# TTP Detail – T1555.005

## TTP Information

Name: Password Managers

Description: Adversaries may acquire user credentials from third-party password managers.(Citation: ise Password Manager February 2019) Password managers are applications designed to store user credentials, normally in an encrypted database. Credentials are typically accessible after a user provides a master password that unlocks the database. After the database is unlocked, these credentials may be copied to memory. These databases can be stored as files on disk.(Citation: ise Password Manager February 2019)  
  
Adversaries may acquire user credentials from password managers by extracting the master password and/or plain-text credentials from memory.(Citation: FoxIT Wocao December 2019)(Citation: Github KeeThief) Adversaries may extract credentials from memory via [Exploitation for Credential Access](https://attack.mitre.org/techniques/T1212).(Citation: NVD CVE-2019-3610)  
 Adversaries may also try brute forcing via [Password Guessing](https://attack.mitre.org/techniques/T1110/001) to obtain the master password of a password manager.(Citation: Cyberreason Anchor December 2019)

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Malware

* MarkiRAT
* Proton
* TrickBot

## APTs (Intrusion Sets)

* Fox Kitten
* Indrik Spider
* LAPSUS$
* Threat Group-3390