Fireball

Tricky Installers & Bundled Adware

~rsk

Virginia Tech CS2604

11/11/2024

1. before we begin...

1.1. focus activity

1.1. focus activity

Figure 1: https://vtluug.org/users/~rsk/files/cs3604focus.html – first person to install the software wins!

1.2. did you see it?

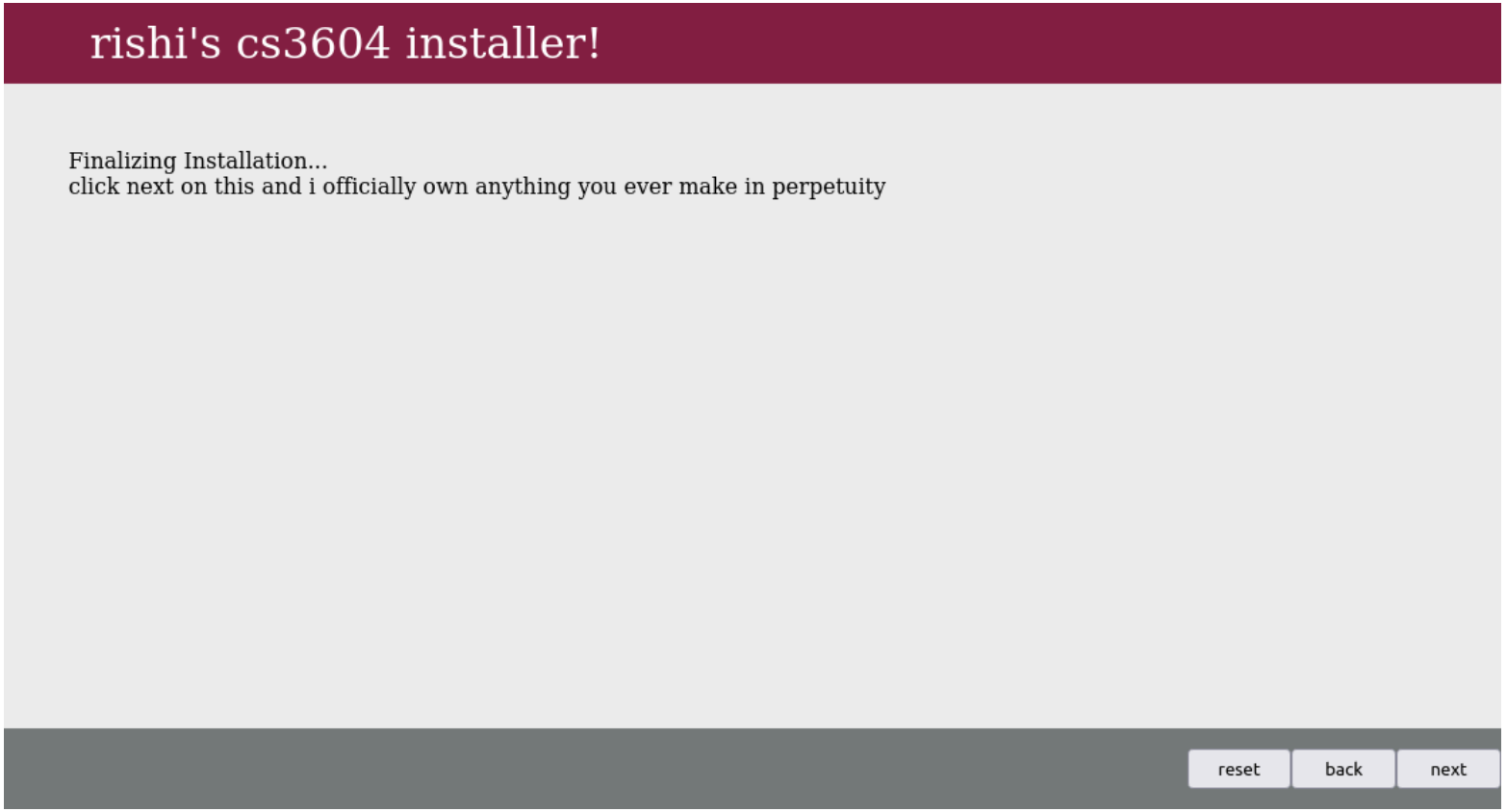

Figure 2: oops. hope ya didn't click next on this one.

