**Malware Analysis Template**

|  |  |  |
| --- | --- | --- |
| **BACKGROUND** | | |
| **Date:** | | **7/21/2018** |
| **Workstation:** | | **VirtualBox: xp unpatched 32bit intel** |
| **File Name:** | | **Lab03-02.dll 32bit gui** |
| **File Location:** | |  |
| **File Timestamps:** | | **Tues, 2010/09/28 1:00:25 (24h) UTC** |
| **Notification Vector:** | |  |
| **STATIC ANALYSIS** | | |
| **File Size (bytes):** | **24,065** | |
| **Icon Graphic:** |  | |
| **Signed?:** |  | |
| **File Hash:** | **MD5: 84882c9d43e23d63b82004fae74ebb61** | |
| **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 | | |
|  | | |
| **Packed** (pescanner, PEiD, ExeInfo)**:** | | |
| Microsoft Visual C++ 6.0 DLL, obfuscated | | |
| **Entropy** (ByteHist, pescanner)**:** File, sections | | |
|  | | |
| **Imported/Exported Functions** (PEStudio, Dependency Walker)**:** | | |
| **Imports: RegCreateKey, RegSetValue, CreateProcess, LoadLibrary, Sleep, InternetOpen, HttpOpenRequest, WSASocket**  **Exports: Install, ServiceMain** | | |
| **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 | | |
| **HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY\_IPRIP\0000\Service: "IPRIP"**  **HKLM\SYSTEM\ControlSet001\Enum\Root\LEGACY\_IPRIP\0000\DeviceDesc: "Intranet Network Awareness (INA+)"**  **HKLM\SYSTEM\ControlSet001\Services\IPRIP\ImagePath: "%SystemRoot%\System32\svchost.exe -k netsvcs"**  **HKLM\SYSTEM\ControlSet001\Services\IPRIP\DisplayName: "Intranet Network Awareness (INA+)"**  **HKLM\SYSTEM\ControlSet001\Services\IPRIP\DisplayName: "Intranet Network Awareness (INA+)"** | | |
| **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):** | | |
| **Network: Windows XP 6.11, practicalmalwareanalysis.com**  **Host: Intranet Network Awareness (INA+), IPRIP (service name)** | | |
| **Key Functionality:** | | |
| **Dll loads into svchost.exe, the dll becons every 10min to the DNS name. Then does a GET request for /serve.html HTTP/1.1 over port 80. Uses computers name appended to user agent.** | | |
| **Purpose:** | | |
|  | | |
| **Persistence:** | | |
|  | | |
| **Environment-specific Impact:** | | |
|  | | |
| **Root Cause:** | | |
|  | | |
| **Attribution:** | | |
|  | | |