# TTP Detail – T1555.004

## TTP Information

Name: Windows Credential Manager

Description: 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](https://attack.mitre.org/techniques/T1555/003), 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 <code>Policy.vpol</code>, 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. <code>vaultcmd.exe</code> is a native Windows executable that can be used to enumerate credentials stored in the Credential Locker through a command-line interface. Adversaries may also gather credentials by directly reading files located inside of the Credential Lockers. Windows APIs, such as <code>CredEnumerateA</code>, may also be absued to list credentials managed by the Credential Manager.(Citation: Microsoft CredEnumerate)(Citation: Delpy Mimikatz Crendential Manager)  
  
Adversaries may also obtain credentials from credential backups. Credential backups and restorations may be performed by running <code>rundll32.exe keymgr.dll KRShowKeyMgr</code> then selecting the “Back up...” button on the “Stored User Names and Passwords” GUI.  
  
Password recovery tools may also obtain plain text passwords from the Credential Manager.(Citation: Malwarebytes The Windows Vault)

## Threat-Mapped Scoring

Score: 3.0

Priority: P2 - Serious (High)

## Kill Chain Phases

**•** mitre-attack: credential-access

## Malware

* KGH\_SPY
* Lizar
* ROKRAT
* RainyDay
* Valak

## Tools

* LaZagne
* Mimikatz
* PowerSploit
* SILENTTRINITY

## APTs (Intrusion Sets)

* OilRig
* Stealth Falcon
* Turla
* Wizard Spider