# TTP Detail – T1059.003

## TTP Information

Name: Windows Command Shell

Description: Adversaries may abuse the Windows command shell for execution. The Windows command shell ([cmd](https://attack.mitre.org/software/S0106)) is the primary command prompt on Windows systems. The Windows command prompt can be used to control almost any aspect of a system, with various permission levels required for different subsets of commands. The command prompt can be invoked remotely via [Remote Services](https://attack.mitre.org/techniques/T1021) such as [SSH](https://attack.mitre.org/techniques/T1021/004).(Citation: SSH in Windows)

Batch files (ex: .bat or .cmd) also provide the shell with a list of sequential commands to run, as well as normal scripting operations such as conditionals and loops. Common uses of batch files include long or repetitive tasks, or the need to run the same set of commands on multiple systems.

Adversaries may leverage [cmd](https://attack.mitre.org/software/S0106) to execute various commands and payloads. Common uses include [cmd](https://attack.mitre.org/software/S0106) to execute a single command, or abusing [cmd](https://attack.mitre.org/software/S0106) interactively with input and output forwarded over a command and control channel.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: execution

## Malware

* 4H RAT
* ABK
* ADVSTORESHELL
* Action RAT
* Akira
* Anchor
* Astaroth
* AuTo Stealer
* AuditCred
* BACKSPACE
* BADHATCH
* BADNEWS
* BBK
* BISCUIT
* BLACKCOFFEE
* BLINDINGCAN
* BONDUPDATER
* Babuk
* BabyShark
* BackConfig
* Bandook
* Bankshot
* Bazar
* Bisonal
* Black Basta
* BlackCat
* BlackMould
* BoxCaon
* Bumblebee
* CALENDAR
* CARROTBAT
* Carbanak
* Cardinal RAT
* Caterpillar WebShell
* Chaes
* CharmPower
* China Chopper
* Clambling
* Clop
* Cobalt Strike
* Cobian RAT
* CoinTicker
* ComRAT
* Comnie
* Conti
* CozyCar
* Crimson
* Cuba
* DEADEYE
* DUSTTRAP
* DanBot
* DarkComet
* DarkGate
* DarkTortilla
* DarkWatchman
* Daserf
* DealersChoice
* Denis
* Dipsind
* DnsSystem
* DownPaper
* DropBook
* Dtrack
* ECCENTRICBANDWAGON
* Egregor
* Emissary
* Emotet
* EnvyScout
* EvilBunny
* Exaramel for Windows
* FELIXROOT
* Felismus
* Flagpro
* FlawedAmmyy
* FunnyDream
* Gelsemium
* Gold Dragon
* GoldMax
* GoldenSpy
* Goopy
* GravityRAT
* GreyEnergy
* GrimAgent
* H1N1
* HARDRAIN
* HAWKBALL
* HOMEFRY
* HOPLIGHT
* HTTPBrowser
* Hannotog
* Helminth
* HermeticWiper
* HermeticWizard
* Hi-Zor
* HiddenWasp
* Hikit
* HotCroissant
* IPsec Helper
* InnaputRAT
* InvisiMole
* Ixeshe
* JCry
* JHUHUGIT
* JPIN
* KEYMARBLE
* KGH\_SPY
* KOCTOPUS
* KOMPROGO
* KONNI
* Kapeka
* Kasidet
* Kazuar
* Kevin
* KeyBoy
* Latrodectus
* LightNeuron
* Linfo
* Lizar
* LockBit 2.0
* Lokibot
* LookBack
* LoudMiner
* Lucifer
* LunarWeb
* MURKYTOP
* Mafalda
* MagicRAT
* Manjusaka
* MarkiRAT
* Maze
* MechaFlounder
* MegaCortex
* Megazord
* Metamorfo
* Meteor
* Micropsia
* Milan
* MirageFox
* Mis-Type
* Misdat
* Mivast
* MoleNet
* MoonWind
* More\_eggs
* Mosquito
* MultiLayer Wiper
* NETEAGLE
* NETWIRE
* NanoCore
* NavRAT
* Nebulae
* Netwalker
* Nightdoor
* ODAgent
* OceanSalt
* OilBooster
* Okrum
* OopsIE
* Orz
* OutSteel
* PHOREAL
* PLAINTEE
* PLEAD
* POWRUNER
* Peppy
* Pikabot
* PingPull
* Pisloader
* PlugX
* PoetRAT
* PoisonIvy
* Pony
* PowerDuke
* Proxysvc
* Pteranodon
* PyDCrypt
* QUADAGENT
* QakBot
* RATANKBA
* RCSession
* RDAT
* REvil
* RGDoor
* ROADSWEEP
* RTM
* Ragnar Locker
* RainyDay
* RansomHub
* Raspberry Robin
* RedLeaves
* Remexi
* Revenge RAT
* Rising Sun
* RobbinHood
* RogueRobin
* RunningRAT
* Ryuk
* S-Type
* SDBbot
* SEASHARPEE
* SLOTHFULMEDIA
* SNUGRIDE
* SQLRat
* STARWHALE
* SUGARUSH
* SYSCON
* Saint Bot
* Sakula
* SamSam
* SampleCheck5000
* Samurai
* Sardonic
* SeaDuke
* Seasalt
* ServHelper
* Seth-Locker
* Shark
* SharpDisco
* SharpStage
* ShimRat
* SideTwist
* Siloscape
* Small Sieve
* Spark
* Squirrelwaffle
* StreamEx
* StrelaStealer
* StrifeWater
* TAINTEDSCRIBE
* TAMECAT
* TDTESS
* TEXTMATE
* TSCookie
* TURNEDUP
* TYPEFRAME
* Taidoor
* Tarrask
* TinyTurla
* TinyZBot
* TrickBot
* Trojan.Karagany
* Troll Stealer
* Turian
* UBoatRAT
* UPPERCUT
* USBferry
* Umbreon
* Uroburos
* Volgmer
* WEBC2
* WarzoneRAT
* WastedLocker
* WellMess
* WhisperGate
* Wiarp
* Woody RAT
* XTunnel
* ZLib
* Zebrocy
* Zeus Panda
* ZxShell
* adbupd
* ccf32
* hcdLoader
* httpclient
* jRAT
* njRAT
* xCaon
* zwShell

