Threat Name: Loader_MSIL_NETAssemblyInject

Threat Category: Code Injection, Malware Loader

Threat Description: The YARA rule Loader_MSIL_NETAssemblyInject_1 detects .NET-based process injection tools that manipulate assemblies to execute payloads in memory. The rule looks for specific TypeLibGUIDs associated with the NET-Assembly-Inject project.

Indicators of Compromise (IoCs):

TypeLibGUIDs:

af09c8c3-b271-4c6c-8f48-d5f0e1d1cac6

c5e56650-dfb0-4cd9-8d06-51defdad5da1

e8fa7329-8074-4675-9588-d73f88a8b5b6

MD5 Hash: dd8805d0e470e59b829d98397507d8c2

Detection Mechanism:

Identifies .NET PE files with project GUIDs linked to assembly injection techniques.

Possible Attribution & Use Cases:

Used for process hollowing and memory injection attacks.

Recommended Actions:

Monitor for suspicious .NET PE execution.

Investigate code injection behaviors in running processes.

Author & Attribution:

Rule Author: FireEye