Threat Name: HackTool_Win32_AndrewSpecial

Threat Category: Exploitation Tool, Shellcode Injector

Threat Description: The YARA rule HackTool_Win32_AndrewSpecial_1 detects Windows-based shellcode loaders, often used in malware droppers and post-exploitation tools.

Indicators of Compromise (IoCs):

Shellcode sequences related to Win32 PE exploitation.

MD5 Hash: e89efa88e3fda86be48c0cc8f2ef7230

Detection Mechanism:

Identifies inline assembly techniques used for process injection.

Possible Attribution & Use Cases:

Strings:

```
$dump = { 6A 00 68 FF FF 1F 00 FF 15 [4] 89 45 ?? 83 [2] 00 [1-50] 6A 00 68 80 00 00 00 6A 02 6A 00 6A 00 68 00 00 00 10 68 [4] FF 15 [4] 89 45 [10-70] 6A 00 6A 00 6A 00 6A 02 8B [2-4] 5? 8B [2-4] 5? 8B [2-4] 5? E8 [4-20] FF 15 }
$shellcode_x86 = { B8 3C 00 00 00 33 C9 8D 54 24 04 64 FF 15 C0 00 00 00 83 C4 04 C2 14 00 }
$shellcode_x86_inline = { C6 45 ?? B8 C6 45 ?? 3C C6 45 ?? 00 C6 45 ?? 00 C6 45 ?? 00 C6 45 ?? 33 C6 45 ?? C9 C6 45 ?? 8D C6 45 ?? 54 C6 45 ?? 24 C6 45 ?? 04 C6 45 ?? 64 C6 45 ?? FF C6 45 ?? 15 C6 45 ?? C0 C6 45 ?? 00 C6 45 ?? 00 C6 45 ?? 00 C6 45 ?? 83 C6 45 ?? C4 C6 45 ?? 04 C6 45 ?? C2 C6 45 ?? 14 C6 45 ?? 00 }
```

Used in APT malware to evade detection.

Could be a part of exploit kits targeting Windows systems.

Recommended Actions:

Block malicious shellcode execution.

Monitor memory for unusual injection attempts.

Author & Attribution:

Rule Author: FireEye