Threat Name: Registry_Key_Detection

Threat Category: Windows Registry Monitoring

Threat Description:

The YARA rule Registry_Key detects references to Windows Registry keys, which may indicate system modifications, persistence mechanisms, or malware configurations.

Indicators of Compromise (IoCs):

"HKEY_" (Windows registry key prefix)

Detection Mechanism:

Matches Windows Registry key manipulations in scripts and logs.

Possible Attribution & Use Cases:

Used in malware persistence and system modifications.

Recommended Actions:

Monitor registry changes for signs of unauthorized modifications.