# TTP Detail – T1574.012

## TTP Information

Name: COR\_PROFILER

Description: Adversaries may leverage the COR\_PROFILER environment variable to hijack the execution flow of programs that load the .NET CLR. The COR\_PROFILER is a .NET Framework feature which allows developers to specify an unmanaged (or external of .NET) profiling DLL to be loaded into each .NET process that loads the Common Language Runtime (CLR). These profilers are designed to monitor, troubleshoot, and debug managed code executed by the .NET CLR.(Citation: Microsoft Profiling Mar 2017)(Citation: Microsoft COR\_PROFILER Feb 2013)

The COR\_PROFILER environment variable can be set at various scopes (system, user, or process) resulting in different levels of influence. System and user-wide environment variable scopes are specified in the Registry, where a [Component Object Model](https://attack.mitre.org/techniques/T1559/001) (COM) object can be registered as a profiler DLL. A process scope COR\_PROFILER can also be created in-memory without modifying the Registry. Starting with .NET Framework 4, the profiling DLL does not need to be registered as long as the location of the DLL is specified in the COR\_PROFILER\_PATH environment variable.(Citation: Microsoft COR\_PROFILER Feb 2013)

Adversaries may abuse COR\_PROFILER to establish persistence that executes a malicious DLL in the context of all .NET processes every time the CLR is invoked. The COR\_PROFILER can also be used to elevate privileges (ex: [Bypass User Account Control](https://attack.mitre.org/techniques/T1548/002)) if the victim .NET process executes at a higher permission level, as well as to hook and [Impair Defenses](https://attack.mitre.org/techniques/T1562) provided by .NET processes.(Citation: RedCanary Mockingbird May 2020)(Citation: Red Canary COR\_PROFILER May 2020)(Citation: Almond COR\_PROFILER Apr 2019)(Citation: GitHub OmerYa Invisi-Shell)(Citation: subTee .NET Profilers May 2017)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: persistence

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

**•** mitre-attack: defense-evasion

## Malware

* DarkTortilla

## APTs (Intrusion Sets)

* Blue Mockingbird