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

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	%TEMP%\RadminViewer.msi
radmin_exe	The radmin.exe executable from RadminViewer.msi	Path	%PROGRAMFILES(x86)%/Radmin Viewer 3/Radmin.exe

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

```
"#{radmin_exe}"
```

Dependencies: Run with `command_prompt`!

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

Check Prereq Commands:

```
if not exist "#{radmin_exe}" (exit /b 1)
```

Get Prereq Commands:

```
echo Downloading radmin installer
bitsadmin /transfer myDownloadJob /download /priority normal "https://www.radmin.c
```

```
msiexec /i "#{radmin_installer}" /qn
```