1.3. did you see it?

Figure 3: or this one

2. Fireball

2.1. what is Fireball?

- made by Chinese company, Rafotech

2.1. what is Fireball?

- made by Chinese company, Rafotech
- subtle adware/malware

2.1. what is Fireball?

- made by Chinese company, Rafotech
- subtle adware/malware
- discovered in 2017

2.1. what is Fireball?

- made by Chinese company, Rafotech
- subtle adware/malware
- discovered in 2017
- thought to have infected 250,000,000 machines by that point

2.2. installation vector

Figure 4: while you click through the installer, you accidentally agree to install something you don't want

2.3. installation vector

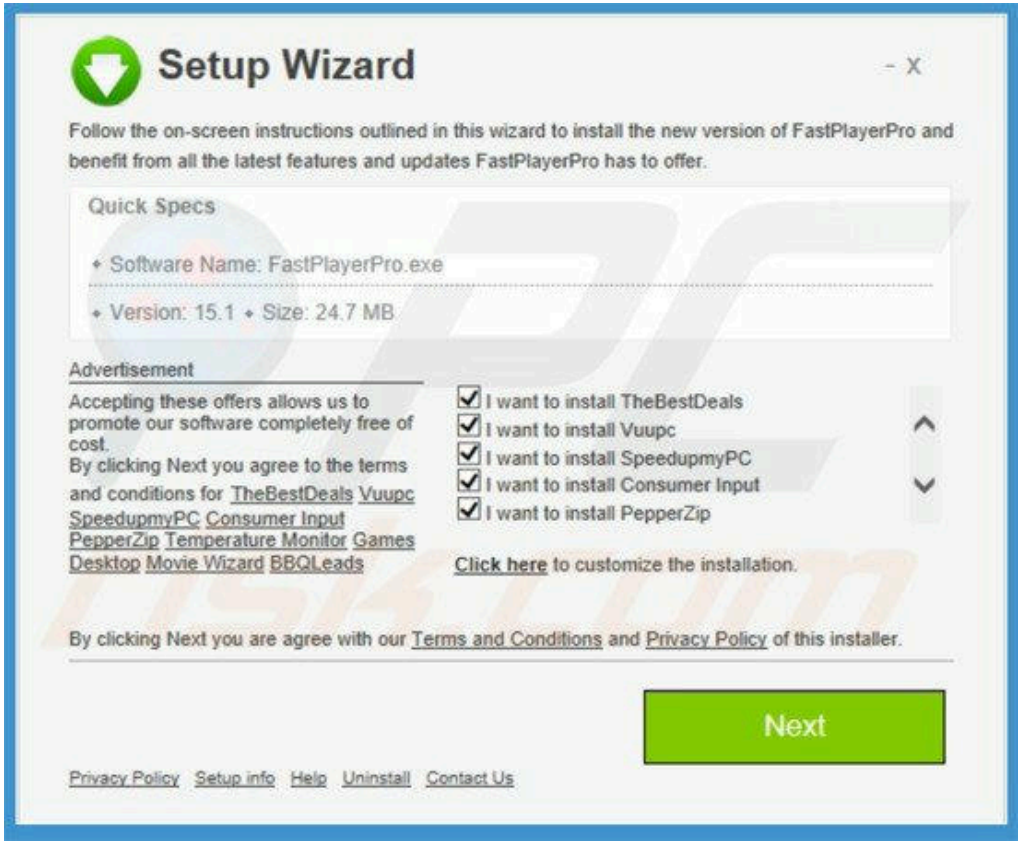

Figure 5: other software is subtly bundled with software you do want

2.4. reach via these methods

Country	% infected	Number of infections (in millions)	Hit Rate
India	10.1%	25.3	43%
Brazil	9.6%	24.1	38%
Mexico	6.4%	16.1	N/A
Indonesia	5.2%	13.1	60%
US	2.2%	5.5	10.7%

Figure 6: what percent of **every computer in the named country** is infected (data circa 2017)

2.5. changing web data

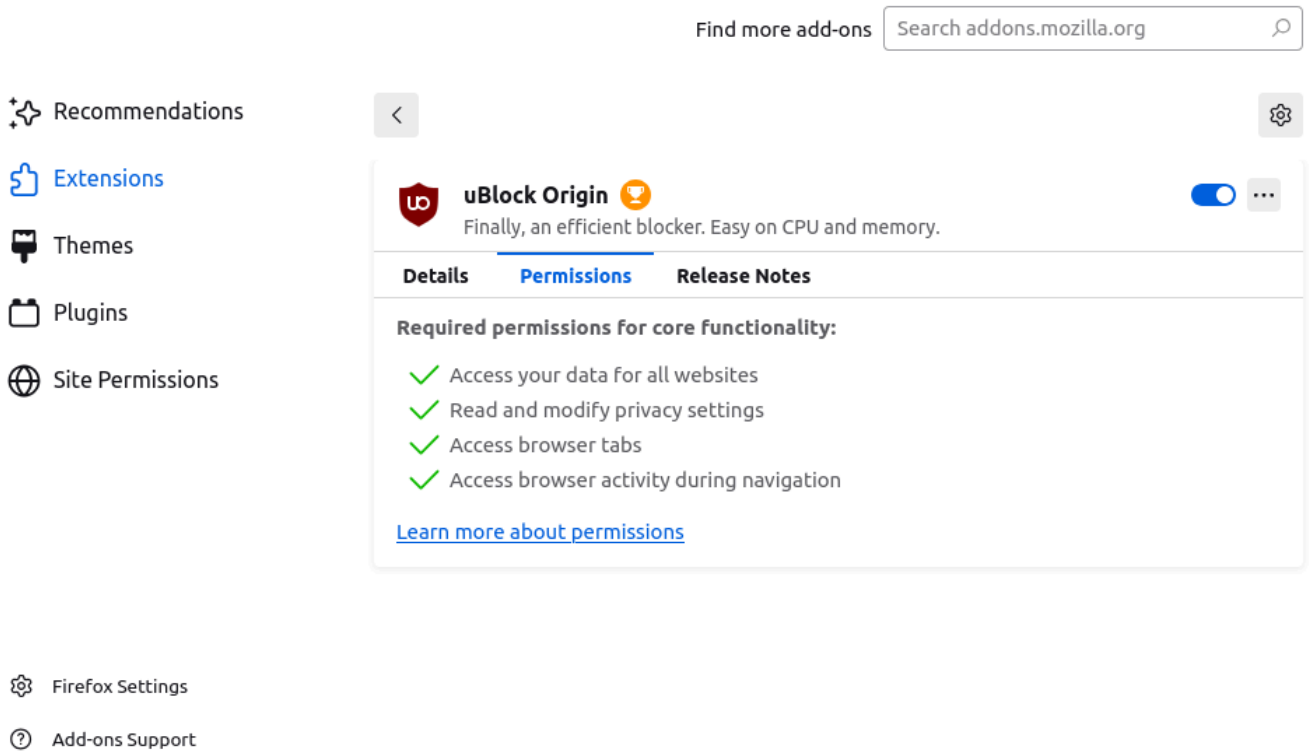

Figure 7: extensions added to your browser have the permission to edit web data without certificate errors

2.6. malicious activity

- changing advertisement frames to ones that pay the adware creators
- collecting browsing data to sell to ad marketing firms

2.6. malicious activity

- changing advertisement frames to ones that pay the adware creators
- collecting browsing data to sell to ad marketing firms
- though seemingly unused, the software also contains the self-unpacking code for arbitrary code excecution and installation
  - i.e. a rootkit

