# TTP Detail – T1486

## TTP Information

Name: Data Encrypted for Impact

Description: Adversaries may encrypt data on target systems or on large numbers of systems in a network to interrupt availability to system and network resources. They can attempt to render stored data inaccessible by encrypting files or data on local and remote drives and withholding access to a decryption key. This may be done in order to extract monetary compensation from a victim in exchange for decryption or a decryption key (ransomware) or to render data permanently inaccessible in cases where the key is not saved or transmitted.(Citation: US-CERT Ransomware 2016)(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017)(Citation: US-CERT SamSam 2018)

In the case of ransomware, it is typical that common user files like Office documents, PDFs, images, videos, audio, text, and source code files will be encrypted (and often renamed and/or tagged with specific file markers). Adversaries may need to first employ other behaviors, such as [File and Directory Permissions Modification](https://attack.mitre.org/techniques/T1222) or [System Shutdown/Reboot](https://attack.mitre.org/techniques/T1529), in order to unlock and/or gain access to manipulate these files.(Citation: CarbonBlack Conti July 2020) In some cases, adversaries may encrypt critical system files, disk partitions, and the MBR.(Citation: US-CERT NotPetya 2017) Adversaries may also encrypt virtual machines hosted on ESXi or other hypervisors.(Citation: Crowdstrike Hypervisor Jackpotting Pt 2 2021)

To maximize impact on the target organization, malware designed for encrypting data may have worm-like features to propagate across a network by leveraging other attack techniques like [Valid Accounts](https://attack.mitre.org/techniques/T1078), [OS Credential Dumping](https://attack.mitre.org/techniques/T1003), and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002).(Citation: FireEye WannaCry 2017)(Citation: US-CERT NotPetya 2017) Encryption malware may also leverage [Internal Defacement](https://attack.mitre.org/techniques/T1491/001), such as changing victim wallpapers or ESXi server login messages, or otherwise intimidate victims by sending ransom notes or other messages to connected printers (known as "print bombing").(Citation: NHS Digital Egregor Nov 2020)(Citation: Varonis)

In cloud environments, storage objects within compromised accounts may also be encrypted.(Citation: Rhino S3 Ransomware Part 1) For example, in AWS environments, adversaries may leverage services such as AWS’s Server-Side Encryption with Customer Provided Keys (SSE-C) to encrypt data.(Citation: Halcyon AWS Ransomware 2025)

## Threat-Mapped Scoring

Score: 2.15

Priority: P3 - Important (Medium)

## Kill Chain Phases

**•** mitre-attack: impact

## Malware

* Akira
* Akira \_v2
* Apostle
* Avaddon
* AvosLocker
* Babuk
* Bad Rabbit
* BitPaymer
* Black Basta
* BlackByte 2.0 Ransomware
* BlackByte Ransomware
* BlackCat
* Cheerscrypt
* Clop
* Conti
* Cuba
* DCSrv
* DEATHRANSOM
* DarkGate
* Diavol
* EKANS
* Egregor
* FIVEHANDS
* HELLOKITTY
* INC Ransomware
* JCry
* KillDisk
* LockBit 2.0
* LockBit 3.0
* LockerGoga
* Maze
* MegaCortex
* Megazord
* Moneybird
* Netwalker
* NotPetya
* Pay2Key
* Playcrypt
* Prestige
* ProLock
* Pysa
* REvil
* ROADSWEEP
* Ragnar Locker
* RansomHub
* RobbinHood
* Royal
* Ryuk
* SamSam
* Seth-Locker
* Shamoon
* ShrinkLocker
* SynAck
* ThiefQuest
* WannaCry
* WastedLocker
* XCSSET
* Xbash

## APTs (Intrusion Sets)

* APT38
* APT41
* Akira
* BlackByte
* FIN7
* FIN8
* INC Ransom
* Indrik Spider
* Magic Hound
* Moonstone Sleet
* Sandworm Team
* Scattered Spider
* Storm-1811
* TA505