T1003.005 - OS Credential Dumping: Cached Domain Credentials

Description from ATT&CK

> 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 to recover the plaintext password.(Citation: ired

> With SYSTEM access, the tools/utilities such as Mimikatz, Reg, and secretsdump.py can be used to extract the cached credentials.
>
> Note: Cached credentials for Windows Vista are derived using PBKDF2.(Citation: PassLib mscache)

Atomic Tests

Atomic Test #1 - Cached Credential Dump via Cmdkey

List credentials currently stored on the host via the built-in Windows utility cmdkey.exe Credentials listed with Cmdkey only pertain to the current user Passwords will not be displayed once they are stored https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/cmdkey https://www.peew.pw/blog/2017/11/26/exploring-cmdkey-an-edge-case-for-privilege-escalation

Supported Platforms: Windows

auto_generated_guid: 56506854-89d6-46a3-9804-b7fde90791f9

Attack Commands: Run with `command_prompt`!

```
cmdkey /list
```