# TTP Detail – T1003.005

## TTP Information

Name: Cached Domain Credentials

Description: Adversaries may attempt to access cached domain credentials used to allow authentication to occur in the event a domain controller is unavailable.(Citation: Microsoft - Cached Creds)

On Windows Vista and newer, the hash format is DCC2 (Domain Cached Credentials version 2) hash, also known as MS-Cache v2 hash.(Citation: PassLib mscache) The number of default cached credentials varies and can be altered per system. This hash does not allow pass-the-hash style attacks, and instead requires [Password Cracking](https://attack.mitre.org/techniques/T1110/002) to recover the plaintext password.(Citation: ired mscache)

On Linux systems, Active Directory credentials can be accessed through caches maintained by software like System Security Services Daemon (SSSD) or Quest Authentication Services (formerly VAS). Cached credential hashes are typically located at `/var/lib/sss/db/cache.[domain].ldb` for SSSD or `/var/opt/quest/vas/authcache/vas\_auth.vdb` for Quest. Adversaries can use utilities, such as `tdbdump`, on these database files to dump the cached hashes and use [Password Cracking](https://attack.mitre.org/techniques/T1110/002) to obtain the plaintext password.(Citation: Brining MimiKatz to Unix)

With SYSTEM or sudo access, the tools/utilities such as [Mimikatz](https://attack.mitre.org/software/S0002), [Reg](https://attack.mitre.org/software/S0075), and secretsdump.py for Windows or Linikatz for Linux can be used to extract the cached credentials.(Citation: Brining MimiKatz to Unix)

Note: Cached credentials for Windows Vista are derived using PBKDF2.(Citation: PassLib mscache)

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Malware

* Okrum

## Tools

* Cachedump
* LaZagne
* Pupy

## APTs (Intrusion Sets)

* APT33
* Leafminer
* MuddyWater
* OilRig