# TTP Detail – T1027.001

## TTP Information

Name: Binary Padding

Description: Adversaries may use binary padding to add junk data and change the on-disk representation of malware. This can be done without affecting the functionality or behavior of a binary, but can increase the size of the binary beyond what some security tools are capable of handling due to file size limitations.

Binary padding effectively changes the checksum of the file and can also be used to avoid hash-based blocklists and static anti-virus signatures.(Citation: ESET OceanLotus) The padding used is commonly generated by a function to create junk data and then appended to the end or applied to sections of malware.(Citation: Securelist Malware Tricks April 2017) Increasing the file size may decrease the effectiveness of certain tools and detection capabilities that are not designed or configured to scan large files. This may also reduce the likelihood of being collected for analysis. Public file scanning services, such as VirusTotal, limits the maximum size of an uploaded file to be analyzed.(Citation: VirusTotal FAQ)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Bisonal
* Black Basta
* CHIMNEYSWEEP
* Comnie
* CostaBricks
* Emissary
* Emotet
* Goopy
* Grandoreiro
* GrimAgent
* Javali
* Kwampirs
* Latrodectus
* LightSpy
* QakBot
* Rifdoor
* Snip3
* TAINTEDSCRIBE

## APTs (Intrusion Sets)

* APT29
* Akira
* BRONZE BUTLER
* Higaisa
* Leviathan
* Moafee
* Patchwork