Threat Name: Windows_API_Detection

Threat Category: System Call Monitoring

Threat Description: The YARA rule Windows_API detects the usage of Windows API functions commonly used in file operations and malware behaviors.

Indicators of Compromise (IoCs):

"CreateFile", "ReadFile", "WriteFile"

Detection Mechanism:

Flags files containing two or more of these Windows API calls.

Possible Attribution & Use Cases:

Used in malware with file read/write capabilities.

Recommended Actions:

Investigate suspicious binaries interacting with system files.