**(Package, part 1 of 2)DLL Launcher with file system capababilities**

|  |  |  |
| --- | --- | --- |
| **BACKGROUND** | | |
| **Date:** | | 7/14/18 |
| **Workstation:** | | VirtualBox: winXP unpatched 32bit intel |
| **File Name:** | | Lab01-01.exe //i386 CUI |
| **File Location:** | |  |
| **File Timestamps:** | | 2010/12/19 sun 16:16:19 utc |
| **Notification Vector:** | |  |
| **STATIC ANALYSIS** | | |
| **File Size (bytes):** | Actual: 16,384 KB , virtual data sizes match raw | |
| **Icon Graphic:** | CUI | |
| **Signed?:** | at 1908: visualC | |
| **File Hash:** | **MD5: bb7425b82141a1c0f7d60e5106676bb1** | |
| **Imp Hash:** |  | |
| **PE Section Hashes:** | | |
|  | | |
| **Compile Time** (pescanner, PEView)**:** | | |
|  | | |
| **File Properties** (PEStudio, PeView)**:** Description, version, file header characteristics | | |
| MV C++ 6.0, | | |
| **Strings** (strings, strings2, BinText)**:** Functions, domains, IP addresses, commands, error msgs | | |
| -kerne123.dll(has no l in kernel, loads its own dll) //host sig  -C:\\*  -Has a directory path to: C:\windows\system32\kernel123.dll  -WARNING\_THIS\_WILL\_DESTROY\_YOUR\_MACHINE //host sig  -.exe (Directory searching func's are probably looking for exe files) | | |
| **Packed** (pescanner, PEiD, ExeInfo)**:** | | |
| Not packed, Entry point/offset: 1820, | | |
| **Entropy** (ByteHist, pescanner)**:** File, sections | | |
| - | | |
| **Imported/Exported Functions** (PEStudio, Dependency Walker)**:** | | |
| NO EXPORTS(small dll luancher program)  DLL IMPORTS: Kernel32.dll(ntdll.dll)  FUNC's TO NOTE: CsrNewThread, CreateFile, CopyFile, (many directory searching func's), CloseHandle | | |
| **Open Source Research** (VirusTotal, search engines, malware repositories)**:** | | |
|  | | |
| **BEHAVIORAL ANALYSIS** | | |
| **File System Artifacts** (Regshot, CaptureBAT, Process Monitor, Cuckoo)**:**  *Triggers:*Browser, mail client, specific web pages (google, bank), time, reboot, user/admin privs  *Dependencies:* DNS, HTTP, IRC, ARP | | |
|  | | |
| **Network Artifacts** (SmartSniff, Fakedns, INetSim, NetworkMiner Wireshark)**:** C2 domains/IP addresses, protocols, user-agent | | |
|  | | |
| **Memory Analysis** (Volatility, Rekall, Redline, Process Hacker)**:** rogue processes, code injection, rootkits, network artifacts | | |
|  | | |
| **Open Source Research** (centralops, robtex, urlvoid, ipvoid, TrustedSource)**:** | | |
|  | | |
| **CODE ANALYSIS** | | |
| **Static Analysis** (IDA Pro)**:** Strings, CALLs, program flow, loops | | |
|  | | |
| **Debugging** (OllyDbg)**:** Function breakpoints, monitor stack, memory map, plugins for unpacking, find OEP | | |
|  | | |
| **ANALYSIS SUMMARY** | | |
| **Key Host and Network Indicators of Compromise (IOCs):** | | |
|  | | |
| **Key Functionality:** | | |
|  | | |
| **Purpose:** | | |
|  | | |
| **Persistence:** | | |
|  | | |
| **Environment-specific Impact:** | | |
|  | | |
| **Root Cause:** | | |
|  | | |
| **Attribution:** | | |
|  | | |