Indicator Removal: Clear Command History, Sub-technique T1070.003 - Enterprise

Archived: 2026-04-05 15:48:32 UTC

In addition to clearing system logs, an adversary may clear the command history of a compromised account to conceal the actions undertaken during an intrusion. Various command interpreters keep track of the commands users type in their terminal so that users can retrace what they've done.

On Linux and macOS, these command histories can be accessed in a few different ways. While logged in, this command history is tracked in a file pointed to by the environment variable `HISTFILE`. When a user logs off a system, this information is flushed to a file in the user's home directory called `~/.bash_history`. The benefit of this is that it allows users to go back to commands they've used before in different sessions. Adversaries may delete their commands from these logs by manually clearing the history (`history -c`) or deleting the bash history file `rm ~/.bash_history`.

Adversaries may also leverage a Network Device CLI on network devices to clear command history data (`clear logging` and/or `clear history`).[1] On ESXi servers, command history may be manually removed from the `/var/log/shell.log` file.[2]

On Windows hosts, PowerShell has two different command history providers: the built-in history and the command history managed by the `PSReadLine` module. The built-in history only tracks the commands used in the current session. This command history is not available to other sessions and is deleted when the session ends.

The `PSReadLine` command history tracks the commands used in all PowerShell sessions and writes them to a file (`$env:APPDATA\Microsoft\Windows\PowerShell\PSReadLine\ConsoleHost_history.txt` by default). This history file is available to all sessions and contains all past history since the file is not deleted when the session ends.[3]

Adversaries may run the PowerShell command `Clear-History` to flush the entire command history from a current PowerShell session. This, however, will not delete/flush the `ConsoleHost_history.txt` file. Adversaries may also delete the `ConsoleHost_history.txt` file or edit its contents to hide PowerShell commands they have run.[4][5]

Source: https://attack.mitre.org/techniques/T1070/003