# TTP Detail – T1560.003

## TTP Information

Name: Archive via Custom Method

Description: An adversary may compress or encrypt data that is collected prior to exfiltration using a custom method. Adversaries may choose to use custom archival methods, such as encryption with XOR or stream ciphers implemented with no external library or utility references. Custom implementations of well-known compression algorithms have also been used.(Citation: ESET Sednit Part 2)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: collection

## Malware

* ADVSTORESHELL
* Agent.btz
* Attor
* BLUELIGHT
* Duqu
* FLASHFLOOD
* FoggyWeb
* FrameworkPOS
* FunnyDream
* HAWKBALL
* InvisiMole
* MESSAGETAP
* Machete
* NETWIRE
* OSX\_OCEANLOTUS.D
* Okrum
* OopsIE
* OwaAuth
* RGDoor
* Ramsay
* RawPOS
* Reaver
* Rising Sun
* SPACESHIP
* SUGARDUMP
* SombRAT
* Squirrelwaffle
* StrongPity
* Stuxnet
* T9000
* metaMain

## APTs (Intrusion Sets)

* CopyKittens
* FIN6
* Kimsuky
* Lazarus Group
* Lotus Blossom
* Mustang Panda