Event Triggered Execution: Change Default File Association, Sub-technique T1546.001 - Enterprise

Archived: 2026-04-05 17:27:10 UTC

Adversaries may establish persistence by executing malicious content triggered by a file type association. When a file is opened, the default program used to open the file (also called the file association or handler) is checked. File association selections are stored in the Windows Registry and can be edited by users, administrators, or programs that have Registry access or by administrators using the built-in assoc utility.[1][2][3] Applications can modify the file association for a given file extension to call an arbitrary program when a file with the given extension is opened.

System file associations are listed under `HKEY_CLASSES_ROOT.[extension]`, for example `HKEY_CLASSES_ROOT.txt`. The entries point to a handler for that extension located at `HKEY_CLASSES_ROOT\[handler]`. The various commands are then listed as subkeys underneath the shell key at `HKEY_CLASSES_ROOT\[handler]\shell\[action]\command`. For example:

- `HKEY_CLASSES_ROOT\txtfile\shell\open\command`
- `HKEY_CLASSES_ROOT\txtfile\shell\print\command`
- `HKEY_CLASSES_ROOT\txtfile\shell\printto\command`

The values of the keys listed are commands that are executed when the handler opens the file extension. Adversaries can modify these values to continually execute arbitrary commands.[4]

Source: https://attack.mitre.org/techniques/T1546/001