04-16 16:10:06 UTC+0000
.... 0x81f739b0:svchost.exe                      1088    704     70   1445 2009-04-16 16:10:07 UTC+0000
..... 0x81f96220:wscntfy.exe                     1260   1088      1     39 2009-04-16 16:10:22 UTC+0000
.... 0x81da4590:svchost.exe                       968    704     10    241 2009-04-16 16:10:07 UTC+0000
.... 0x81dc2570:VMwareService.e                  1032    704      3    175 2009-04-16 16:10:16 UTC+0000
.... 0x8231eda0:msiexec.exe                      1464    704      6    294 2009-04-16 16:11:02 UTC+0000
.... 0x81e54da0:svchost.exe                       884    704     17    208 2009-04-16 16:10:07 UTC+0000
..... 0x81dbdda0:iexplore.exe                     796    884      8    152 2009-05-05 19:28:28 UTC+0000
.... 0x81e91da0:svchost.exe                      1212    704     14    208 2009-04-16 16:10:09 UTC+0000
.... 0x81d33628:alg.exe                           464    704      6    105 2009-04-16 16:10:21 UTC+0000
.... 0x8219b630:spoolsv.exe                      1512    704     10    129 2009-04-16 16:10:10 UTC+0000
.... 0x822cb458:vmacthlp.exe                      872    704      1     25 2009-04-16 16:10:07 UTC+0000
.... 0x8232c020:svchost.exe                      1140    704      5     60 2009-04-16 16:10:08 UTC+0000
... 0x82164da0:lsass.exe                          716    660     21    342 2009-04-16 16:10:06 UTC+0000
.. 0x822ca2c0:csrss.exe                           636    564     10    356 2009-04-16 16:10:06 UTC+0000
 0x81da71a8:explorer.exe                         1672   1624     15    586 2009-04-16 16:10:10 UTC+0000
. 0x81f1c7e8:VMwareTray.exe                      1984   1672      1     37 2009-04-16 16:10:11 UTC+0000
. 0x81e4d648:cmd.exe                              840   1672      1     33 2009-05-05 15:56:24 UTC+0000
.. 0x82161558:MIRAgent.exe                        456    840      1     77 2009-05-05 19:28:40 UTC+0000
. 0x81dc1a78:VMwareUser.exe                      2004   1672      8    228 2009-04-16 16:10:11 UTC+0000
. 0x81f1a650:ctfmon.exe                          2020   1672      1     71 2009-04-16 16:10:11 UTC+0000
```

  პროცესი სადაც ვირუსმა ინჯექშენი გააკეთა არის explorer.exe და რატომ ყველაფერი ახსნილი იქნება ჩემს პოსტში. დამპი გავუკეთოთ პროცეს და შემდეგ ავტვირთოთ ვირუსტოტალზე:

```
Process(V) ImageBase  Name                 Result
---------- ---------- -------------------- ------
0x81da71a8 0x01000000 explorer.exe         OK: executable.1672.exe
```

ეხლა ავტვირთოთ ბინარი ფაილი ვირუსტოტალზე:

SHA256: 6e1f6b9735bdfbc54c1b6ee76fc84a47b1c29c31a22314bbd842b30cef0a2f55

File name: executable.1672.exe

Detection ratio: 4 / 49

Analysis date: 2013-12-13 18:39:31 UTC (1 minute ago)

1 0

Analysis | File detail | Additional information | Comments | Votes

Antivirus	Result	Update
Ad-Aware	✓	20131211
Agnitum	✓	20131213
AhnLab-V3	✓	20131213
AntiVir	TR/Crypt.EPACK.Gen2	20131213

49-ა ანტივირუსიდან მხოლოდ 4-მა ანტი ვირუსმა შეძლე მისი დაჭერა.

გადავიდეთ კოდის ინჯექშენზე , გამოვიყენოთ malfind ფუნქცია, რომელიც იდენდიფიკაციას გაუკეთებს 20-ზე მეტ სხვადასხვა მემორი სეგმენტს, რომელსაც შეიცავს ჩაინჯექტებული კოდი. მოკლედ ამის გაკეთება ძალიან მარტივია ამ ხელსაწყოს გამოყენებით.

