# TTP Detail – T1027.005

## TTP Information

Name: Indicator Removal from Tools

Description: Adversaries may remove indicators from tools if they believe their malicious tool was detected, quarantined, or otherwise curtailed. They can modify the tool by removing the indicator and using 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 modify the file to explicitly avoid that signature, and then re-use the malware.

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Cobalt Strike
* Daserf
* GravityRAT
* InvisiMole
* Penquin
* QakBot
* SUNBURST
* Waterbear

## Tools

* PowerSploit

## APTs (Intrusion Sets)

* APT3
* Deep Panda
* GALLIUM
* OilRig
* Patchwork
* Turla