








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 / T1072 / T1072.md 






113 lines (64 loc) · 3.84 KB


Preview


Code

Blame

Raw







T1072 - Software Deployment Tools

Description from ATT&CK

Adversaries may gain access to and use third-party software suites installed within an enterprise network, such as administration, monitoring, and deployment systems, to move laterally through the network. Third-party applications and software deployment systems may be in use in the network environment for administration purposes (e.g., SCCM, HBSS, Altiris, etc.).

Access to a third-party network-wide or enterprise-wide software system may enable an adversary to have remote code execution on all systems that are connected to such a system. The access may be used to laterally move to other systems, gather information, or cause a specific effect, such as wiping the hard drives on all endpoints.

The permissions required for this action vary by system configuration; local credentials may be sufficient with direct access to the third-party system, or specific domain credentials may be required. However, the system may require an administrative account to log in or to perform it's intended purpose.

Atomic Tests

- [Atomic Test #1 - Radmin Viewer Utility](#)
- [Atomic Test #2 - PDQ Deploy RAT](#)

Atomic Test #1 - Radmin Viewer Utility

An adversary may use Radmin Viewer Utility to remotely control Windows device, this will start the radmin console.

Supported Platforms: Windows

auto_generated_guid: b4988cad-6ed2-434d-ace5-ea2670782129

Inputs:

Name	Description	Type	Default Value
radmin_installer	Radmin Viewer installer	Path	RadminViewer.msi
radmin_exe	The radmin.exe executable from RadminViewer.msi	Path	Radmin Viewer 3/Radmin.exe

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

```
"%PROGRAMFILES(x86)%/#{radmin_exe}"
```



Dependencies: Run with `powershell` !

Description: Radmin Viewer Utility must be installed at specified location (#{radmin_exe})

Check Prereq Commands:

```
if (Test-Path "${env:ProgramFiles(x86)}/#{radmin_exe}") {exit 0} else {exit 1}
```



Get Prereq Commands:

Write-Host Downloading radmin installer

(New-Object Net.WebClient).DownloadFile("https://www.radmin.com/download/Radmin_Vi

Write-Host Install Radmin

Start-Process msixexec -Wait -ArgumentList /i , \$ENV:Temp\#{radmin_installer}, /qn



Atomic Test #2 - PDQ Deploy RAT

An adversary may use PDQ Deploy Software to deploy the Remote Adminstartion Tool, this will start the PDQ console.

Supported Platforms: Windows

auto_generated_guid: e447b83b-a698-4feb-bed1-a7aaf45c3443

Inputs:

Name	Description	Type	Default Value
PDQ_Deploy_installer	PDQ Deploy Install	Path	PDQDeploysetup.exe
PDQ_Deploy_exe	The PDQDeployConsole.exe executable from PDQDeploysetup.exe	Path	Admin Arsenal/PDQ Deploy/PDQDeployConsole.exe

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

"%PROGRAMFILES(x86)%/#{PDQ_Deploy_exe}"



Dependencies: Run with `powershell` !

Description: PDQ Deploy will be installed at specified location (#{PDQ_Deploy_exe})

Check Prereq Commands:

```
if (Test-Path "${env:ProgramFiles(x86)}/{PDQ_Deploy_exe}") {exit 0} else {exit 1}
```

Get Prereq Commands:

```
Write-Host Downloading PDQ Deploy installer  
(New-Object Net.WebClient).DownloadFile("https://download.pdq.com/release/19/Deploy.exe")  
Write-Host Install PDQ Deploy  
Start-Process $ENV:Temp\#{PDQ_Deploy_installer} -Wait -ArgumentList "/s"
```