Threat Name: Trojan_MSIL_GORAT_Plugin_DOTNET

Threat Category: Advanced Persistent Threat (APT), Remote Access Trojan (RAT)

Threat Description: The YARA rule Trojan_MSIL_GORAT_Plugin_DOTNET_1 detects .NET-based RAT plugins linked to the GORAT malware family.

Indicators of Compromise (IoCs):

TypeLibGUIDs:

cd9407d0-fc8d-41ed-832d-da94daa3e064

fc3daedf-1d01-4490-8032-b978079d8c2d

MD5 Hash: dd8805d0e470e59b829d98397507d8c2

Detection Mechanism:

Identifies .NET PE files containing project GUIDs associated with GORAT RAT plugins.

Possible Attribution & Use Cases:

Used for covert remote access operations.

Recommended Actions:

Investigate persistent RAT activity on detected hosts.

Author & Attribution:

Rule Author: FireEye