ID: x-mitre-collection--23320f4-22ad-8467-3b73-ed0c869a12838
Description: ATT&CK for Enterprise provides a knowledge base of real-world adversary behavior targeting traditional enterprise networks. ATT&CK for Enterprise covers the following platforms: Windows, macOS, Linux, PRE, Office 365, Google Workspace, IaaS, Network, and Containers.
Created by: identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5
Date Created: 2018-01-17T12:56:55.080Z
Platforms: Not Specified
Kill chain: null
ID: course-of-action--4f170666-7edb-4489-85c2-9affa28a72e0
Description: Making these files immutable and only changeable by certain administrators will limit the ability for adversaries to easily create user level persistence.
Created by: identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5
Date Created: 2018-01-17T12:56:55.080Z
Platforms: Not Specified
Kill chain: null
ID: attack-pattern--01df3350-ce05-4bdf-bdf8-0a919a66d4a8
Description: <code>~/.bash_profile</code> and <code>~/.bashrc</code> are executed in a user's context when a new shell opens or when a user logs in so that their environment is set correctly. <code>~/.bash_profile</code> is executed for login shells and <code>~/.bashrc</code> is executed for interactive non-login shells. This means that when a user logs in (via username and password) to the console (either locally or remotely via something like SSH), <code>~/.bash_profile</code> is executed before the initial command prompt is returned to the user. After that, every time a new shell is opened, <code>~/.bashrc</code> is executed. This allows users more fine grained control over when they want certain commands executed.

Mac's Terminal.app is a little different in that it runs a login shell by default each time a new terminal window is opened, thus calling <code>~/.bash_profile</code> each time instead of <code>~/.bashrc</code>.

These files are meant to be written to by the local user to configure their own environment; however, adversaries can also insert code into these files to gain persistence each time a user logs in or opens a new shell.

Detection: While users may customize their <code>~/.bashrc</code> and <code>~/.bash_profile</code> files , there are only certain types of commands that typically appear in these files. Monitor for abnormal commands such as execution of unknown programs, opening network sockets, or reaching out across the network when user profiles are loaded during the login process.

Platforms: Linux, macOS

Data Sources: File monitoring, Process Monitoring, Process command-line parameters, Process use of network

Permissions Required: User, Administrator

Created by: identity--c78cb6e5-0c4b-4611-8297-d1b8b55e40b5

Date Created: 2017-12-14T16:46:06.044Z

Platforms: Linux, macOS

Kill chain: [mitre-attack, persistence]