Threat Name: HackTool_MSIL_CoreHound

Threat Category: Malware / HackTool, .NET-based Threat

Threat Description: The YARA rule HackTool_MSIL_CoreHound_1 is designed to detect malicious .NET executables that contain a specific TypeLibGUID linked to the CoreHound project. This project can be used for offensive security purposes, including post-exploitation activities.

Indicators of Compromise (IoCs):

TypeLibGUID / ProjectGuid: 1fff2aee-a540-4613-94ee-4f208b30c599

MD5 Hash: dd8805d0e470e59b829d98397507d8c2

Detection Mechanism:

Detects .NET PE files containing the CoreHound project GUID.

Matches unique project GUIDs linked to known hacking tools.

Possible Attribution & Use Cases:

Used for penetration testing and potential malicious activity.

Recommended Actions:

Investigate detected files for unauthorized red team activity.

Monitor .NET PE file execution for suspicious behavior.

Author & Attribution:

Rule Author: FireEye