

Product

▼

Solutions

▼

Resources

▼

Open Source

▼

Enterprise

▼

Pricing

Q

Search

Sign in

Sign up

redcanaryco

/

atomic-red-team

Public

Notifications

Fork2.8k

Star9.7k

<>Code

Issues6

Pull requests5

Actions

Wiki

Security

Insights

atomic-red-team / atomics / T1531 / T1531.md

Atomic Red Team doc generat...

Generated docs from job=generate-d...819934c · 2 years ago

History

T1531 - Account Access Removal

Description from ATT&CK

Adversaries may interrupt availability of system and network resources by inhibiting access to accounts utilized by legitimate users. Accounts may be deleted, locked, or manipulated (ex: changed credentials) to remove access to accounts. Adversaries may also subsequently log off and/or perform a [System Shutdown/Reboot] (<https://attack.mitre.org/techniques/T1529>) to set malicious changes into place. (Citation: CarbonBlack LockerGoga 2019)(Citation: Unit42 LockerGoga 2019) In Windows, [Net](#) utility, `Set-LocalUser` and `Set-ADAccountPassword` [PowerShell](#) cmdlets may be used by adversaries to modify user accounts. In Linux, the `passwd` utility may be used to change passwords. Accounts could also be disabled by Group Policy.

Adversaries who use ransomware may first perform this and other Impact behaviors, such as [Data Destruction](#) and [Defacement](#), before completing the [Data Encrypted for Impact](#) objective.

Atomic Tests

[Atomic Test #1 - Change User Password - Windows](#)

[Atomic Test #2 - Delete User - Windows](#)

[Atomic Test #3 - Remove Account From Domain Admin Group](#)

Atomic Test #1 - Change User Password - Windows

Changes the user password to hinder access attempts. Seen in use by LockerGoga. Upon execution, log into the user account "AtomicAdministrator" with the password "HuHuHUHoHo283283".

Supported Platforms: Windows

auto_generated_guid: 1b99ef28-f83c-4ec5-8a08-1a56263a5bb2

Inputs:

Name	Description	Type	Default Value
user_account	User account whose password will be changed.	String	AtomicAdministrator

Page 1 of 3

Files

f339e7d

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

new_user_password	Password to use if user account must be created first	String	User2ChangePW!
new_password	New password for the specified account.	String	HuHuHUHoHo283283@dJD

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

```
net user #{user_account} #{new_user_password} /add
net.exe user #{user_account} #{new_password}
```

Cleanup Commands:

```
net.exe user #{user_account} /delete >nul 2>&1
```

Atomic Test #2 - Delete User - Windows

Deletes a user account to prevent access. Upon execution, run the command "net user" to verify that the new "AtomicUser" account was deleted.

Supported Platforms: Windows

auto_generated_guid: f21a1d7d-a62f-442a-8c3a-2440d43b19e5

Inputs:

atomic-red-team / atomics / T1531 / T1531.md↑ Top

PreviewCodeBlame

146 lines (79 loc) · 4.87 KB

RawCopyDownloadMenu

new_user_password	must be created first	String	User2DeletePW!
user_account	User account to be deleted.	String	AtomicUser

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

```
net user #{user_account} #{new_user_password} /add
net.exe user #{user_account} /delete
```

Atomic Test #3 - Remove Account From Domain Admin Group























This test will remove an account from the domain admins group

Supported Platforms: Windows

auto_generated_guid: 43f71395-6c37-498e-ab17-897d814a0947

Inputs:

Name	Description	Type	Default Value
super_user	Account used to run the execution command (must include domain).	String	domain\super_user
super_pass	super_user account password.	String	password

- ▶  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

remove_user	Account to remove from domain admins.	String	remove_user
-------------	---------------------------------------	--------	-------------

Attack Commands: Run with powershell!

```
$PWord = ConvertTo-SecureString -String #{super_pass} -AsPlainText -Force
$Credential = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList $PWord, $Credential
if((Get-ADUser #{remove_user} -Properties memberof).memberof -like "CN=Domain Admins,DC=corp,DC=contoso,DC=com") {
    Remove-ADGroupMember -Identity "Domain Admins" -Members #{remove_user}
} else {
    write-host "Error - Make sure #{remove_user} is in the domain admins"
}
```

Dependencies: Run with `powershell`!

Description: Requires the Active Directory module for powershell to be installed.

Check Prereq Commands:

```
if(Get-Module -ListAvailable -Name ActiveDirectory) {exit 0} else {exit 1}
```

Get Prereq Commands:

```
Add-WindowsCapability -Online -Name "Rsat.ActiveDirectory.DS-LDS.Tools~
```