Threat Name: APT_Trojan_Win_REDFLARE

Threat Category: Advanced Persistent Threat (APT), Remote Access Trojan (RAT)

Threat Description: The YARA rule APT_Trojan_Win_REDFLARE_1 detects RedFlare malware, a trojan used in APT operations for command execution and persistence.

Indicators of Compromise (IoCs):

Function calls associated with malware activity:

"initialize", "runCommand", "stop", "VirtualAllocEx", "WriteProcessMemory", "stop", "fini" fullword

MD5 Hash: 100d73b35f23b2fe84bf7cd37140bf4d,4e7e90c7147ee8aa01275894734f4492

Detection Mechanism:

Identifies malware persistence mechanisms and execution commands.

Possible Attribution & Use Cases:

Used in long-term cyber-espionage operations.

Recommended Actions:

Block suspicious remote access attempts.

Author & Attribution:

Rule Author: FireEye