# TTP Detail – T1041

## TTP Information

Name: Exfiltration Over C2 Channel

Description: Adversaries may steal data by exfiltrating it over an existing command and control channel. Stolen data is encoded into the normal communications channel using the same protocol as command and control communications.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: exfiltration

## Malware

* ADVSTORESHELL
* Amadey
* AppleJeus
* AppleSeed
* Astaroth
* Attor
* AuTo Stealer
* BACKSPACE
* BADHATCH
* BLINDINGCAN
* BLUELIGHT
* Bandook
* Bankshot
* Bisonal
* BoxCaon
* Bumblebee
* CHIMNEYSWEEP
* CallMe
* Cannon
* Carberp
* Caterpillar WebShell
* CharmPower
* Chrommme
* CreepySnail
* Crimson
* Crutch
* Cuckoo Stealer
* Cyclops Blink
* DUSTTRAP
* DarkGate
* DnsSystem
* Doki
* Drovorub
* DustySky
* Dyre
* EVILNUM
* Ebury
* Emotet
* Flagpro
* FlawedAmmyy
* FoggyWeb
* FunnyDream
* GoldMax
* GoldenSpy
* Goopy
* Grandoreiro
* GrimAgent
* HAWKBALL
* HOPLIGHT
* HotCroissant
* IPsec Helper
* IceApple
* Industroyer
* KGH\_SPY
* KONNI
* KOPILUWAK
* Kessel
* Kevin
* Latrodectus
* LightNeuron
* LightSpy
* Line Dancer
* Line Runner
* LitePower
* Lokibot
* Lumma Stealer
* LunarMail
* MacMa
* Machete
* Mafalda
* MagicRAT
* Mango
* Manjusaka
* MarkiRAT
* MechaFlounder
* Metamorfo
* Mis-Type
* Misdat
* Mispadu
* MobileOrder
* Mongall
* NETEAGLE
* NightClub
* ODAgent
* Octopus
* OilBooster
* Okrum
* OopsIE
* OutSteel
* Penquin
* Pikabot
* PingPull
* PoetRAT
* PowerExchange
* PowerShower
* Proxysvc
* Psylo
* Pteranodon
* QakBot
* RDAT
* REvil
* ROKRAT
* Raccoon Stealer
* Remexi
* Rising Sun
* RotaJakiro
* S-Type
* SDBbot
* SLOTHFULMEDIA
* SMOKEDHAM
* STARWHALE
* SUGARDUMP
* SVCReady
* Sagerunex
* Shark
* SharpDisco
* ShrinkLocker
* SideTwist
* Solar
* SombRAT
* Spark
* Squirrelwaffle
* StrelaStealer
* StrifeWater
* StrongPity
* Stuxnet
* SysUpdate
* TRANSLATEXT
* TajMahal
* ThiefQuest
* Tomiris
* Torisma
* TrickBot
* Troll Stealer
* Ursnif
* Valak
* WarzoneRAT
* Woody RAT
* XCSSET
* ZLib
* Zebrocy
* metaMain
* njRAT

## Tools

* Empire
* Imminent Monitor
* PcShare
* Pupy
* SILENTTRINITY
* ShimRatReporter
* Sliver

## APTs (Intrusion Sets)

* APT3
* APT32
* APT39
* Agrius
* BlackByte
* CURIUM
* Chimera
* Confucius
* GALLIUM
* Gamaredon Group
* Higaisa
* Ke3chang
* Kimsuky
* Lazarus Group
* Leviathan
* LuminousMoth
* MuddyWater
* Sandworm Team
* Stealth Falcon
* Winter Vivern
* Wizard Spider
* ZIRCONIUM