# TTP Detail – T1218.014

## TTP Information

Name: MMC

Description: Adversaries may abuse mmc.exe to proxy execution of malicious .msc files. Microsoft Management Console (MMC) is a binary that may be signed by Microsoft and is used in several ways in either its GUI or in a command prompt.(Citation: win\_mmc)(Citation: what\_is\_mmc) MMC can be used to create, open, and save custom consoles that contain administrative tools created by Microsoft, called snap-ins. These snap-ins may be used to manage Windows systems locally or remotely. MMC can also be used to open Microsoft created .msc files to manage system configuration.(Citation: win\_msc\_files\_overview)

For example, <code>mmc C:\Users\foo\admintools.msc /a</code> will open a custom, saved console msc file in author mode.(Citation: win\_mmc) Another common example is <code>mmc gpedit.msc</code>, which will open the Group Policy Editor application window.

Adversaries may use MMC commands to perform malicious tasks. For example, <code>mmc wbadmin.msc delete catalog -quiet</code> deletes the backup catalog on the system (i.e. [Inhibit System Recovery](https://attack.mitre.org/techniques/T1490)) without prompts to the user (Note: <code>wbadmin.msc</code> may only be present by default on Windows Server operating systems).(Citation: win\_wbadmin\_delete\_catalog)(Citation: phobos\_virustotal)

Adversaries may also abuse MMC to execute malicious .msc files. For example, adversaries may first create a malicious registry Class Identifier (CLSID) subkey, which uniquely identifies a [Component Object Model](https://attack.mitre.org/techniques/T1559/001) class object.(Citation: win\_clsid\_key) Then, adversaries may create custom consoles with the “Link to Web Address” snap-in that is linked to the malicious CLSID subkey.(Citation: mmc\_vulns) Once the .msc file is saved, adversaries may invoke the malicious CLSID payload with the following command: <code>mmc.exe -Embedding C:\path\to\test.msc</code>.(Citation: abusing\_com\_reg)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion