# TTP Detail – T1048

## TTP Information

Name: Exfiltration Over Alternative Protocol

Description: Adversaries may steal data by exfiltrating it over a different protocol than that of the existing command and control channel. The data may also be sent to an alternate network location from the main command and control server.

Alternate protocols include FTP, SMTP, HTTP/S, DNS, SMB, or any other network protocol not being used as the main command and control channel. Adversaries may also opt to encrypt and/or obfuscate these alternate channels.

[Exfiltration Over Alternative Protocol](https://attack.mitre.org/techniques/T1048) can be done using various common operating system utilities such as [Net](https://attack.mitre.org/software/S0039)/SMB or FTP.(Citation: Palo Alto OilRig Oct 2016) On macOS and Linux <code>curl</code> may be used to invoke protocols such as HTTP/S or FTP/S to exfiltrate data from a system.(Citation: 20 macOS Common Tools and Techniques)

Many IaaS and SaaS platforms (such as Microsoft Exchange, Microsoft SharePoint, GitHub, and AWS S3) support the direct download of files, emails, source code, and other sensitive information via the web console or [Cloud API](https://attack.mitre.org/techniques/T1059/009).

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: exfiltration

## Malware

* Bundlore
* Chaes
* FrameworkPOS
* Hydraq
* Kobalos
* PoetRAT

## Tools

* AADInternals

## APTs (Intrusion Sets)

* Play
* TeamTNT