Threat Name: APT_Loader_Raw64_REDFLARE

Threat Category: Malware Loader, In-Memory Execution

Description: This YARA rule is designed to detect a specific pattern of bytes in a file, indicated by the hexadecimal string $load. The rule is intended to identify a potential loader associated with the APT group REDFLARE. The rule looks for a sequence of bytes that match the provided pattern, which may indicate the presence of malicious code. This rule was created by FireEye and is useful for identifying specific malware variants or threat actors known to use this loader technique.

Threat Description:

The YARA rule APT_Loader_Raw64_REDFLARE_1 is designed to detect raw 64-bit loader components of the REDFLARE malware framework. Unlike traditional PE files, this loader operates without a standard Windows executable header to evade detection.

Indicators of Compromise (IoCs):

Hex signature related to raw memory execution:

EB ?? 58 48 8B 10 4C 8B 48 ?? 48 8B C8

MD5 Hash: 5e14f77f85fd9a5be46e7f04b8a144f5

Detection Mechanism:

Identifies headerless binary execution.

Matches low-level shellcode execution patterns.

Possible Attribution & Use Cases:

Used in stealthy in-memory execution for malware deployment.

Recommended Actions:

Monitor for suspicious memory execution patterns.

Implement EDR rules to detect raw executable memory allocations.

Author & Attribution:

Rule Author: FireEye