# TTP Detail – T1070.009

## TTP Information

Name: Clear Persistence

Description: Adversaries may clear artifacts associated with previously established persistence on a host system to remove evidence of their activity. This may involve various actions, such as removing services, deleting executables, [Modify Registry](https://attack.mitre.org/techniques/T1112), [Plist File Modification](https://attack.mitre.org/techniques/T1647), or other methods of cleanup to prevent defenders from collecting evidence of their persistent presence.(Citation: Cylance Dust Storm) Adversaries may also delete accounts previously created to maintain persistence (i.e. [Create Account](https://attack.mitre.org/techniques/T1136)).(Citation: Talos - Cisco Attack 2022)

In some instances, artifacts of persistence may also be removed once an adversary’s persistence is executed in order to prevent errors with the new instance of the malware.(Citation: NCC Group Team9 June 2020)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: defense-evasion

## Malware

* Bazar
* GrimAgent
* IPsec Helper
* KOCTOPUS
* Kapeka
* Misdat
* Pillowmint
* RTM
* Raspberry Robin
* S-Type
* SUNBURST
* njRAT

## Tools

* MCMD