# TTP Detail – T1556.006

## TTP Information

Name: Multi-Factor Authentication

Description: Adversaries may disable or modify multi-factor authentication (MFA) mechanisms to enable persistent access to compromised accounts.

Once adversaries have gained access to a network by either compromising an account lacking MFA or by employing an MFA bypass method such as [Multi-Factor Authentication Request Generation](https://attack.mitre.org/techniques/T1621), adversaries may leverage their access to modify or completely disable MFA defenses. This can be accomplished by abusing legitimate features, such as excluding users from Azure AD Conditional Access Policies, registering a new yet vulnerable/adversary-controlled MFA method, or by manually patching MFA programs and configuration files to bypass expected functionality.(Citation: Mandiant APT42)(Citation: Azure AD Conditional Access Exclusions)

For example, modifying the Windows hosts file (`C:\windows\system32\drivers\etc\hosts`) to redirect MFA calls to localhost instead of an MFA server may cause the MFA process to fail. If a "fail open" policy is in place, any otherwise successful authentication attempt may be granted access without enforcing MFA. (Citation: Russians Exploit Default MFA Protocol - CISA March 2022)

Depending on the scope, goals, and privileges of the adversary, MFA defenses may be disabled for individual accounts or for all accounts tied to a larger group, such as all domain accounts in a victim's network environment.(Citation: Russians Exploit Default MFA Protocol - CISA March 2022)

## Threat-Mapped Scoring

Score: 0.0

Priority: Unclassified

## Kill Chain Phases

**•** mitre-attack: credential-access

**•** mitre-attack: defense-evasion

**•** mitre-attack: persistence

## Malware

* SLOWPULSE

## Tools

* AADInternals

## APTs (Intrusion Sets)

* Scattered Spider