## Tools

* Brute Ratel C4
* Covenant
* Empire
* Koadic
* MCMD
* Out1
* PcShare
* QuasarRAT
* Remcos
* SILENTTRINITY
* cmd

## APTs (Intrusion Sets)

* APT1
* APT18
* APT28
* APT3
* APT32
* APT37
* APT38
* APT41
* APT5
* Agrius
* Aquatic Panda
* BRONZE BUTLER
* BlackByte
* Blue Mockingbird
* Chimera
* Cinnamon Tempest
* Cobalt Group
* Dark Caracal
* Darkhotel
* Dragonfly
* FIN10
* FIN13
* FIN6
* FIN7
* FIN8
* Fox Kitten
* GALLIUM
* Gamaredon Group
* Gorgon Group
* HAFNIUM
* Higaisa
* INC Ransom
* Indrik Spider
* Ke3chang
* Kimsuky
* Lazarus Group
* LazyScripter
* Machete
* Magic Hound
* Metador
* MuddyWater
* Mustang Panda
* Nomadic Octopus
* OilRig
* Patchwork
* Play
* Rancor
* RedCurl
* Saint Bear
* Silence
* Sowbug
* Storm-1811
* Suckfly
* TA505
* TA551
* TA577
* TeamTNT
* Threat Group-1314
* Threat Group-3390
* ToddyCat
* Tropic Trooper
* Turla
* Volt Typhoon
* Winter Vivern
* Wizard Spider
* ZIRCONIUM
* admin@338
* menuPass