# TTP Detail – T1567.002

## TTP Information

Name: Exfiltration to Cloud Storage

Description: Adversaries may exfiltrate data to a cloud storage service rather than over their primary command and control channel. Cloud storage services allow for the storage, edit, and retrieval of data from a remote cloud storage server over the Internet.

Examples of cloud storage services include Dropbox and Google Docs. Exfiltration to these cloud storage services can provide a significant amount of cover to the adversary if hosts within the network are already communicating with the service.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: exfiltration

## Malware

* BoomBox
* BoxCaon
* Clambling
* CreepyDrive
* Crutch
* HAMMERTOSS
* ODAgent
* Octopus
* OilBooster
* Pcexter
* ROKRAT
* RainyDay

## Tools

* Empire
* Rclone

## APTs (Intrusion Sets)

* Akira
* Chimera
* Cinnamon Tempest
* Confucius
* Earth Lusca
* Ember Bear
* FIN7
* HAFNIUM
* HEXANE
* Indrik Spider
* Kimsuky
* Leviathan
* LuminousMoth
* POLONIUM
* Scattered Spider
* Threat Group-3390
* ToddyCat
* Turla
* Wizard Spider
* ZIRCONIUM