Sign in

redcanaryco / **atomic-red-team** Public

Notifications · Fork 2.8k · Star 9.7k

Code · Issues 6 · Pull requests 5 · Actions · Wiki · Security · Insights

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

```
72 lines (45 loc) · 3.74 KB
```

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, Kubernetes API server,

> kubelet, or web application such as the Kubernetes dashboard.(Citation: Trend Micro Exposed Docker Server)(Citation: Unit 42 Hildegard Malware)

Atomic Tests

Preview Code Blame Raw

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 download URL	Url	https://dl.google.com/tag/s/appguid%3D%7B8A69D345-D5 C7744738E422%7D%26lang%3Den%26browser%3D3%26 stable-statsdef_1%26installdataindex%3Dempty/chrome/in
extension_id	chrome extension id	String	"fcfhplploccackoneaefokcmbjfbkenj", "fdcgdnkidjaadafnichf

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 -F
  New-ItemProperty -Path "HKLM:\Software\Wow6432Node\Google\Chrome\Extensions\$ext
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"
```

Dependencies: Run with `powershell`!

Description: Chrome must be installed

Check Prereq Commands:

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

Get Prereq Commands:

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