# TTP Detail – T1657

## TTP Information

Name: Financial Theft

Description: Adversaries may steal monetary resources from targets through extortion, social engineering, technical theft, or other methods aimed at their own financial gain at the expense of the availability of these resources for victims. Financial theft is the ultimate objective of several popular campaign types including extortion by ransomware,(Citation: FBI-ransomware) business email compromise (BEC) and fraud,(Citation: FBI-BEC) "pig butchering,"(Citation: wired-pig butchering) bank hacking,(Citation: DOJ-DPRK Heist) and exploiting cryptocurrency networks.(Citation: BBC-Ronin)

Adversaries may [Compromise Accounts](https://attack.mitre.org/techniques/T1586) to conduct unauthorized transfers of funds.(Citation: Internet crime report 2022) In the case of business email compromise or email fraud, an adversary may utilize [Impersonation](https://attack.mitre.org/techniques/T1656) of a trusted entity. Once the social engineering is successful, victims can be deceived into sending money to financial accounts controlled by an adversary.(Citation: FBI-BEC) This creates the potential for multiple victims (i.e., compromised accounts as well as the ultimate monetary loss) in incidents involving financial theft.(Citation: VEC)

Extortion by ransomware may occur, for example, when an adversary demands payment from a victim after [Data Encrypted for Impact](https://attack.mitre.org/techniques/T1486) (Citation: NYT-Colonial) and [Exfiltration](https://attack.mitre.org/tactics/TA0010) of data, followed by threatening to leak sensitive data to the public unless payment is made to the adversary.(Citation: Mandiant-leaks) Adversaries may use dedicated leak sites to distribute victim data.(Citation: Crowdstrike-leaks)

Due to the potentially immense business impact of financial theft, an adversary may abuse the possibility of financial theft and seeking monetary gain to divert attention from their true goals such as [Data Destruction](https://attack.mitre.org/techniques/T1485) and business disruption.(Citation: AP-NotPetya)

## Threat-Mapped Scoring

Score: 3.15

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: impact

## Malware

* DarkGate

## APTs (Intrusion Sets)

* Akira
* Cinnamon Tempest
* FIN13
* INC Ransom
* Kimsuky
* Malteiro
* Play
* Scattered Spider
* SilverTerrier