**Malware Analysis Template**

|  |  |  |
| --- | --- | --- |
| **BACKGROUND** | | |
| **Date:** | | 7/20/2018 |
| **Workstation:** | | VirtBox: win xp unpatched x86 intel |
| **File Name:** | | Lab03-01.exe GUI |
| **File Location:** | | - |
| **File Timestamps:** | | 2008/01/06 14:51:31 UTC |
| **Notification Vector:** | |  |
| **STATIC ANALYSIS** | | |
| **File Size (bytes):** | 7,168 | |
| **Icon Graphic:** |  | |
| **Signed?:** |  | |
| **File Hash:** | MD5: d537acb8f56a1ce206bc35cf8ff959c0 | |
| **Imp Hash:** |  | |
| **PE Section Hashes:** | | |
|  | | |
| **Compile Time** (pescanner, PEView)**:** | | |
|  | | |
| **File Properties** (PEStudio, PeView)**:** Description, version, file header characteristics | | |
| File is packed and only shows one function import. However strings are mostly all visable. | | |
| **Strings** (strings, strings2, BinText)**:** Functions, domains, IP addresses, commands, error msgs | | |
| ws2\_32, **CONNECT %S %I HTTP/1.0**, advapi32, ntdll, user32, stubpath, test, admin, **VideoDriver**, WinVMX32-, **vmx32to64.exe(hard-coded)**, AppData,  Many registry locations:  \*\**CurrentVersion\Run**  \*\CurrentVersion\Explorer\Shell Folders  software\classes\http\shell\open\commandV  software\microsoft\active setup\installed components\  DNS:  **www. practicalmalwareanalysis.com** | | |
| **Packed** (pescanner, PEiD, ExeInfo)**:** | | |
| PEncrypt 3.1 Final -> junkcode | | |
| **Entropy** (ByteHist, pescanner)**:** File, sections | | |
|  | | |
| **Imported/Exported Functions** (PEStudio, Dependency Walker)**:** | | |
| **Packed: Imports: ExitProcess, kernel32.dll**  **Runtime: dnsapi.dll, mswsock.dll, secure32.dll, ws\_32.dll, wshtcpip** | | |
| **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 | | |
| Files written:  C:\\windows\system32\vmx32to64.exe  HKLM\SOFTWARE\Microsoft\\Windows\CurrentVersion\Run\VideoDriver : [path to vmx32to64.exe] | | |
| **Network Artifacts** (SmartSniff, Fakedns, INetSim, NetworkMiner Wireshark)**:** C2 domains/IP addresses, protocols, user-agent | | |
| Shell nops, **www. practicalmalwareanalysis.com(no other IP's or DNS names), uses port 443, beacons 256 bytes always random characters, sets up for comand server with shell** | | |
| **Memory Analysis** (Volatility, Rekall, Redline, Process Hacker)**:** rogue processes, code injection, rootkits, network artifacts | | |
| Creates a Mutex: \BaseNamedObjects\WinVMX32 | | |
| **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):** | | |
| Host: vmx32to64.exe //the malware copies itself to a hardcoded file name    Network: www .malwareanalysis.com /dns it becons out to | | |
| **Key Functionality:** | | |
| Backdoor for shell commands | | |
| **Purpose:** | | |
| **comand and control** | | |
| **Persistence:** | | |
| **Set in reg to always run and beacon to its control server** | | |
| **Environment-specific Impact:** | | |
|  | | |
| **Root Cause:** | | |
|  | | |
| **Attribution:** | | |
|  | | |