# TTP Detail – T1071.001

## TTP Information

Name: Web Protocols

Description: Adversaries may communicate using application layer protocols associated with web traffic to avoid detection/network filtering by blending in with existing traffic. Commands to the remote system, and often the results of those commands, will be embedded within the protocol traffic between the client and server.

Protocols such as HTTP/S(Citation: CrowdStrike Putter Panda) and WebSocket(Citation: Brazking-Websockets) that carry web traffic may be very common in environments. HTTP/S packets have many fields and headers in which data can be concealed. An adversary may abuse these protocols to communicate with systems under their control within a victim network while also mimicking normal, expected traffic.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: command-and-control

## Malware

* 3PARA RAT
* 4H RAT
* ABK
* ADVSTORESHELL
* ANDROMEDA
* Action RAT
* Agent Tesla
* Amadey
* Anchor
* AppleJeus
* AppleSeed
* Aria-body
* AuTo Stealer
* Avenger
* BACKSPACE
* BADHATCH
* BADNEWS
* BBK
* BBSRAT
* BLINDINGCAN
* BLUELIGHT
* BOLDMOVE
* BUBBLEWRAP
* BackConfig
* BadPatch
* Bankshot
* Bazar
* Bisonal
* BlackEnergy
* BlackMould
* BoomBox
* Bundlore
* CHIMNEYSWEEP
* CHOPSTICK
* COATHANGER
* CORESHELL
* Carbanak
* Carberp
* Carbon
* Cardinal RAT
* ChChes
* Chaes
* CharmPower
* China Chopper
* Clambling
* CloudDuke
* Cobalt Strike
* ComRAT
* Comnie
* CosmicDuke
* CozyCar
* CreepyDrive
* CreepySnail
* Crimson
* Crutch
* Cuckoo Stealer
* Cyclops Blink
* DEATHRANSOM
* DRATzarus
* Dacls
* DanBot
* DarkComet
* DarkTortilla
* DarkWatchman
* Daserf
* DealersChoice
* Diavol
* Dipsind
* Doki
* DownPaper
* Dridex
* Drovorub
* DustySky
* Dyre
* ELMER
* Egregor
* Elise
* Emissary
* Emotet
* Epic
* EvilBunny
* Exaramel for Linux
* Explosive
* FELIXROOT
* FRAMESTING
* FatDuke
* Felismus
* Final1stspy
* Flagpro
* FlawedAmmyy
* FoggyWeb
* Gazer
* Gelsemium
* GeminiDuke
* Get2
* Gold Dragon
* GoldFinder
* GoldMax
* GoldenSpy
* Gomir
* Goopy
* Grandoreiro
* GravityRAT
* GreyEnergy
* GrimAgent
* GuLoader
* HAMMERTOSS
* HAWKBALL
* HTTPBrowser
* Helminth
* Hi-Zor
* Hikit
* HyperBro
* IPsec Helper
* IceApple
* IcedID
* Industroyer
* InvisiMole
* Ixeshe
* JHUHUGIT
* KEYPLUG
* KGH\_SPY
* KONNI
* KOPILUWAK
* Kapeka
* Kazuar
* Kevin
* Keydnap
* Kinsing
* Komplex
* LIGHTWIRE
* LOWBALL
* Latrodectus
* LightSpy
* Line Dancer
* Line Runner
* LiteDuke
* LitePower
* LockBit 3.0
* Lokibot
* LookBack
* Lumma Stealer
* LunarWeb
* MacSpy
* Machete
* Mafalda
* MagicRAT
* Mango
* Manjusaka
* MarkiRAT
* Maze
* MechaFlounder
* Metamorfo
* Micropsia
* Milan
* MiniDuke
* Mis-Type
* Mongall
* More\_eggs
* Mori
* NETEAGLE
* NETWIRE
* NGLite
* NICECURL
* NOKKI
* Neo-reGeorg
* Neoichor
* Ninja
* OLDBAIT
* OSX\_OCEANLOTUS.D
* Octopus
* OilBooster
* Okrum
* OnionDuke
* OopsIE
* OutSteel
* OwaAuth
* P.A.S. Webshell
* PLEAD
* POWERTON
* POWRUNER
* PULSECHECK
* PUNCHBUGGY
* Pandora
* Peppy
* PinchDuke
* PingPull
* PlugX
* PoetRAT
* PolyglotDuke
* Pony
* PowGoop
* PowerShower
* Proxysvc
* Psylo
* Pteranodon
* QUADAGENT
* QUIETCANARY
* QakBot
* QuietSieve
* RATANKBA
* RCSession
* RDAT
* REvil
* RGDoor
* RIPTIDE
* ROKRAT
* RTM
* Raccoon Stealer
* RainyDay
* Ramsay
* Raspberry Robin
* Reaver
* RedLeaves
* Regin
* Remexi
* Remsec
* Rising Sun
* S-Type
* SLIGHTPULSE
* SLOTHFULMEDIA
* SMOKEDHAM
* SNUGRIDE
* STARWHALE
* STEADYPULSE
* SUGARDUMP
* SUNBURST
* SUPERNOVA
* SVCReady
* Sagerunex
* Saint Bot
* Sakula
* SampleCheck5000
* Samurai
* SeaDuke
* Seasalt
* ServHelper
* ShadowPad
* Shamoon
* Shark
* ShimRat
* ShrinkLocker
* Sibot
* SideTwist
* Small Sieve
* Smoke Loader
* SnappyTCP
* SoreFang
* Spark
* SpeakUp
* Squirrelwaffle
* StealBit
* StrelaStealer
* StrongPity
* Stuxnet
* Sys10
* TAMECAT
* TRANSLATEXT
* TSCookie
* Taidoor
* ThiefQuest
* TinyTurla
* Tomiris
* Torisma
* TrailBlazer
* TrickBot
* Trojan.Karagany
* Troll Stealer
* Turian
* UBoatRAT
* UPPERCUT
* Uroburos
* Ursnif
* VBShower
* VERMIN
* Valak
* VaporRage
* Vasport
* WIREFIRE
* WellMess
* WhisperGate
* WinMM
* WindTail
* Winnti for Linux
* Winnti for Windows
* Woody RAT
* XLoader
* Xbash
* YAHOYAH
* ZLib
* Zebrocy
* ZeroT
* Zeus Panda
* ZxShell
* down\_new
* httpclient
* metaMain
* njRAT
* pngdowner
* reGeorg
* xCaon

