credhist

`dpapi::credhist` describes a Credhist file. Passcape mentions that `CREDHIST` is a password history file, made out as a chain, where each link represents the user's older password hashes (NT and SHA1). Each time user changes the password, the old password hash is appended to the file and encrypted with a new password. It has the following command line arguments:

- `/in` : the path of the CREDHIST. According to this guide, it can be found at `C:\users<UserName>\appdata\Roaming\Microsoft\Protect\CREDHIST`
- `/sid` : the Security Identifier of the target user
- `/sha1` : the SHA1 hash of the target user password. It can be obtained through `sekurlsa::logonpasswords`.
- `/password` : the password of the target user

```
mimikatz# dpapi::credhist in:"C:\users<UserName>\appdata\Roaming\Microsoft\Protect\
```

During our test on a Windows 10 20H2 box, we could not find the `CREDHIST` file.

Previous
cred

Next
luna

Last updated 2 years ago