# TTP Detail – T1127.002

## TTP Information

Name: ClickOnce

Description: Adversaries may use ClickOnce applications (.appref-ms and .application files) to proxy execution of code through a trusted Windows utility.(Citation: Burke/CISA ClickOnce BlackHat) ClickOnce is a deployment that enables a user to create self-updating Windows-based .NET applications (i.e, .XBAP, .EXE, or .DLL) that install and run from a file share or web page with minimal user interaction. The application launches as a child process of DFSVC.EXE, which is responsible for installing, launching, and updating the application.(Citation: SpectorOps Medium ClickOnce)

Because ClickOnce applications receive only limited permissions, they do not require administrative permissions to install.(Citation: Microsoft Learn ClickOnce) As such, adversaries may abuse ClickOnce to proxy execution of malicious code without needing to escalate privileges.

ClickOnce may be abused in a number of ways. For example, an adversary may rely on [User Execution](https://attack.mitre.org/techniques/T1204). When a user visits a malicious website, the .NET malware is disguised as legitimate software and a ClickOnce popup is displayed for installation.(Citation: NetSPI ClickOnce)

Adversaries may also abuse ClickOnce to execute malware via a [Rundll32](https://attack.mitre.org/techniques/T1218/011) script using the command `rundll32.exe dfshim.dll,ShOpenVerbApplication1`.(Citation: LOLBAS /Dfsvc.exe)

Additionally, an adversary can move the ClickOnce application file to a remote user’s startup folder for continued malicious code deployment (i.e., [Registry Run Keys / Startup Folder](https://attack.mitre.org/techniques/T1547/001)).(Citation: Burke/CISA ClickOnce BlackHat)(Citation: Burke/CISA ClickOnce Paper)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion