# TTP Detail – T1556.003

## TTP Information

Name: Pluggable Authentication Modules

Description: Adversaries may modify pluggable authentication modules (PAM) to access user credentials or enable otherwise unwarranted access to accounts. PAM is a modular system of configuration files, libraries, and executable files which guide authentication for many services. The most common authentication module is <code>pam\_unix.so</code>, which retrieves, sets, and verifies account authentication information in <code>/etc/passwd</code> and <code>/etc/shadow</code>.(Citation: Apple PAM)(Citation: Man Pam\_Unix)(Citation: Red Hat PAM)

Adversaries may modify components of the PAM system to create backdoors. PAM components, such as <code>pam\_unix.so</code>, can be patched to accept arbitrary adversary supplied values as legitimate credentials.(Citation: PAM Backdoor)

Malicious modifications to the PAM system may also be abused to steal credentials. Adversaries may infect PAM resources with code to harvest user credentials, since the values exchanged with PAM components may be plain-text since PAM does not store passwords.(Citation: PAM Creds)(Citation: Apple PAM)

## Threat-Mapped Scoring

Score: 1.8

Priority: P4 - Informational (Low)

## Kill Chain Phases

**•** mitre-attack: credential-access

**•** mitre-attack: defense-evasion

**•** mitre-attack: persistence

## Malware

* Ebury
* Skidmap