3. mitigations

3.1. package managers

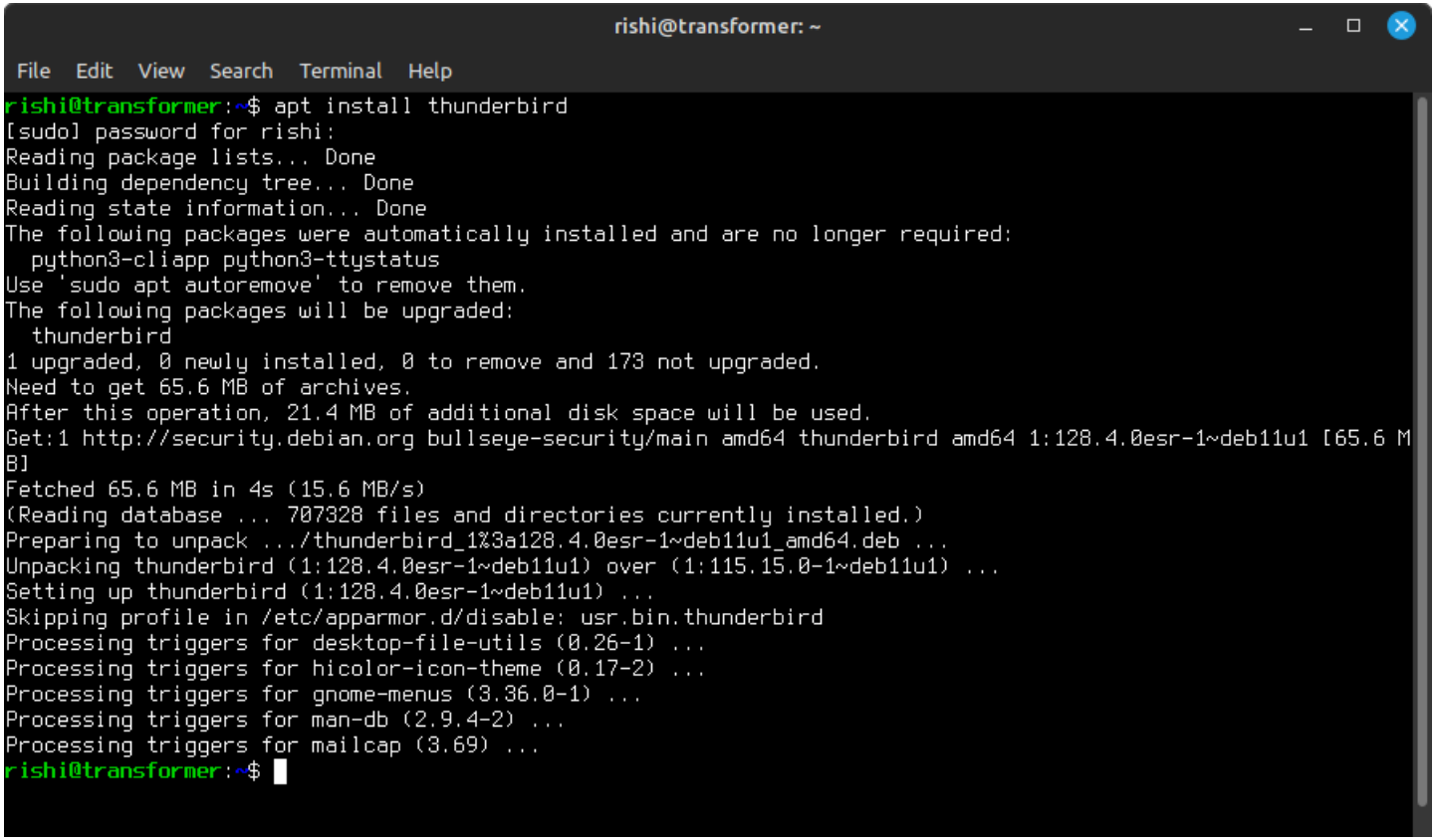

Figure 5: package managers, like the ones common on unixlike systems, avoid the whole installer question

