# TTP Detail – T1021.006

## TTP Information

Name: Windows Remote Management

Description: Adversaries may use [Valid Accounts](https://attack.mitre.org/techniques/T1078) to interact with remote systems using Windows Remote Management (WinRM). The adversary may then perform actions as the logged-on user.

WinRM is the name of both a Windows service and a protocol that allows a user to interact with a remote system (e.g., run an executable, modify the Registry, modify services).(Citation: Microsoft WinRM) It may be called with the `winrm` command or by any number of programs such as PowerShell.(Citation: Jacobsen 2014) WinRM can be used as a method of remotely interacting with [Windows Management Instrumentation](https://attack.mitre.org/techniques/T1047).(Citation: MSDN WMI)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: lateral-movement

## Malware

* Cobalt Strike

## Tools

* Brute Ratel C4
* SILENTTRINITY

## APTs (Intrusion Sets)

* Chimera
* FIN13
* Threat Group-3390
* Wizard Spider