# TTP Detail – T1546.003

## TTP Information

Name: Windows Management Instrumentation Event Subscription

Description: Adversaries may establish persistence and elevate privileges by executing malicious content triggered by a Windows Management Instrumentation (WMI) event subscription. WMI can be used to install event filters, providers, consumers, and bindings that execute code when a defined event occurs. Examples of events that may be subscribed to are the wall clock time, user login, or the computer's uptime.(Citation: Mandiant M-Trends 2015)

Adversaries may use the capabilities of WMI to subscribe to an event and execute arbitrary code when that event occurs, providing persistence on a system.(Citation: FireEye WMI SANS 2015)(Citation: FireEye WMI 2015) Adversaries may also compile WMI scripts – using `mofcomp.exe` –into Windows Management Object (MOF) files (.mof extension) that can be used to create a malicious subscription.(Citation: Dell WMI Persistence)(Citation: Microsoft MOF May 2018)

WMI subscription execution is proxied by the WMI Provider Host process (WmiPrvSe.exe) and thus may result in elevated SYSTEM privileges.

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

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

**•** mitre-attack: persistence

## Malware

* BADHATCH
* HOPLIGHT
* Kevin
* POSHSPY
* POWERTON
* RegDuke
* Sardonic
* SeaDuke
* TrailBlazer
* adbupd
* metaMain

## Tools

* PoshC2
* SILENTTRINITY

## APTs (Intrusion Sets)

* APT29
* APT33
* Blue Mockingbird
* FIN8
* HEXANE
* Leviathan
* Metador
* Mustang Panda
* Rancor
* Turla