```
Process: explorer.exe Pid: 1672 Address: 0x1820000
Vad Tag: VadS Protection: PAGE_EXECUTE_READWRITE
Flags: CommitCharge: 1, MemCommit: 1, PrivateMemory: 1, Protection: 6

0x01820000  00 11 42 ab 71 07 4a ab 71 2b 3e ab 71 27 4c ab   ..B.q.J.q+>.q'L.
0x01820010  71 6f 67 ab 71 53 2e ab 71 e1 2e ab 71 55 53 ab   qog.qS..q...qUS.
0x01820020  71 e1 9a 80 7c 74 9b 80 7c c7 06 81 7c 6b 23 80   q...|t..|...|k#.
0x01820030  7c 17 6c dd 77 42 78 dd 77 ab 7a dd 77 d7 ea dd   |.l.wBx.w.z.w...

0x1820000 0011            ADD [ECX], DL
0x1820002 42              INC EDX
0x1820003 ab              STOSD
0x1820004 7107            JNO 0x182000d
0x1820006 4a              DEC EDX
0x1820007 ab              STOSD
0x1820008 712b            JNO 0x1820035
0x182000a 3eab            STOSD
0x182000c 7127            JNO 0x1820035
0x182000e 4c              DEC ESP
0x182000f ab              STOSD
0x1820010 716f            JNO 0x1820081
```

მოკლედ ამის გარჩევე ძაან მარტივია შეგვიძლია დავაკვირდეთ სხა მემორი სეგმენტებს, ყველა მემორი სეგმენტი ერთმანეთს გავს გარდა ამ სეგმენტისა მაშ ასე ინჯექშენის მემორი სეგმენტიც ვიპოვეთ, დანამდვილებით შემიძლია ვთქვა, რომ ვირუსმა ინჯექშენი ამ პროცესში გააკეთა :) ეხლა დავადგინოთ ნამდვილად შეიცავს თუ არა პროცესი ინჯექშენი ფუნქციებს ამის გაკეთება ძალიან მარტივია საჭიროა გავაკეთოთ პროცესის მემორი დამპი და შევხედოთ ფუქციებს:

```
ch3k1 ~ # python /usr/local/bin/vol.py -f /home/ch3k1/Desktop/sans/APT.img --profile=WinXPSP2x86 memdump -p 1672 -D /home/ch3k1/
Volatility Foundation Volatility Framework 2.3.1
************************************************************************
Writing explorer.exe [  1672] to 1672.dmp
```

შევამოწმოთ ფუნქციები, ვირუსული პროცესი შეიცავს explorer.exe-სგან განსხვავებულ ფუნქციებს, რასაც რეალურად explorer.exe არ იყენებს:

