Indicator Type	Trigger / Metric	Example Keywords / APIs	Explanation / Notes
Network API	Count of network-related APIs	`socket`, `connect`, `send`, `recv`, `inet_pton`, `htons`	High count indicates possible network communication for C2 or data exfiltration.
Suspicious API	Count of APIs often misused by malware	`system`, `exec`, `popen`, `CreateProcess`, `fork`	APIs enabling arbitrary execution, command injection, or control flow manipulation.
Persistence API	Count of registry/cron/startup modification APIs	`SetWindowsHookEx`, `RegSetValue`, `crontab`	Indicates attempts to persist across reboots.
Dynamic Loading / Injection	Count of APIs for loading external modules or code	`LoadLibrary`, `dlopen`, `CreateRemoteThread`, `VirtualAlloc`	Used for code injection or loading external modules at runtime.
Suspicious Strings	Count of suspicious keywords or patterns in strings	`"password"`, `"cmd.exe"`, `"Decoded string"`, `"exec"`	Could be hard-coded passwords, commands, or encoded payloads.
Base64 Blobs	Count of Base64-encoded strings	Any string matching Base64 regex: `[A-Za-z0-9+/=]{20,}`	May hide malicious payloads or configuration data.
Hex Blobs	Count of large hexadecimal blobs	Strings like `0x90,0x90,0xCC...`	Often used for embedded binaries or shellcode.
High Entropy Blobs	Count of high-entropy regions in code/data	Any sequence with Shannon entropy > 7.5	Indicates obfuscation, encryption, or compressed payloads.
Obfuscation Matches	Number of matched obfuscation patterns	Control flow flattening, variable masking patterns	Detects obfuscation tricks to evade analysis.
Network Indicators (IPs/URLs/Domains)	Count or list of IPs, URLs, and domains	`192.168.1.100`, `malicious.com`	Helps detect C2 servers, phishing endpoints, or malware communication targets.