# TTP Detail – T1218.008

## TTP Information

Name: Odbcconf

Description: Adversaries may abuse odbcconf.exe to proxy execution of malicious payloads. Odbcconf.exe is a Windows utility that allows you to configure Open Database Connectivity (ODBC) drivers and data source names.(Citation: Microsoft odbcconf.exe) The Odbcconf.exe binary may be digitally signed by Microsoft.

Adversaries may abuse odbcconf.exe to bypass application control solutions that do not account for its potential abuse. Similar to [Regsvr32](https://attack.mitre.org/techniques/T1218/010), odbcconf.exe has a <code>REGSVR</code> flag that can be misused to execute DLLs (ex: <code>odbcconf.exe /S /A &lbrace;REGSVR "C:\Users\Public\file.dll"&rbrace;</code>). (Citation: LOLBAS Odbcconf)(Citation: TrendMicro Squiblydoo Aug 2017)(Citation: TrendMicro Cobalt Group Nov 2017)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Bumblebee
* Raspberry Robin

## APTs (Intrusion Sets)

* Cobalt Group