# TTP Detail – T1047

## TTP Information

Name: Windows Management Instrumentation

Description: Adversaries may abuse Windows Management Instrumentation (WMI) to execute malicious commands and payloads. WMI is designed for programmers and is the infrastructure for management data and operations on Windows systems.(Citation: WMI 1-3) WMI is an administration feature that provides a uniform environment to access Windows system components.  
  
The WMI service enables both local and remote access, though the latter is facilitated by [Remote Services](https://attack.mitre.org/techniques/T1021) such as [Distributed Component Object Model](https://attack.mitre.org/techniques/T1021/003) and [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006).(Citation: WMI 1-3) Remote WMI over DCOM operates using port 135, whereas WMI over WinRM operates over port 5985 when using HTTP and 5986 for HTTPS.(Citation: WMI 1-3) (Citation: Mandiant WMI)  
  
An adversary can use WMI to interact with local and remote systems and use it as a means to execute various behaviors, such as gathering information for [Discovery](https://attack.mitre.org/tactics/TA0007) as well as [Execution](https://attack.mitre.org/tactics/TA0002) of commands and payloads.(Citation: Mandiant WMI) For example, `wmic.exe` can be abused by an adversary to delete shadow copies with the command `wmic.exe Shadowcopy Delete` (i.e., [Inhibit System Recovery](https://attack.mitre.org/techniques/T1490)).(Citation: WMI 6)  
  
\*\*Note:\*\* `wmic.exe` is deprecated as of January of 2024, with the WMIC feature being “disabled by default” on Windows 11+. WMIC will be removed from subsequent Windows releases and replaced by [PowerShell](https://attack.mitre.org/techniques/T1059/001) as the primary WMI interface.(Citation: WMI 7,8) In addition to PowerShell and tools like `wbemtool.exe`, COM APIs can also be used to programmatically interact with WMI via C++, .NET, VBScript, etc.(Citation: WMI 7,8)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: execution

## Malware

* Action RAT
* Agent Tesla
* Akira
* Astaroth
* Avaddon
* BADHATCH
* Bazar
* Black Basta
* BlackCat
* BlackEnergy
* Bumblebee
* CharmPower
* Cobalt Strike
* DEATHRANSOM
* DarkGate
* DarkTortilla
* DarkWatchman
* DustySky
* EKANS
* EVILNUM
* Emotet
* EvilBunny
* FELIXROOT
* FIVEHANDS
* FlawedAmmyy
* FunnyDream
* GravityRAT
* HALFBAKED
* HELLOKITTY
* HOPLIGHT
* HermeticWizard
* IMAPLoader
* INC Ransomware
* IcedID
* KOMPROGO
* Kazuar
* Latrodectus
* LockBit 2.0
* Lucifer
* LunarWeb
* Maze
* Meteor
* Micropsia
* MoleNet
* Mosquito
* Netwalker
* NotPetya
* Octopus
* Olympic Destroyer
* OopsIE
* POWERSTATS
* POWRUNER
* ProLock
* PyDCrypt
* QakBot
* RATANKBA
* REvil
* Raspberry Robin
* Remexi
* RogueRobin
* SUNBURST
* SVCReady
* Sardonic
* SharpStage
* ShrinkLocker
* Sibot
* Snip3
* SocGholish
* StoneDrill
* Stuxnet
* SysUpdate
* TAMECAT
* Ursnif
* Valak
* WannaCry
* Zebrocy
* jRAT

## Tools

* Brute Ratel C4
* Covenant
* CrackMapExec
* Empire
* Impacket
* Koadic
* PoshC2
* PowerSploit
* SILENTTRINITY

## APTs (Intrusion Sets)

* APT29
* APT32
* APT41
* APT42
* Aquatic Panda
* BlackByte
* Blue Mockingbird
* Chimera
* Cinnamon Tempest
* Deep Panda
* Earth Lusca
* Ember Bear
* FIN13
* FIN6
* FIN7
* FIN8
* GALLIUM
* Gamaredon Group
* INC Ransom
* Indrik Spider
* Lazarus Group
* Leviathan
* Lotus Blossom
* Magic Hound
* MuddyWater
* Mustang Panda
* Naikon
* OilRig
* Sandworm Team
* Stealth Falcon
* TA2541
* Threat Group-3390
* ToddyCat
* Velvet Ant
* Volt Typhoon
* Windshift
* Wizard Spider
* menuPass