3.2. installation manifests

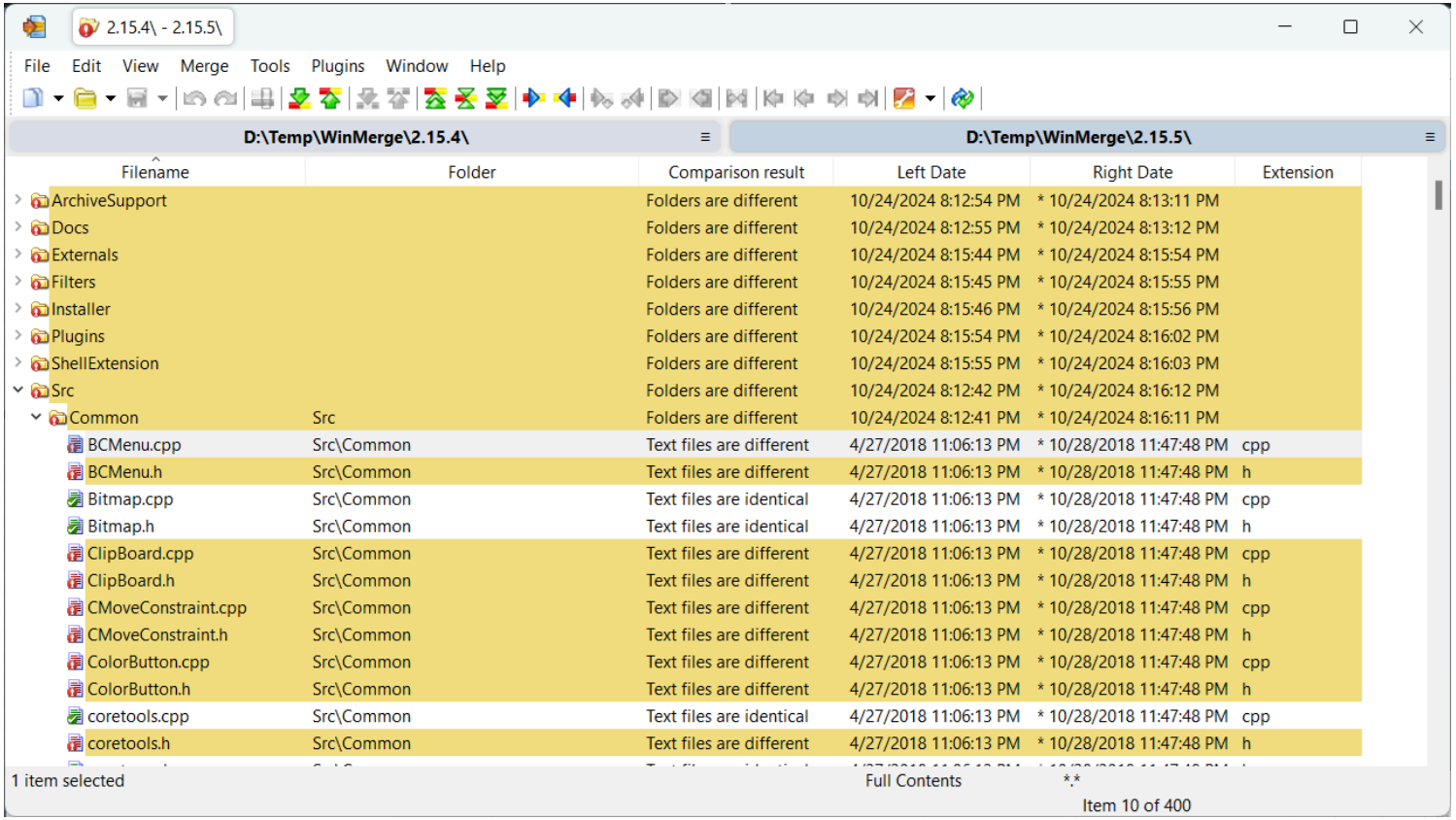

Figure 6: show what files are changed after an installation

4. relevance

4.1. persuasive/deceptive design

- you guys went through the example. if one of those screens you flipped through installed malware, would you say you were decieved?

4.1. persuasive/deceptive design

- you guys went through the example. if one of those screens you flipped through installed malware, would you say you were decieved?
- the people impacted by this technically agreed to install some software, but they didn't read or understand what they were actually agreeing to

4.1. persuasive/deceptive design

- you guys went through the example. if one of those screens you flipped through installed malware, would you say you were decieved?
- the people impacted by this technically agreed to install some software, but they didn't read or understand what they were actually agreeing to
- it's like a EULA or TOS

5. discussion

5.1. discussion questions

- One of the major selling points of Windows as an Operating System is its ease of use, and this includes the ability to simply distribute .exe or .msi installers for software. Is the convenience this provides better in the long term than the technical upkeep of a dependency-based package manager, like those used on most Linux systems?
- Ethics aside, should it be legal to install software on to the system of a user if they agree to it, but you know they probably don't understand what is being agreed to? Keep in mind this affects backround analytics and similar tools as well.

5.2. shoutout the luug

the linux & unix users group @ virginia tech meets every wednesday at 7pm in McBryde 240. we have

- a linked chatroom on IRC and Matrix (Discord is nonfree privacy-infringing software)
- a bunch of servers and IPv4 addresses to play with
- a bunch of services for members, incl. NAS storage

for more info visit vtluug.org