# TTP Detail – T1167

## TTP Information

Name: Securityd Memory

Description: In OS X prior to El Capitan, users with root access can read plaintext keychain passwords of logged-in users because Apple’s keychain implementation allows these credentials to be cached so that users are not repeatedly prompted for passwords. (Citation: OS X Keychain) (Citation: External to DA, the OS X Way) Apple’s securityd utility takes the user’s logon password, encrypts it with PBKDF2, and stores this master key in memory. Apple also uses a set of keys and algorithms to encrypt the user’s password, but once the master key is found, an attacker need only iterate over the other values to unlock the final password. (Citation: OS X Keychain)

If an adversary can obtain root access (allowing them to read securityd’s memory), then they can scan through memory to find the correct sequence of keys in relatively few tries to decrypt the user’s logon keychain. This provides the adversary with all the plaintext passwords for users, WiFi, mail, browsers, certificates, secure notes, etc. (Citation: OS X Keychain) (Citation: OSX Keydnap malware)

## Threat-Mapped Scoring

Score: 3.25

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access