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 / T1070.005 / T1070.005.md

193 lines (92 loc) · 4.83 KB

Preview Code Blame Raw

T1070.005 - Network Share Connection Removal

Description from ATT&CK

> Adversaries may remove share connections that are no longer useful in order to clean up traces of their operation. Windows shared drive and [SMB/Windows Admin Shares](https://attack.mitre.org/techniques/T1021/002) connections can be removed when no longer needed. [Net](https://attack.mitre.org/software/S0039) is an example utility that can be used to remove network share connections with the `net use \\system\share /delete` command. (Citation: Technet Net Use)

Atomic Tests

- Atomic Test #1 - Add Network Share
- Atomic Test #2 - Remove Network Share
- Atomic Test #3 - Remove Network Share PowerShell
- Atomic Test #4 - Disable Administrative Share Creation at Startup

- Atomic Test #5 - Remove Administrative Shares

Atomic Test #1 - Add Network Share

Add a Network Share utilizing the command_prompt

Supported Platforms: Windows

auto_generated_guid: 14c38f32-6509-46d8-ab43-d53e32d2b131

Inputs:

Name	Description	Type	Default Value
share_name	Share to add.	String	\\test\share

Attack Commands: Run with `command_prompt`!

```
net use c: #{share_name}
net share test=#{share_name} /REMARK:"test share" /CACHE:No
```

Atomic Test #2 - Remove Network Share

Removes a Network Share utilizing the command_prompt

Supported Platforms: Windows

auto_generated_guid: 09210ad5-1ef2-4077-9ad3-7351e13e9222

Inputs:

Name	Description	Type	Default Value
share_name	Share to remove.	String	\\test\share

Attack Commands: Run with `command_prompt`!

```
net share #{share_name} /delete
```

Atomic Test #3 - Remove Network Share PowerShell

Removes a Network Share utilizing PowerShell

Supported Platforms: Windows

auto_generated_guid: 0512d214-9512-4d22-bde7-f37e058259b3

Inputs:

Name	Description	Type	Default Value
share_name	Share to remove.	String	\\test\share

Attack Commands: Run with `powershell`!

```
Remove-SmbShare -Name #{share_name}
Remove-FileShare -Name #{share_name}
```

Atomic Test #4 - Disable Administrative Share Creation at Startup

Administrative shares are hidden network shares created by Microsoft’s Windows NT operating systems that grant system administrators remote access to every disk volume on a network-connected system. These shares are automatically created at started unless they have been purposefully disabled and is done in this Atomic test. As Microsoft puts it, "Missing administrative shares typically indicate that the computer in question has been compromised by malicious software." https://threatpost.com/conti-ransomware-gang-has-full-log4shell-attack-chain/177173/

Supported Platforms: Windows

auto_generated_guid: 99c657aa-ebeb-4179-a665-69288fdd12b8

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

```
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Paramet
reg add "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Paramet
```

Cleanup Commands:

```
reg delete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Para
reg delete "HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Para
```

Atomic Test #5 - Remove Administrative Shares

Administrative shares are hidden network shares created by Microsoft's Windows NT operating systems that grant system administrators remote access to every disk volume on a network-connected system. As Microsoft puts it, "Missing administrative shares typically indicate that the computer in question has been compromised by malicious software. https://threatpost.com/conti-ransomware-gang-has-full-log4shell-attack-chain/177173/

Supported Platforms: Windows

auto_generated_guid: 4299eff5-90f1-4446-b2f3-7f4f5cfd5d62

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

```
for %i in (C$ IPC$ ADMIN$) do net share %i /delete
```

Cleanup Commands:

```
net share ADMIN$ /UNLIMITED >nul 2>&1
net share C$=C:\ >nul 2>&1
net share IPC$ >nul 2>&1
```