# TTP Detail – T1027.016

## TTP Information

Name: Junk Code Insertion

Description: Adversaries may use junk code / dead code to obfuscate a malware’s functionality. Junk code is code that either does not execute, or if it does execute, does not change the functionality of the code. Junk code makes analysis more difficult and time-consuming, as the analyst steps through non-functional code instead of analyzing the main code. It also may hinder detections that rely on static code analysis due to the use of benign functionality, especially when combined with [Compression](https://attack.mitre.org/techniques/T1027/015) or [Software Packing](https://attack.mitre.org/techniques/T1027/002).(Citation: ReasonLabs)(Citation: ReasonLabs Cyberpedia Junk Code)

No-Operation (NOP) instructions are an example of dead code commonly used in x86 assembly language. They are commonly used as the 0x90 opcode. When NOPs are added to malware, the disassembler may show the NOP instructions, leading to the analyst needing to step through them.(Citation: ReasonLabs)

The use of junk / dead code insertion is distinct from [Binary Padding](https://attack.mitre.org/techniques/T1027/001) because the purpose is to obfuscate the functionality of the code, rather than simply to change the malware’s signature.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* CORESHELL
* FatDuke
* FinFisher
* Gelsemium
* Goopy
* Maze
* POWERSTATS
* Pony
* SamSam
* StrelaStealer
* WastedLocker
* XTunnel
* ZeroT
* yty

## APTs (Intrusion Sets)

* APT32
* FIN7
* Gamaredon Group
* Mustang Panda