**dll saved as kerne123.dll by lab01-01(launcher)**

This dll comes packaged with lab01-01.exe and is used as a launcher to save and utilize this dll. The dll is to open a backdoor into the system.

|  |  |  |
| --- | --- | --- |
| **BACKGROUND** | | |
| **Date:** | | 7/14/2018 |
| **Workstation:** | | VirtualBox: winXP unpatched 32bit intel |
| **File Name:** | | Lab01-01.dll, i386 |
| **File Location:** | |  |
| **File Timestamps:** | | 2010/12/19 SUN 16:16:38 UTC |
| **Notification Vector:** | |  |
| **STATIC ANALYSIS** | | |
| **File Size (bytes):** |  | |
| **Icon Graphic:** | GUI, | |
| **Signed?:** | IMAGE\_NT\_SIGNATURE PE | |
| **File Hash:** | **MD5:290934c61de9176ad682ffdd65f0a669** | |
| **Imp Hash:** |  | |
| **PE Section Hashes:** | | |
|  | | |
| **Compile Time** (pescanner, PEView)**:** | | |
|  | | |
| **File Properties** (PEStudio, PeView)**:** Description, version, file header characteristics | | |
|  | | |
| **Strings** (strings, strings2, BinText)**:** Functions, domains, IP addresses, commands, error msgs | | |
| 127.26.152.13 //network sig  exec | | |
| **Packed** (pescanner, PEiD, ExeInfo)**:** | | |
| Microsoft Visual C++ 6.0 DLL | | |
| **Entropy** (ByteHist, pescanner)**:** File, sections | | |
|  | | |
| **Imported/Exported Functions** (PEStudio, Dependency Walker)**:** | | |
| IMPORTS: WS2\_32.dll (listen, accept, connect, bind, htonl/htons/ntohs, inet\_addr, GetHostByName/Addr,  Secur32.dll (functions to edit and force a user logon)  netapi.dll (GetDCName, GetDcNameWithAccount)  FUNC'S TO NOTE: CreateProcess(used with sleep to make a backdoor and sends "exec" over network), Sleep(uses system time), CreateMutex, RegCreateKey, DNSQuery, RegDeleteKey, RegSetValueExA, HeapAlloc/Create, | | |
| **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:** | | |
|  | | |