Indicator Type	Trigger / Metric	Example Keywords / APIs	Triggered in `func0()`	Explanation / Notes
Network API	Count of network-related APIs	`socket`, `connect`, `send`, `recv`, `inet_pton`, `htons`	4 (`socket`, `htons`, `inet_pton`, `connect`)	Code opens a socket and connects to IP `192.168.1.100:4444`, potential C2 comms.
Suspicious API	Count of APIs often misused by malware	`system`, `exec`, `popen`, `CreateProcess`, `fork`	1 (`system`)	Executes shell command `"echo Hello > test.txt"`; could be malicious if modified.
Persistence API	Count of registry/cron/ startup modification APIs	`SetWindowsHookEx`, `RegSetValue`, `crontab`	0	No persistence behavior in this code.
Dynamic Loading / Injection	Count of APIs for loading external modules or code	`LoadLibrary`, `dlopen`, `CreateRemoteThread`, `VirtualAlloc`	0	No code injection or dynamic library loading.
Suspicious Strings	Count of suspicious keywords or patterns in strings	`"password"`, `"cmd.exe"`, `"Decoded string"`, `"exec"`	1 (`"Decoded string: %s"`)	Shows possible encoded or sensitive string handling.
Base64 Blobs	Count of Base64-encoded strings	`[A-Za-z0-9+/=]{20,}`	1 (`"U29tZSBzZWNyZXQgdGV4dCBmb3IgdGVzdGluZw=="`)	Encoded string present; could hide payload or config.
Hex Blobs	Count of large hexadecimal	`0x90,0x90,0xCC...`	0	No embedded hex blobs.
High Entropy Blobs	Count of high-entropy regions in code/data	Shannon entropy > 7.5	0	No obfuscation detected.
Obfuscation Matches	Number of matched obfuscation patterns	Control flow flattening, variable masking patterns	0	Code is straightforward; no obfuscation.
Network Indicators (IPs/URLs/Domains)	IPs, URLs, domains	`192.168.1.100`	1 IP	Hardcoded C2-style IP present.