# TTP Detail – T1560

## TTP Information

Name: Archive Collected Data

Description: An adversary may compress and/or encrypt data that is collected prior to exfiltration. Compressing the data can help to obfuscate the collected data and minimize the amount of data sent over the network.(Citation: DOJ GRU Indictment Jul 2018) Encryption can be used to hide information that is being exfiltrated from detection or make exfiltration less conspicuous upon inspection by a defender.

Both compression and encryption are done prior to exfiltration, and can be performed using a utility, 3rd party library, or custom method.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: collection

## Malware

* ADVSTORESHELL
* Agent Tesla
* AppleSeed
* Aria-body
* BLUELIGHT
* Backdoor.Oldrea
* Bumblebee
* Cadelspy
* Chrommme
* Daserf
* Dtrack
* Epic
* Exaramel for Windows
* FELIXROOT
* Gold Dragon
* JumbledPath
* KONNI
* Kessel
* LightNeuron
* Lizar
* LoFiSe
* Lurid
* Machete
* NETWIRE
* Pillowmint
* PowerLess
* Prikormka
* Proton
* Raccoon Stealer
* Remexi
* RunningRAT
* Spica
* TAINTEDSCRIBE
* Troll Stealer
* VERMIN
* WellMail
* XCSSET
* Zebrocy

## Tools

* BloodHound
* Empire
* ShimRatReporter

## APTs (Intrusion Sets)

* APT28
* APT32
* Axiom
* BlackByte
* Dragonfly
* Ember Bear
* FIN6
* Ke3chang
* Lazarus Group
* Leviathan
* LuminousMoth
* Patchwork
* menuPass