# TTP Detail – T1059.001

## TTP Information

Name: PowerShell

Description: Adversaries may abuse PowerShell commands and scripts for execution. PowerShell is a powerful interactive command-line interface and scripting environment included in the Windows operating system.(Citation: TechNet PowerShell) Adversaries can use PowerShell to perform a number of actions, including discovery of information and execution of code. Examples include the <code>Start-Process</code> cmdlet which can be used to run an executable and the <code>Invoke-Command</code> cmdlet which runs a command locally or on a remote computer (though administrator permissions are required to use PowerShell to connect to remote systems).

PowerShell may also be used to download and run executables from the Internet, which can be executed from disk or in memory without touching disk.

A number of PowerShell-based offensive testing tools are available, including [Empire](https://attack.mitre.org/software/S0363), [PowerSploit](https://attack.mitre.org/software/S0194), [PoshC2](https://attack.mitre.org/software/S0378), and PSAttack.(Citation: Github PSAttack)

PowerShell commands/scripts can also be executed without directly invoking the <code>powershell.exe</code> binary through interfaces to PowerShell's underlying <code>System.Management.Automation</code> assembly DLL exposed through the .NET framework and Windows Common Language Interface (CLI).(Citation: Sixdub PowerPick Jan 2016)(Citation: SilentBreak Offensive PS Dec 2015)(Citation: Microsoft PSfromCsharp APR 2014)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: execution

## Malware

* Akira
* AppleSeed
* AutoIt backdoor
* BADHATCH
* BONDUPDATER
* Bandook
* Bazar
* Black Basta
* Bumblebee
* CHIMNEYSWEEP
* CharmPower
* Clambling
* Cobalt Strike
* ComRAT
* CreepyDrive
* CreepySnail
* Cuba
* DarkGate
* DarkWatchman
* Denis
* DownPaper
* Egregor
* Emotet
* FatDuke
* Ferocious
* FlawedAmmyy
* GLASSTOKEN
* GRIFFON
* Gootloader
* HALFBAKED
* HAMMERTOSS
* Hancitor
* Helminth
* IPsec Helper
* JCry
* JSS Loader
* KGH\_SPY
* KOCTOPUS
* KONNI
* KeyBoy
* LitePower
* Lizar
* LockBit 2.0
* LockBit 3.0
* Lokibot
* Lumma Stealer
* LunarWeb
* Mafalda
* Meteor
* MoleNet
* Mosquito
* NETWIRE
* Netwalker
* OSX\_OCEANLOTUS.D
* POSHSPY
* POWERSOURCE
* POWERSTATS
* POWERTON
* POWRUNER
* PS1
* PUNCHBUGGY
* Pillowmint
* PowGoop
* PowerExchange
* PowerLess
* PowerPunch
* PowerShower
* PowerStallion
* Prestige
* PyDCrypt
* Pysa
* QUADAGENT
* QakBot
* RATANKBA
* REvil
* RansomHub
* RegDuke
* Revenge RAT
* RogueRobin
* SHARPSTATS
* SMOKEDHAM
* SQLRat
* Saint Bot
* Sardonic
* SeaDuke
* ServHelper
* SharpStage
* ShrinkLocker
* Snip3
* Socksbot
* Spica
* Squirrelwaffle
* StrelaStealer
* StrongPity
* TAMECAT
* TRANSLATEXT
* TrickBot
* Troll Stealer
* Ursnif
* Valak
* WarzoneRAT
* WellMess
* WhisperGate
* Woody RAT
* Xbash
* ZeroCleare
* Zeus Panda
* njRAT

## Tools

* AADInternals
* BloodHound
* ConnectWise
* Covenant
* CrackMapExec
* Donut
* Empire
* Koadic
* PowerSploit
* Pupy
* SILENTTRINITY
* Sliver

## APTs (Intrusion Sets)

* APT19
* APT28
* APT29
* APT3
* APT32
* APT33
* APT38
* APT39
* APT41
* APT42
* APT5
* Akira
* Aquatic Panda
* BRONZE BUTLER
* BlackByte
* Blue Mockingbird
* CURIUM
* Chimera
* Cinnamon Tempest
* Cobalt Group
* Confucius
* CopyKittens
* Daggerfly
* DarkHydrus
* DarkVishnya
* Deep Panda
* Dragonfly
* Earth Lusca
* Ember Bear
* FIN10
* FIN13
* FIN6
* FIN7
* FIN8
* Fox Kitten
* GALLIUM
* GOLD SOUTHFIELD
* Gallmaker
* Gamaredon Group
* Gorgon Group
* HAFNIUM
* HEXANE
* Inception
* Indrik Spider
* Kimsuky
* Lazarus Group
* LazyScripter
* Leviathan
* Magic Hound
* Molerats
* MoustachedBouncer
* MuddyWater
* Mustang Panda
* Nomadic Octopus
* OilRig
* Patchwork
* Play
* Poseidon Group
* RedCurl
* Saint Bear
* Sandworm Team
* Sidewinder
* Silence
* Stealth Falcon
* Storm-1811
* TA2541
* TA459
* TA505
* TeamTNT
* Threat Group-3390
* Thrip
* ToddyCat
* Tonto Team
* Turla
* Volt Typhoon
* WIRTE
* Winter Vivern
* Wizard Spider
* menuPass