Threat Name: HackTool_MSIL_SHARPZEROLOGON

Threat Category: Exploitation Tool, Windows Domain Exploitation

Threat Description: The YARA rule HackTool_MSIL_SHARPZEROLOGON_1 detects SharpZeroLogon, a .NET-based proof-of-concept exploit for the CVE-2020-1472 (ZeroLogon) vulnerability in Windows domain controllers.

Indicators of Compromise (IoCs):

TypeLibGUID / ProjectGuid: 15ce9a3c-4609-4184-87b2-e29fc5e2b770

MD5 Hash: dd8805d0e470e59b829d98397507d8c2

Detection Mechanism:

Detects .NET Portable Executables (PEs) that contain project GUIDs linked to SharpZeroLogon.

condition: (uint16(0) == 0x5A4D and uint32(uint32(0x3C)) == 0x00004550) and any of them

Possible Attribution & Use Cases:

Used for privilege escalation and domain takeover.

Recommended Actions:

Patch Windows domain controllers against CVE-2020-1472.

Monitor unauthorized authentication attempts on Netlogon service.

Author & Attribution:

Rule Author: FireEye

Reference: ZeroLogon Advisory