

T1556.002 - Password Filter DLL

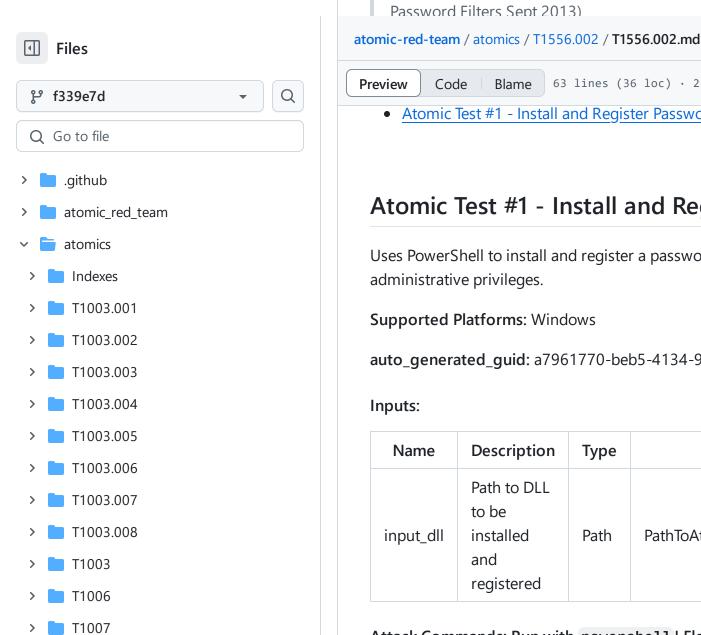
Description from ATT&CK

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)

↑ Top

Raw 📮 🕹



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.

63 lines (36 loc) · 2.76 KB

Supported Platforms: Windows

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

Atomic Test #1 - Install and Register Password Filter DLL

Inputs:

Preview

Name	Description	Туре	Default Value
input_dll	Path to DLL to be installed and registered	Path	PathToAtomicsFolder\T1556.002\src\AtomicPasswor

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

```
> T1010
  T1012
  T1014
  T1016
  T1018
  T1020
 T1021.001
 T1021.002
> T1021.003
> T1021.006
 T1027.001
 T1027.002
 T1027.004
 T1027
 T1030
 T1033
 T1036.003
 T1036.004
> T1036.005
 T1036.006
 T1036
> T1037.001
> T1037.002
> T1037.004
```

> T1037.005

> T1039

> T1040

```
$passwordFilterName = (Copy-Item "#{input_dll}" -Destination "C:\Windows {\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text{\text
```