# TTP Detail – T1573.001

## TTP Information

Name: Symmetric Cryptography

Description: Adversaries may employ a known symmetric encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Symmetric encryption algorithms use the same key for plaintext encryption and ciphertext decryption. Common symmetric encryption algorithms include AES, DES, 3DES, Blowfish, and RC4.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

## Malware

* 3PARA RAT
* 4H RAT
* ADVSTORESHELL
* Attor
* Azorult
* BADCALL
* BADNEWS
* BBSRAT
* BLINDINGCAN
* Bandook
* Bazar
* BendyBear
* Bisonal
* Bonadan
* Bumblebee
* CHOPSTICK
* CORESHELL
* CallMe
* Carbanak
* Cardinal RAT
* ChChes
* Chaos
* CharmPower
* Cobalt Strike
* Comnie
* CosmicDuke
* Daserf
* Derusbi
* Dipsind
* Downdelph
* Dridex
* Duqu
* Ebury
* Elise
* Emissary
* Emotet
* Epic
* Explosive
* FALLCHILL
* FakeM
* FatDuke
* Felismus
* FlawedAmmyy
* FoggyWeb
* Gazer
* GreyEnergy
* GrimAgent
* H1N1
* HAMMERTOSS
* Helminth
* Hi-Zor
* HiddenWasp
* Hikit
* HotCroissant
* Hydraq
* HyperStack
* IceApple
* InvisiMole
* KEYMARBLE
* KONNI
* Kobalos
* Komplex
* LIGHTWIRE
* Latrodectus
* LightNeuron
* LockBit 3.0
* LookBack
* Lucifer
* LunarWeb
* Lurid
* Machete
* Mafalda
* Mango
* Metamorfo
* Mongall
* MoonWind
* More\_eggs
* Mosquito
* NDiskMonitor
* NETEAGLE
* NETWIRE
* NGLite
* NanoCore
* Nebulae
* Ninja
* OSX\_OCEANLOTUS.D
* Okrum
* PLAINTEE
* PLEAD
* POWERTON
* Pandora
* Pikabot
* PingPull
* PipeMon
* PlugX
* PoisonIvy
* Prikormka
* QUIETCANARY
* QakBot
* RDAT
* RIPTIDE
* RTM
* RainyDay
* RedLeaves
* Rifdoor
* RotaJakiro
* SLIGHTPULSE
* SMOKEDHAM
* SNUGRIDE
* SUNBURST
* Sakula
* Samurai
* Sardonic
* SeaDuke
* SideTwist
* SodaMaster
* Solar
* SombRAT
* StrifeWater
* Stuxnet
* Sys10
* SysUpdate
* TAINTEDSCRIBE
* TAMECAT
* TSCookie
* Taidoor
* Torisma
* TrickBot
* Troll Stealer
* UBoatRAT
* UPPERCUT
* Uroburos
* Volgmer
* WIREFIRE
* WarzoneRAT
* WellMess
* Winnti for Linux
* Winnti for Windows
* Woody RAT
* XCSSET
* ZIPLINE
* ZeroT
* down\_new
* gh0st RAT
* httpclient
* metaMain
* xCaon

## Tools

* FRP
* QuasarRAT
* Sliver

## APTs (Intrusion Sets)

* APT28
* APT33
* BRONZE BUTLER
* Darkhotel
* Higaisa
* Inception
* Lazarus Group
* MuddyWater
* Mustang Panda
* RedCurl
* Stealth Falcon
* Volt Typhoon
* ZIRCONIUM