Squirrel packages' manager as a lolbin (a.k.a. many Electron apps are lolbins by default)

A week ago, or so I posted this Twit that refers to Slack's executables as lolbins… I have already posted about it last year – the Slack's *update.exe* is a nice lolbin, because it's actually a Squirrel packages' manager in disguise. A side effect of using Electron.

I was wondering if this is a common pattern, and if Slack is the only software producer that relies on this software paradigm. Right… yeah, I know, the *paradigm* sounds very academic and serious, but it's just about software development frameworks, file naming, their final placement on the user's system, their behavior, and in the end… what you get from a command line when you run *update.exe /?*. Or something along these lines if the software authors relied on the same Electron framework as the one Slack did , and as my Twit shown – it was deemed to be 'Lolbinish'.

So, before we go any further, here's is a TL; DR; for you – run this on your (test/targeted) system:

```
C:\Users>dir /a/b/s update.exe
```

This will give you a list of potential candidates of programs that may in fact be wrappers of Squirrel packages' manager.

Once you run the cherry-picked *update.exe* you will typically get this banner:

```
Usage: Squirrel.exe command [OPTS]
   Manages Squirrel packages
[...]
```

– and… yup… you can use it as a Lolbin as described in my Twit and last year's post:

- %USERPROFILE%\AppData\Local\<app>\update.exe –processStart "test.exe" (*where test.exe must be placed in a app-* subfolder)*

You can not only run programs via proxy, but also e.g. create shortcuts:

- %USERPROFILE%\AppData\Local\<app> \update.exe –createShortcut -l <parameters> e.g.:
  - %USERPROFILE%\AppData\Local\slack\update.exe –createShortcut c:\WINDOWS\system32\mspaint.exe -l Desktop,StartMenu

After googling around, I can confirm that there are more apps placing *update.exe* on user's systems, including, but not limited to:

- Discord
- Slack

- Huddly
- Whatsapp
- Yammer

I bet there is more. I bet there will be more in the future, because Electron is a popular framework for the current app ecosystem that wants to deliver to Windows, Linux, OSX at the same time.

When you browse the https://electronjs.org/ web site, you can find references to many applications built using this framework:

- 1Clipboard
- Atom
- Beaker Browser
- Caret
- Collectie
- Discord
- Figma
- Flow
- Ghost
- GitHub Desktop
- GitKraken
- Hyper
- Insomnia
- JIBO
- Kap
- Kitematic
- Now Desktop
- Simplenote
- Skype
- Slack
- Svgsus
- WebTorrent
- WordPress.com

Also, in some cases the update.exe doesn't produce any output if ran w/o any command line (e.g. when you run Discord). In such case you can just blindly try *Update.exe –processStart <file_inside_the_app_folder>*. I can confirm it still works and launches the program of our choice. Your mileage for other Electron apps may vary.

All in all, not a big deal, but good to know about. Both on a blue and red team side of the puzzle.

This entry was posted in **Living off the land**, **LOLBins** by **adam**. Bookmark the **permalink**.