Threat Name: Trojan_Raw_Generic_4

Threat Category: Malware, Trojan

Threat Description: The YARA rule detects generic Trojan behaviors based on executable binary patterns. It focuses on identifying obfuscation techniques used to bypass traditional signature-based detection.

Indicators of Compromise (IoCs): Unique binary instruction sequences commonly used in Trojanized executables.

MD5 Hash: f41074be5b423afb02a74bc74222e35d

Detection Mechanism: Uses low-level instruction patterns to identify packed or obfuscated trojans.

Possible Attribution & Use Cases:

Used for Trojan malware detection across various APT campaigns.

Recommended Actions:

Perform static and dynamic malware analysis.

Investigate files that evade traditional antivirus detection.

Author & Attribution:

Rule Author: FireEye