# TTP Detail – T1573.002

## TTP Information

Name: Asymmetric Cryptography

Description: Adversaries may employ a known asymmetric encryption algorithm to conceal command and control traffic rather than relying on any inherent protections provided by a communication protocol. Asymmetric cryptography, also known as public key cryptography, uses a keypair per party: one public that can be freely distributed, and one private. Due to how the keys are generated, the sender encrypts data with the receiver’s public key and the receiver decrypts the data with their private key. This ensures that only the intended recipient can read the encrypted data. Common public key encryption algorithms include RSA and ElGamal.

For efficiency, many protocols (including SSL/TLS) use symmetric cryptography once a connection is established, but use asymmetric cryptography to establish or transmit a key. As such, these protocols are classified as [Asymmetric Cryptography](https://attack.mitre.org/techniques/T1573/002).

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

## Malware

* ADVSTORESHELL
* Attor
* BADHATCH
* BISCUIT
* BOLDMOVE
* Bazar
* CHOPSTICK
* COATHANGER
* Carbon
* Cobalt Strike
* ComRAT
* Cyclops Blink
* DarkWatchman
* Doki
* Dridex
* Gazer
* GoldMax
* Gomir
* Grandoreiro
* GreyEnergy
* GrimAgent
* Hi-Zor
* IcedID
* J-magic
* KEYPLUG
* Kobalos
* LITTLELAMB.WOOLTEA
* Lumma Stealer
* LunarWeb
* Machete
* Mango
* Metamorfo
* Mispadu
* NICECURL
* OilBooster
* PITSTOP
* POSHSPY
* POWERSTATS
* Pay2Key
* Penquin
* PoetRAT
* REvil
* Rising Sun
* Sagerunex
* Sardonic
* ServHelper
* Small Sieve
* SnappyTCP
* SodaMaster
* SombRAT
* StrongPity
* Sykipot
* TinyTurla
* Trojan.Karagany
* Uroburos
* Volgmer
* WannaCry
* WellMail
* WellMess
* Woody RAT
* XTunnel
* Zebrocy
* adbupd

## Tools

* Covenant
* Empire
* FRP
* Koadic
* Mythic
* Pupy
* Sliver
* Tor

## APTs (Intrusion Sets)

* APT42
* Cobalt Group
* FIN6
* FIN8
* OilRig
* RedCurl
* RedEcho
* TA2541
* Tropic Trooper
* Velvet Ant