# TTP Detail – T1562.004

## TTP Information

Name: Disable or Modify System Firewall

Description: Adversaries may disable or modify system firewalls in order to bypass controls limiting network usage. Changes could be disabling the entire mechanism as well as adding, deleting, or modifying particular rules. This can be done numerous ways depending on the operating system, including via command-line, editing Windows Registry keys, and Windows Control Panel.

Modifying or disabling a system firewall may enable adversary C2 communications, lateral movement, and/or data exfiltration that would otherwise not be allowed. For example, adversaries may add a new firewall rule for a well-known protocol (such as RDP) using a non-traditional and potentially less securitized port (i.e. [Non-Standard Port](https://attack.mitre.org/techniques/T1571)).(Citation: change\_rdp\_port\_conti)

Adversaries may also modify host networking settings that indirectly manipulate system firewalls, such as interface bandwidth or network connection request thresholds.(Citation: Huntress BlackCat) Settings related to enabling abuse of various [Remote Services](https://attack.mitre.org/techniques/T1021) may also indirectly modify firewall rules.

In ESXi, firewall rules may be modified directly via the esxcli command line interface (e.g., via `esxcli network firewall set`) or via the vCenter user interface.(Citation: Trellix Rnasomhouse 2024)(Citation: Broadcom ESXi Firewall)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* BACKSPACE
* BADCALL
* BPFDoor
* BlackByte 2.0 Ransomware
* CookieMiner
* Cyclops Blink
* DarkComet
* Grandoreiro
* H1N1
* HARDRAIN
* HOPLIGHT
* Hannotog
* InvisiMole
* Kasidet
* NanoCore
* PlugX
* PyDCrypt
* Remsec
* ShrinkLocker
* TYPEFRAME
* ZxShell
* njRAT

## Tools

* netsh

## APTs (Intrusion Sets)

* APT38
* BlackByte
* Carbanak
* Dragonfly
* Kimsuky
* Lazarus Group
* Magic Hound
* Moses Staff
* OilRig
* Rocke
* Salt Typhoon
* TeamTNT
* ToddyCat
* Velvet Ant