# TTP Detail – T1066

## TTP Information

Name: Indicator Removal from Tools

Description: If a malicious tool is detected and quarantined or otherwise curtailed, an adversary may be able to determine why the malicious tool was detected (the indicator), modify the tool by removing the indicator, and use the updated version that is no longer detected by the target's defensive systems or subsequent targets that may use similar systems.

A good example of this is when malware is detected with a file signature and quarantined by anti-virus software. An adversary who can determine that the malware was quarantined because of its file signature may use [Software Packing](https://attack.mitre.org/techniques/T1045) or otherwise modify the file so it has a different signature, and then re-use the malware.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion