

Product

▼

Solutions

▼

Resources

▼

Open Source

▼

Enterprise

▼

Pricing

Q

Sign in

Sign up

📄

redcanaryco / atomic-red-team

Public

🔔

Notifications

🍴

Fork

2.8k

★

Star

9.7k

<>

Code

🕒

Issues

6

🔗

Pull requests

5

🔄

Actions

📖

Wiki

🛡️

Security

📊

Insights

📁

Files

🔗

40b77d6

▼

🔍

🔍

Go to file

>

📁

.github

>

📁

atomic_red_team

▼

📁

atomics

>

📁

Indexes

>

📁

T1003.001

>

📁

T1003.002

>

📁

T1003.003

>

📁

T1003.004

>

📁

T1003.005

>

📁

T1003.006

>

📁

T1003.007

>

📁

T1003.008

>

📁

T1003

>

📁

T1006

>

📁

T1007

>

📁

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

atomic-red-team / atomics / T1564.002 / T1564.002.md

📄

...

🌐

Atomic Red Team doc generat...

Generated docs from job=generate-d...

659e4e2 · 2 years ago

🕒 History

Preview

Code

Blame

134 lines (68 loc) · 5.11 KB

Raw

📄

📥

☰

T1564.002 - Hidden Users

Description from ATT&CK

Adversaries may use hidden users to hide the presence of user accounts they create or modify. Administrators may want to hide users when there are many user accounts on a given system or if they want to hide their administrative or other management accounts from other users.

In macOS, adversaries can create or modify a user to be hidden through manipulating plist files, folder attributes, and user attributes. To prevent a user from being shown on the login screen and in System Preferences, adversaries can set the userID to be under 500 and set the key value `Hide500Users` to `TRUE` in the `/Library/Preferences/com.apple.loginwindow` plist file.(Citation: Cybereason OSX Pirrit) Every user has a userID associated with it. When the `Hide500Users` key value is set to `TRUE`, users with a userID under 500 do not appear on the login screen and in System Preferences. Using the command line, adversaries can use the `dsc1` utility to create hidden user accounts by setting the `IsHidden` attribute to `1`. Adversaries can also hide a user’s home folder by changing the `chflags` to hidden.(Citation: Apple Support Hide a User Account)

Adversaries may similarly hide user accounts in Windows. Adversaries can set the `HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList` Registry key value to `0` for a specific user to prevent that user from being listed on the logon screen.(Citation: FireEye SMOKEDHAM June 2021)(Citation: US-CERT TA18-074A)

On Linux systems, adversaries may hide user accounts from the login screen, also referred to as the greeter. The method an adversary may use depends on which Display Manager the distribution is currently using. For example, on an Ubuntu system using the GNOME Display Manger (GDM), accounts may be hidden from the greeter using the `gsettings` command (ex: `sudo -u gdm gsettings set org.gnome.login-screen disable-user-list true`).(Citation: Hide GDM User Accounts) Display Managers are not anchored to specific distributions and may be changed by a user or adversary.

Atomic Tests

- [Atomic Test #1 - Create Hidden User using UniqueID < 500](#)
- [Atomic Test #2 - Create Hidden User using IsHidden option](#)
- [Atomic Test #3 - Create Hidden User in Registry](#)

Page 1 of 3

- >  T1037.001
- >  T1037.002
- >  T1037.004
- >  T1037.005
- >  T1039
- >  T1040

Atomic Test #1 - Create Hidden User using UniqueID < 500


Add a hidden user on macOS using Unique ID < 500 (users with that ID are hidden by default)

Supported Platforms: macOS

auto_generated_guid: 4238a7f0-a980-4fff-98a2-dfc0a363d507

Inputs:

Name	Description	Type	Default Value
user_name	username to add	String	APT

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

```
sudo dscl . -create /Users/#{user_name} UniqueID 333
```

Cleanup Commands:

```
sudo dscl . -delete /Users/#{user_name}
```

Atomic Test #2 - Create Hidden User using IsHidden option

Add a hidden user on macOS using IsHidden optoin

Supported Platforms: macOS

auto_generated_guid: de87ed7b-52c3-43fd-9554-730f695e7f31

Inputs:

Name	Description	Type	Default Value
user_name	username to add	String	APT

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

```
sudo dscl . -create /Users/#{user_name} IsHidden 1
```

Cleanup Commands:

```
sudo dscl . -delete /Users/#{user_name}
```

Atomic Test #3 - Create Hidden User in Registry

Adversaries may similarly hide user accounts in Windows. Adversaries can set the HKLM\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\SpecialAccounts\UserList Registry key value to 0 for a specific user to prevent that user from being listed on the logon screen. Reference

<https://attack.mitre.org/techniques/T1564/002/> and <https://thedfirreport.com/2022/07/11/select-xmrig-from-sqlserver/>

Supported Platforms: Windows

auto_generated_guid: 173126b7-afe4-45eb-8680-fa9f6400431c

Inputs:

Name	Description	Type	Default Value
user_password	Password for new user account	String	At0micRedTeam!
user_name	Username	String	AtomicOperator

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

```
NET USER #{user_name}$ #{user_password} /ADD /expires:never
REG ADD "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\Spec
```

Cleanup Commands:

```
reg delete "HKLM\Software\Microsoft\Windows NT\CurrentVersion\Winlogon\S
net user ${user_name}$ /delete >nul 2>&1
```