Threat Name: Loader_Win_Generic_20

Threat Category: Malware Loader, Code Injection

Threat Description: The YARA rule Loader_Win_Generic_20 detects a generic Windows malware loader designed for code injection and process hollowing techniques.

Indicators of Compromise (IoCs):

Memory manipulation functions:

"VirtualProtect", "malloc"

Strings:

$s0 = { 8B [1-16] 89 [1-16] E8 [4-32] F3 A4 [0-16] 89 [1-8] E8 }

$s2 = { 83 EC [4-24] 00 10 00 00 [4-24] C7 44 24 ?? ?? 00 00 00 [0-8] FF 15 [4-24] 89 [1-4] 89 [1-4] 89 [1-8] FF 15 [4-16] 3? ?? 7? [4-24] 20 00 00 00 [4-24] FF 15 [4-32] F3 A5 }

$si1 = "VirtualProtect" fullword

$si2 = "malloc" fullword

MD5 Hash: 5125979110847d35a338caac6bff2aa8

Detection Mechanism: Identifies executable files attempting to inject shellcode into processes.

Possible Attribution & Use Cases: Used in malware obfuscation and payload execution.

Recommended Actions:

Monitor memory allocations for signs of process injection.

Analyze any detections for potential malware persistence techniques.

Author & Attribution:

Rule Author: FireEye