**Downloader(part 1 of 2, has another hidden exe)**

|  |  |  |
| --- | --- | --- |
| **BACKGROUND** | | |
| **Date:** | | 7/14/2018 |
| **Workstation:** | | VirtualBox: win xp unpatched 32bit intel |
| **File Name:** | | Lab01-04.exe //i386 GUI |
| **File Location:** | |  |
| **File Timestamps:** | | 2019/08/30 fri 22:26:59 UTC (date and time are spoofed) |
| **Notification Vector:** | |  |
| **STATIC ANALYSIS** | | |
| **File Size (bytes):** | 36 KB | |
| **Icon Graphic:** |  | |
| **Signed?:** |  | |
| **File Hash:** | **MD5: 625ac05fd47adc3c63700c3b30de79ab** | |
| **Imp Hash:** | **MD5: 6a95c2f88e0c09a91d69ffb98bc6fce8** | |
| **PE Section Hashes:** | | |
|  | | |
| **Compile Time** (pescanner, PEView)**:** | | |
|  | | |
| **File Properties** (PEStudio, PeView)**:** Description, version, file header characteristics | | |
| has a hidden PE exe file in the .rsrc as BIN data. | | |
| **Strings** (strings, strings2, BinText)**:** Functions, domains, IP addresses, commands, error msgs | | |
| w ww.practicalmalwareanalysis.com/updater.exe //network sig , downloadable malware  \system32\wupdmgrd.exe (most likly contains more malware)  \winup.exe  BIN 101(has a bin file) | | |
| **Packed** (pescanner, PEiD, ExeInfo)**:** | | |
| unpacked: Microsoft Visual C++ 6.0 | | |
| **Entropy** (ByteHist, pescanner)**:** File, sections | | |
|  | | |
| **Imported/Exported Functions** (PEStudio, Dependency Walker)**:** | | |
| loadlibrary  winlogon.exe  urlmon.dll  psapi.dll  sfc\_os.dll //host sig  urlDownloadToFile  WinExec(writes file to disk then exec)  writefile  createFile  moveFile  openprocess  (many token privlage functions)  LoadResource //to load hidden exe **MD5: 6a95c2f88e0c09a91d69ffb98bc6fce8** | | |
| **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:** | | |
|  | | |