

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 <a href="https://attack.m

Adversaries who use ransomware may first perform this and other Impact behaviors, such as <u>Data Destruction</u> and <u>Defacement</u>, before completing the <u>Data Encrypted for Impact</u> 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

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

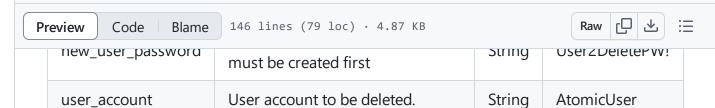
Deletes a user account to prevent access. Upon execution, run the command "net user" to verify that the new "AtomicUser" account was deleted.

Supported Platforms: Windows

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

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





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



↑ Top

Atomic Test #3 - Remove Account From Domain Admin Group

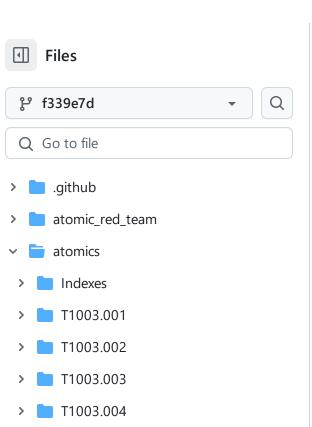
This test will remove an account from the domain admins group

Supported Platforms: Windows

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

Inputs:

Name	Description	Туре	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



T1003.005

T1003.006

T1003.007

T1003.008

T1003

T1006

T1007

T1010

T1012

T1014

T1016

> T1018

Get Prereq Commands:



T1040

```
Account to remove from domain
                                                      String
 remove_user
                                                               remove_user
                admins.
Attack Commands: Run with powershell!
  $PWord = ConvertTo-SecureString -String #{super_pass} -AsPlainText -Forc □
 $Credential = New-Object -TypeName System.Management.Automation.PSCreden
 if((Get-ADUser #{remove_user} -Properties memberof).memberof -like "CN=D
    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
```

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