## Tools

* Brute Ratel C4
* CSPY Downloader
* Covenant
* Donut
* Empire
* FRP
* Koadic
* MCMD
* Mythic
* Out1
* PcShare
* PoshC2
* Pupy
* Quick Assist
* ShimRatReporter
* Sliver

## APTs (Intrusion Sets)

* APT18
* APT19
* APT28
* APT32
* APT33
* APT37
* APT38
* APT39
* APT41
* APT42
* BITTER
* BRONZE BUTLER
* BlackByte
* Chimera
* Cobalt Group
* Confucius
* Daggerfly
* Dark Caracal
* FIN13
* FIN4
* FIN8
* Gamaredon Group
* HAFNIUM
* Higaisa
* Inception
* Ke3chang
* Kimsuky
* Lazarus Group
* LuminousMoth
* Magic Hound
* Metador
* Moonstone Sleet
* MuddyWater
* Mustang Panda
* OilRig
* Orangeworm
* Rancor
* RedCurl
* RedEcho
* Rocke
* Sandworm Team
* Sea Turtle
* Sidewinder
* SilverTerrier
* Stealth Falcon
* TA505
* TA551
* TeamTNT
* Threat Group-3390
* Tropic Trooper
* Turla
* WIRTE
* Windshift
* Winter Vivern
* Wizard Spider