# TTP Detail – T1574.014

## TTP Information

Name: AppDomainManager

Description: Adversaries may execute their own malicious payloads by hijacking how the .NET `AppDomainManager` loads assemblies. The .NET framework uses the `AppDomainManager` class to create and manage one or more isolated runtime environments (called application domains) inside a process to host the execution of .NET applications. Assemblies (`.exe` or `.dll` binaries compiled to run as .NET code) may be loaded into an application domain as executable code.(Citation: Microsoft App Domains)

Known as "AppDomainManager injection," adversaries may execute arbitrary code by hijacking how .NET applications load assemblies. For example, malware may create a custom application domain inside a target process to load and execute an arbitrary assembly. Alternatively, configuration files (`.config`) or process environment variables that define .NET runtime settings may be tampered with to instruct otherwise benign .NET applications to load a malicious assembly (identified by name) into the target process.(Citation: PenTestLabs AppDomainManagerInject)(Citation: PwC Yellow Liderc)(Citation: Rapid7 AppDomain Manager Injection)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence

**•** mitre-attack: privilege-escalation

**•** mitre-attack: defense-evasion

## Malware

* IMAPLoader