# TTP Detail – T1084

## TTP Information

Name: Windows Management Instrumentation Event Subscription

Description: Windows Management Instrumentation (WMI) can be used to install event filters, providers, consumers, and bindings that execute code when a defined event occurs. 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. Adversaries may attempt to evade detection of this technique by compiling WMI scripts into Windows Management Object (MOF) files (.mof extension). (Citation: Dell WMI Persistence) Examples of events that may be subscribed to are the wall clock time or the computer's uptime. (Citation: Kazanciyan 2014) Several threat groups have reportedly used this technique to maintain persistence. (Citation: Mandiant M-Trends 2015)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: persistence