# TTP Detail – T1027.002

## TTP Information

Name: Software Packing

Description: Adversaries may perform software packing or virtual machine software protection to conceal their code. Software packing is a method of compressing or encrypting an executable. Packing an executable changes the file signature in an attempt to avoid signature-based detection. Most decompression techniques decompress the executable code in memory. Virtual machine software protection translates an executable's original code into a special format that only a special virtual machine can run. A virtual machine is then called to run this code.(Citation: ESET FinFisher Jan 2018)

Utilities used to perform software packing are called packers. Example packers are MPRESS and UPX. A more comprehensive list of known packers is available, but adversaries may create their own packing techniques that do not leave the same artifacts as well-known packers to evade defenses.(Citation: Awesome Executable Packing)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Anchor
* AppleSeed
* Astaroth
* BLINDINGCAN
* Babuk
* Bazar
* Bisonal
* COATHANGER
* China Chopper
* Clop
* CostaBricks
* Cuba
* DRATzarus
* DarkComet
* Daserf
* Dok
* Dyre
* Egregor
* Emotet
* FYAnti
* FatDuke
* FinFisher
* GoldMax
* GreyEnergy
* H1N1
* Hildegard
* HotCroissant
* HyperBro
* IcedID
* KONNI
* Latrodectus
* LiteDuke
* LockBit 3.0
* Lokibot
* Lucifer
* Machete
* Melcoz
* Metamorfo
* Misdat
* Mongall
* NETWIRE
* OSX\_OCEANLOTUS.D
* OopsIE
* QakBot
* Raindrop
* Raspberry Robin
* S-Type
* SDBbot
* Sagerunex
* Saint Bot
* SeaDuke
* ShimRat
* Spark
* Squirrelwaffle
* StrelaStealer
* SysUpdate
* Tomiris
* Torisma
* TrickBot
* Trojan.Karagany
* Troll Stealer
* Uroburos
* VERMIN
* Valak
* XLoader
* Zebrocy
* ZeroT
* jRAT
* yty

## Tools

* CSPY Downloader
* Donut

## APTs (Intrusion Sets)

* APT29
* APT3
* APT38
* APT39
* APT41
* Aoqin Dragon
* Dark Caracal
* Elderwood
* GALLIUM
* Kimsuky
* MoustachedBouncer
* Patchwork
* Rocke
* Saint Bear
* TA2541
* TA505
* TeamTNT
* The White Company
* Threat Group-3390
* Volt Typhoon
* ZIRCONIUM