Threat Name: APT_HackTool_MSIL_SHARPGOPHER

Threat Category: Exploitation Tool, Credential Theft

Threat Description: The YARA rule APT_HackTool_MSIL_SHARPGOPHER_1 detects SharpGopher, a tool used for exploiting Gopher protocol vulnerabilities in Windows.

Indicators of Compromise (IoCs):

TypeLibGUID: 83413a89-7f5f-4c3f-805d-f4692bc60173

MD5 Hash: dd8805d0e470e59b829d98397507d8c2

Detection Mechanism: Matches .NET project GUIDs linked to SharpGopher.

Possible Attribution & Use Cases: Used for stealing credentials via Gopher-based exploits.

Recommended Actions: Monitor for abnormal Gopher protocol traffic.

Author & Attribution:

Rule Author: FireEye