Threat Name: HackTool_MSIL_KeeFarce

Threat Category: Credential Theft, Password Dumper

Threat Description: The YARA rule HackTool_MSIL_KeeFarce_1 is designed to detect KeeFarce, a credential theft tool that extracts stored passwords from KeePass password manager databases.

Indicators of Compromise (IoCs):

TypeLibGUID: 17589ea6-fcc9-44bb-92ad-d5b3eea6af03

MD5 Hash: dd8805d0e470e59b829d98397507d8c2

Detection Mechanism:

Identifies .NET PE files associated with KeeFarce?s memory dumping functions.

Strings:

"17589ea6-fcc9-44bb-92ad-d5b3eea6af03" ascii nocase wide

Possible Attribution & Use Cases:

Used by attackers to extract stored credentials from KeePass.

Recommended Actions:

Monitor KeePass execution for suspicious memory access.

Restrict unauthorized access to password management tools.

Author & Attribution:

Rule Author: FireEye

Reference: KeeFarce GitHub