Threat Name: APT_Loader_Win64_REDFLARE

Threat Category: Advanced Persistent Threat (APT), Malware Loader

Threat Description: The YARA rule APT_Loader_Win64_REDFLARE_1 detects the REDFLARE malware loader, a 64-bit executable used in APT campaigns to execute malicious payloads in memory.

Indicators of Compromise (IoCs):

Memory allocation and loading patterns:

41 B9 40 00 00 00 41 B8 00 30 00 00 33 C9

Unique assembly sequences related to in-memory execution.

MD5 Hash: f20824fa6e5c81e3804419f108445368

Detection Mechanism:

Identifies malware loaders in 64-bit Windows executables.

Possible Attribution & Use Cases:

Used in covert malware deployment by APT groups.

Avoids disk-based detection by executing payloads in-memory.

Recommended Actions:

Monitor for unusual memory allocation events.

Conduct behavioral analysis to detect fileless malware execution.

Author & Attribution:

Rule Author: FireEye