# TTP Detail – T1115

## TTP Information

Name: Clipboard Data

Description: Adversaries may collect data stored in the clipboard from users copying information within or between applications.

For example, on Windows adversaries can access clipboard data by using <code>clip.exe</code> or <code>Get-Clipboard</code>.(Citation: MSDN Clipboard)(Citation: clip\_win\_server)(Citation: CISA\_AA21\_200B) Additionally, adversaries may monitor then replace users’ clipboard with their data (e.g., [Transmitted Data Manipulation](https://attack.mitre.org/techniques/T1565/002)).(Citation: mining\_ruby\_reversinglabs)

macOS and Linux also have commands, such as <code>pbpaste</code>, to grab clipboard contents.(Citation: Operating with EmPyre)

## Threat-Mapped Scoring

Score: 2.8

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: collection

## Malware

* Agent Tesla
* Astaroth
* Attor
* CHIMNEYSWEEP
* Cadelspy
* Catchamas
* Clambling
* CosmicDuke
* DarkComet
* DarkGate
* DarkTortilla
* Explosive
* FlawedAmmyy
* Grandoreiro
* Helminth
* JHUHUGIT
* KONNI
* MacSpy
* Machete
* MarkiRAT
* Melcoz
* Metamorfo
* MgBot
* Mispadu
* ROKRAT
* RTM
* Remexi
* RunningRAT
* TajMahal
* TinyZBot
* VERMIN
* XLoader
* Zeus Panda
* jRAT

## Tools

* Empire
* Koadic
* Remcos
* SILENTTRINITY

## APTs (Intrusion Sets)

* APT38
* APT39
* OilRig