Threat Name: HackTool_MSIL_Rubeus

Threat Category: Credential Theft, Red Team Tool

Threat Description: The YARA rule HackTool_MSIL_Rubeus_1 is designed to detect Rubeus, a .NET-based tool used for Kerberos ticket manipulation. It is commonly used for pass-the-ticket (PTT) attacks, Kerberoasting, and overpass-the-hash techniques.

Indicators of Compromise (IoCs):

TypeLibGUID: 658C8B7F-3664-4A95-9572-A3E5871DFC06

MD5 Hash: 66e0681a500c726ed52e5ea9423d2654

rev = 4

condition: uint16(0) == 0x5A4D and $typelibguid

Detection Mechanism:

Detects .NET PE files that contain a ProjectGuid associated with Rubeus.

Possible Attribution & Use Cases:

Used by red teams and threat actors for Kerberos exploitation.

Recommended Actions:

Monitor for abnormal Kerberos ticket requests.

Investigate unauthorized use of Rubeus on endpoints.

Author & Attribution:

Rule Author: FireEye

Reference: Rubeus GitHub