# TTP Detail – T1027.014

## TTP Information

Name: Polymorphic Code

Description: Adversaries may utilize polymorphic code (also known as metamorphic or mutating code) to evade detection. Polymorphic code is a type of software capable of changing its runtime footprint during code execution.(Citation: polymorphic-blackberry) With each execution of the software, the code is mutated into a different version of itself that achieves the same purpose or objective as the original. This functionality enables the malware to evade traditional signature-based defenses, such as antivirus and antimalware tools.(Citation: polymorphic-sentinelone)
Other obfuscation techniques can be used in conjunction with polymorphic code to accomplish the intended effects, including using mutation engines to conduct actions such as [Software Packing](https://attack.mitre.org/techniques/T1027/002), [Command Obfuscation](https://attack.mitre.org/techniques/T1027/010), or [Encrypted/Encoded File](https://attack.mitre.org/techniques/T1027/013).(Citation: polymorphic-linkedin)(Citation: polymorphic-medium)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* BendyBear