# TTP Detail – T1571

## TTP Information

Name: Non-Standard Port

Description: Adversaries may communicate using a protocol and port pairing that are typically not associated. For example, HTTPS over port 8088(Citation: Symantec Elfin Mar 2019) or port 587(Citation: Fortinet Agent Tesla April 2018) as opposed to the traditional port 443. Adversaries may make changes to the standard port used by a protocol to bypass filtering or muddle analysis/parsing of network data.

Adversaries may also make changes to victim systems to abuse non-standard ports. For example, Registry keys and other configuration settings can be used to modify protocol and port pairings.(Citation: change\_rdp\_port\_conti)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

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

## Malware

* BADCALL
* Bankshot
* BendyBear
* Cyclops Blink
* Derusbi
* Emotet
* GoldenSpy
* GravityRAT
* HARDRAIN
* HOPLIGHT
* Hannotog
* MacMa
* Metamorfo
* MoonWind
* OSX\_OCEANLOTUS.D
* Pikabot
* PingPull
* PlugX
* PoetRAT
* RTM
* Raspberry Robin
* RedLeaves
* RotaJakiro
* SUGARUSH
* Sardonic
* StrongPity
* TYPEFRAME
* TrickBot
* WellMail
* ZxShell
* njRAT

## Tools

* Covenant
* QuasarRAT

## APTs (Intrusion Sets)

* APT-C-36
* APT32
* APT33
* DarkVishnya
* Ember Bear
* FIN7
* Lazarus Group
* Magic Hound
* RedEcho
* Rocke
* Sandworm Team
* Silence
* Velvet Ant
* WIRTE