# TTP Detail – T1556.001

## TTP Information

Name: Domain Controller Authentication

Description: Adversaries may patch the authentication process on a domain controller to bypass the typical authentication mechanisms and enable access to accounts.

Malware may be used to inject false credentials into the authentication process on a domain controller with the intent of creating a backdoor used to access any user’s account and/or credentials (ex: [Skeleton Key](https://attack.mitre.org/software/S0007)). Skeleton key works through a patch on an enterprise domain controller authentication process (LSASS) with credentials that adversaries may use to bypass the standard authentication system. Once patched, an adversary can use the injected password to successfully authenticate as any domain user account (until the the skeleton key is erased from memory by a reboot of the domain controller). Authenticated access may enable unfettered access to hosts and/or resources within single-factor authentication environments.(Citation: Dell Skeleton)

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

**•** mitre-attack: defense-evasion

**•** mitre-attack: persistence

## Malware

* Skeleton Key

## APTs (Intrusion Sets)

* Chimera