```
0x01001100 0x7c82c8e5 kernel32.dll          SetProcessShutdownParameters
0x01001104 0x7c8024b7 kernel32.dll          ReleaseMutex
0x01001108 0x7c80e947 kernel32.dll          CreateMutexW
0x0100110c 0x7c82c330 kernel32.dll          SetPriorityClass
0x01001110 0x7c80de85 kernel32.dll          GetCurrentProcess
0x01001114 0x7c801e54 kernel32.dll          GetStartupInfoW
0x01001118 0x7c817013 kernel32.dll          GetCommandLineW
0x0100111c 0x7c80ac9f kernel32.dll          SetErrorMode
0x01001120 0x7c9010e0 ntdll.dll             694
0x01001124 0x7c901000 kernel32.dll          EnterCriticalSection
0x01001128 0x7c80a0cb kernel32.dll          ResetEvent
0x01001130 0x7c810b69 kernel32.dll          CompareFileTime
0x01001134 0x7c8017e9 kernel32.dll          GetSystemTimeAsFileTime
0x01001138 0x7c80c198 kernel32.dll          SetThreadPriority
0x0100113c 0x7c8097b8 kernel32.dll          GetCurrentThreadId
0x01001140 0x7c80a823 kernel32.dll          GetThreadPriority
0x01001144 0x7c80997b kernel32.dll          GetCurrentThread
0x01001148 0x7c80bff4 kernel32.dll          GetUserDefaultLangID
0x01001150 0x7c868bac kernel32.dll          GetBinaryTypeW
0x01001154 0x7c81fca9 kernel32.dll          GetModuleHandleExW
0x01001158 0x7c810bac kernel32.dll          SystemTimeToFileTime
0x0100115c 0x7c80a864 kernel32.dll          GetLocalTime
0x01001160 0x7c8099b0 kernel32.dll          GetCurrentProcessId
0x01001178 0x7c80aa5c kernel32.dll          lstrcmpW
0x0100117c 0x7c801af5 kernel32.dll          LoadLibraryExW
0x01001188 0x7c80ef71 kernel32.dll          FindFirstFileW
0x01001190 0x7c80a0a7 kernel32.dll          SetEvent
0x01001198 0x7c83378d kernel32.dll          GetDateFormatW
0x0100119c 0x7c833feb kernel32.dll          GetTimeFormatW
0x010011a4 0x7c80ba7f kernel32.dll          lstrcpynW
0x010011ac 0x7c90fe10 ntdll.dll             796
0x010011b0 0x7c80ac51 kernel32.dll          GetProcessHeap
0x010011b4 0x7c90ff0d kernel32.dll          HeapFree
0x010011b8 0x7c919b80 ntdll.dll             760
0x010011bc 0x7c9104bd ntdll.dll             812
0x010011c0 0x7c9100a4 kernel32.dll          HeapAlloc
0x010011c8 0x7c8021d0 kernel32.dll          ReadProcessMemory
0x010011cc 0x7c8309d1 kernel32.dll          OpenProcess
0x010011d0 0x7c809832 kernel32.dll          InterlockedCompareExchange
0x010011d4 0x7c801d7b kernel32.dll          LoadLibraryA
0x010011d8 0x7c80a4b7 kernel32.dll          QueryPerformanceCounter
0x010011dc 0x7c863e6a kernel32.dll          UnhandledExceptionFilter
0x010011e0 0x7c8449fd kernel32.dll          SetUnhandledExceptionFilter
0x010011e4 0x7c809b74 kernel32.dll          VirtualFree
0x010011e8 0x7c809ae1 kernel32.dll          VirtualAlloc
0x010011f0 0x7c801e1a kernel32.dll          TerminateProcess
0x010011f8 0x7c80bfcd kernel32.dll          GetSystemDefaultLCID
0x010011fc 0x7c8115f2 kernel32.dll          GetLocaleInfoW
0x01001200 0x7c80a739 kernel32.dll          CreateEventW
```

სურათზე არ ჩანს ისეთი ფუნქციები, როგორიცაა:

[CallNextHookEx/GetKeyboardState/CreateProcessA] ასევე არ ჩანს Network API-ის ფუნქციები, როგორიცაა: [gethostbyname/send/recv], მაგრამ ეხლა გადავიდეთ სთრინგების შემოწმებაზე და გავაკეთოთ პროცესის მემორი დამპის ანალიზი, სურათზე ნაჩვენებია ყველა ჩამოთვლილი ფუნქცია:

```
ch3k1 ~ # strings /home/ch3k1/1672.dmp | grep CallNextHookEx
CallNextHookEx
CallNextHookEx
CallNextHookEx
CallNextHookEx
CallNextHookEx
ch3k1 ~ # strings /home/ch3k1/1672.dmp | grep GetKeyboardState
GetKeyboardState
GetKeyboardState
GetKeyboardState
GetKeyboardState
ch3k1 ~ # strings /home/ch3k1/1672.dmp | grep CreateProcessA
CreateProcessAsUserW
CreateProcessA
CreateProcessAsUserA
CreateProcessAsUserSecure
CreateProcessAsUserW
CreateProcessAsUserW
CreateProcessA
CreateProcessAsUserSecure
CreateProcessA
CreateProcessAsUserW
ch3k1 ~ # strings /home/ch3k1/1672.dmp | grep gethostbyname
gethostbyname
The PrimaryAddressResolutionStatus property holds status information resulting from the gethostbyname call.
 address property) given in the query. It is not related to any other resolution performed.
ch3k1 ~ # strings /home/ch3k1/1672.dmp | grep recv
recv
recvfrom
```

GetKeyboardState კეილოგერის ფუნქცია

WriteProceessMemory/CreateRemoteThread/VirtualAllocEx code injection-ის ფუნქციები

```
ch3k1 ~ # strings /home/ch3k1/1672.dmp | grep WriteProcessMemory
WriteProcessMemory
ch3k1 ~ # strings /home/ch3k1/1672.dmp | grep CreateRemoteThread
CreateRemoteThread
ch3k1 ~ # strings /home/ch3k1/1672.dmp | grep VirtualAllocEx
VirtualAllocEx
VirtualAllocEx
```

მაშ ასე იმედია მოგეწონებათ და გამოგადგებათ, წარმატებებს გისურვებთ