Event Triggered Execution: Installer Packages, Sub-technique T1546.016 - Enterprise

Archived: 2026-04-05 17:22:59 UTC

Adversaries may establish persistence and elevate privileges by using an installer to trigger the execution of malicious content. Installer packages are OS specific and contain the resources an operating system needs to install applications on a system. Installer packages can include scripts that run prior to installation as well as after installation is complete. Installer scripts may inherit elevated permissions when executed. Developers often use these scripts to prepare the environment for installation, check requirements, download dependencies, and remove files after installation.[1]

Using legitimate applications, adversaries have distributed applications with modified installer scripts to execute malicious content. When a user installs the application, they may be required to grant administrative permissions to allow the installation. At the end of the installation process of the legitimate application, content such as macOS `postinstall` scripts can be executed with the inherited elevated permissions. Adversaries can use these scripts to execute a malicious executable or install other malicious components (such as a Launch Daemon) with the elevated permissions.[2][3][4][5]

Depending on the distribution, Linux versions of package installer scripts are sometimes called maintainer scripts or post installation scripts. These scripts can include `preinst`, `postinst`, `prerm`, `postrm` scripts and run as root when executed.

For Windows, the Microsoft Installer services uses `.msi` files to manage the installing, updating, and uninstalling of applications. These installation routines may also include instructions to perform additional actions that may be abused by adversaries.[6]

Source: https://attack.mitre.org/techniques/T1546/016