T1546.001 - Change Default File Association

Description from ATT&CK

> 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. (Citation: Microsoft Change Default Programs)(Citation: Microsoft File Handlers) (Citation: Microsoft Assoc Oct 2017) 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.(Citation: TrendMicro TROJ-FAKEAV OCT 2012)

Atomic Tests

- Atomic Test #1 - Change Default File Association

Atomic Test #1 - Change Default File Association

Change Default File Association From cmd.exe of hta to notepad.

Upon successful execution, cmd.exe will change the file association of .hta to notepad.exe.

Supported Platforms: Windows

auto_generated_guid: 10a08978-2045-4d62-8c42-1957bbbea102

Inputs:

- T1037.001
- T1037.002
- T1037.004
- T1037.005
- T1039
- T1040

Name	Description	Type	Default Value
target_extension_handler	txtfile maps to notepad.exe	Path	txtfile
extension_to_change	File Extension To Hijack	String	.hta
original_extension_handler	File Extension To Revert	String	htafile

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

```
assoc #{extension_to_change}=#{target_extension_handler}
```

Cleanup Commands:

```
assoc  #{extension_to_change}=#{original_extension_handler}
```