# TTP Detail – T1218.010

## TTP Information

Name: Regsvr32

Description: Adversaries may abuse Regsvr32.exe to proxy execution of malicious code. Regsvr32.exe is a command-line program used to register and unregister object linking and embedding controls, including dynamic link libraries (DLLs), on Windows systems. The Regsvr32.exe binary may also be signed by Microsoft. (Citation: Microsoft Regsvr32)

Malicious usage of Regsvr32.exe may avoid triggering security tools that may not monitor execution of, and modules loaded by, the regsvr32.exe process because of allowlists or false positives from Windows using regsvr32.exe for normal operations. Regsvr32.exe can also be used to specifically bypass application control using functionality to load COM scriptlets to execute DLLs under user permissions. Since Regsvr32.exe is network and proxy aware, the scripts can be loaded by passing a uniform resource locator (URL) to file on an external Web server as an argument during invocation. This method makes no changes to the Registry as the COM object is not actually registered, only executed. (Citation: LOLBAS Regsvr32) This variation of the technique is often referred to as a "Squiblydoo" and has been used in campaigns targeting governments. (Citation: Carbon Black Squiblydoo Apr 2016) (Citation: FireEye Regsvr32 Targeting Mongolian Gov)

Regsvr32.exe can also be leveraged to register a COM Object used to establish persistence via [Component Object Model Hijacking](https://attack.mitre.org/techniques/T1546/015). (Citation: Carbon Black Squiblydoo Apr 2016)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* AppleSeed
* Astaroth
* Derusbi
* Dridex
* EVILNUM
* Egregor
* Emotet
* HermeticWizard
* Hi-Zor
* More\_eggs
* Mori
* Orz
* QakBot
* Ragnar Locker
* Raspberry Robin
* RogueRobin
* Saint Bot
* Squirrelwaffle
* Valak
* Xbash

## Tools

* Covenant
* Koadic

## APTs (Intrusion Sets)

* APT19
* APT32
* Blue Mockingbird
* Cobalt Group
* Deep Panda
* Inception
* Kimsuky
* Leviathan
* TA551
* WIRTE