**Malware Analysis Template**

|  |  |  |
| --- | --- | --- |
| **BACKGROUND** | | |
| **Date:** | | 7/14/2018 |
| **Workstation:** | |  |
| **File Name:** | | Lab01-02.exe //i386 CUI |
| **File Location:** | |  |
| **File Timestamps:** | | 2011/01/19 Wed 16:10:41 UTC |
| **Notification Vector:** | |  |
| **STATIC ANALYSIS** | | |
| **File Size (bytes):** | 3,072kb -(after unpacking)-> 16,384kb | |
| **Icon Graphic:** |  | |
| **Signed?:** |  | |
| **File Hash:** | **MD5: 8363436878404da0ae3e46991e355b83** | |
| **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 | | |
| MalService(will most likely be the name of the service it creates) //host based sig  HGL345  Internet Explorer 8.0  www. malwareanalysisbook.com //network based sig | | |
| **Packed** (pescanner, PEiD, ExeInfo)**:** | | |
| Packed: UPX1, unpacks with upx packer | | |
| **Entropy** (ByteHist, pescanner)**:** File, sections | | |
|  | | |
| **Imported/Exported Functions** (PEStudio, Dependency Walker)**:** | | |
| IMPORTED: kernel32.dll, advapi32.dll, msvcrt.dll, wininet.dll  FUNC's TO NOTE: WaitForSingleObject(+ other functions for a wait period), CreateMutex, CreateThread, CreateService, InternetOpenUrl | | |
| **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:** | | |
|  | | |