**Malware Analysis Template**

|  |  |  |
| --- | --- | --- |
| **BACKGROUND** | | |
| **Date:** | |  |
| **Hostname:** | |  |
| **File Name:** | |  |
| **File Location:** | |  |
| **Notification Vector:** | |  |
| **STATIC ANALYSIS** | | |
| **File Hash:** |  | |
| **File Size (bytes):** |  | |
| **File Type:** |  | |
| **Import Hash:** |  | |
| **Icon Graphic:** |  | |
| **Signed?:** |  | |
| **Packer/Compiler Info:** |  | |
| **Compile Time:** |  | |
| **Section Hashes:** | | |
|  | | |
| **File Properties:** Description, version, file header characteristics | | |
|  | | |
| **Strings:** Functions, registry keys, file paths, domains, IP addresses, commands, error messages | | |
|  | | |
| **Entropy:** File and sections | | |
|  | | |
| **Imported/Exported Functions:** Risky API patterns (see “Tips for Reverse Engineering Malicious Code” cheat sheet) | | |
|  | | |
| **Open Source Research:** VirusTotal detections, search engine output, free sandbox results | | |
|  | | |
| **BEHAVIORAL ANALYSIS** | | |
| **File System Artifacts:** Files and registry keys created/modified/deleted | | |
|  | | |
| **Network Artifacts:** Required services, domains, IP addresses, ports, protocols, user-agent | | |
|  | | |
| **Memory Analysis:** Rogue processes, code injection, API hooks, network artifacts | | |
|  | | |
| **Open Source Research:** VirusTotal, PassiveTotal, Open Threat Exchange | | |
|  | | |
| **CODE ANALYSIS** | | |
| **Static Code Analysis:** Pivot by API patterns and strings, observe function arguments, variables, return values and control flow | | |
|  | | |
| **Debugging:** Set API breakpoints, monitor stack/registers/addresses, unpack malware | | |
|  | | |
| **ANALYSIS SUMMARY** | | |
| **Key Host and Network Indicators of Compromise (IOCs):** | | |
|  | | |
| **Key Functionality:** | | |
|  | | |
| **Malware Type and Family (if identified):** | | |
|  | | |