

Fireball

Tricky Installers & Bundled Adware

~rsk

Virginia Tech CS2604

11/11/2024

1. before we begin...

1.1. focus activity



1. before we begin...



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

1.2. did you see it?



1. before we begin...

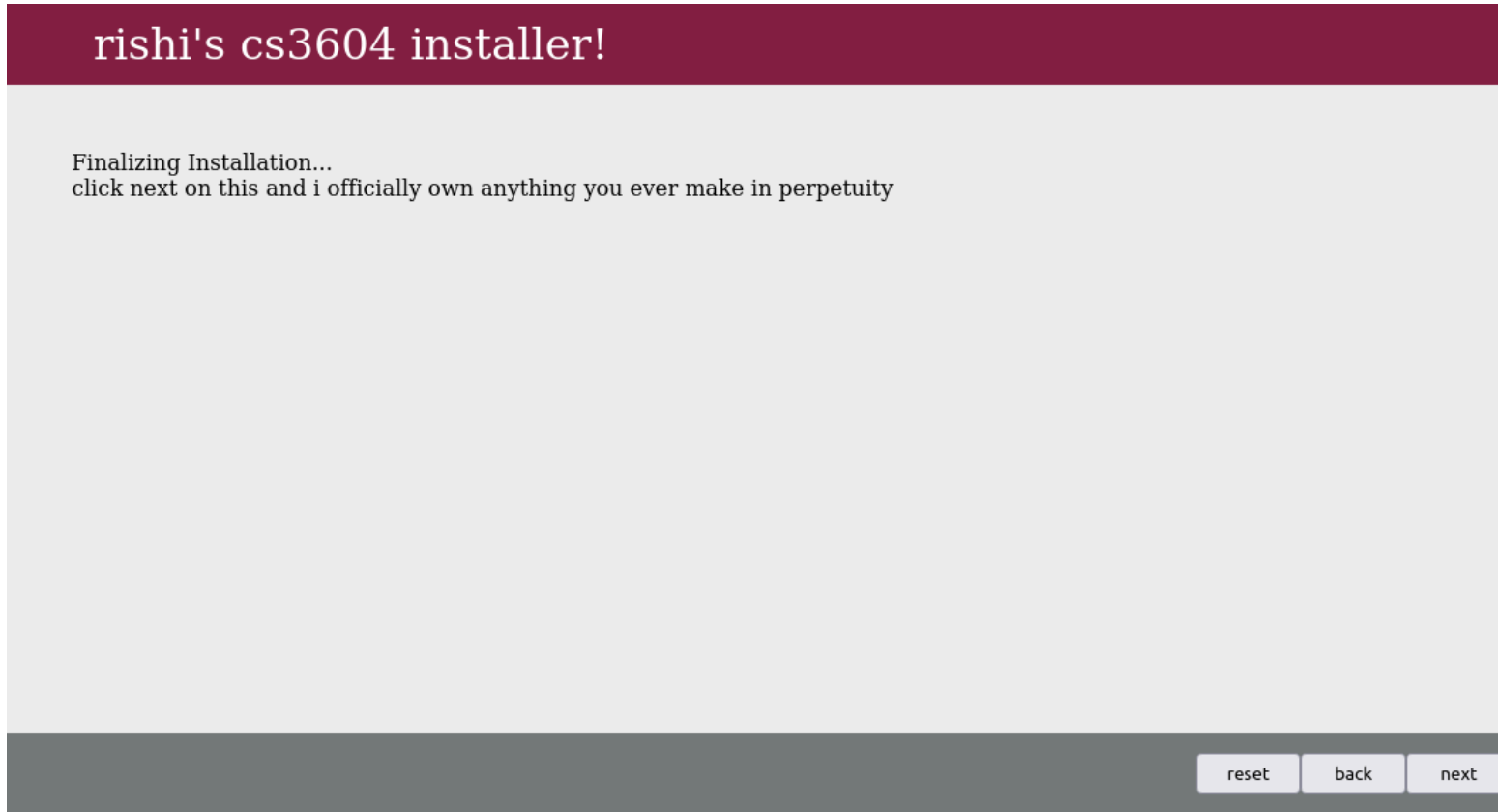


Figure 2: oops. hope ya didn't click next on this one.

1.3. did you see it?



1. before we begin...

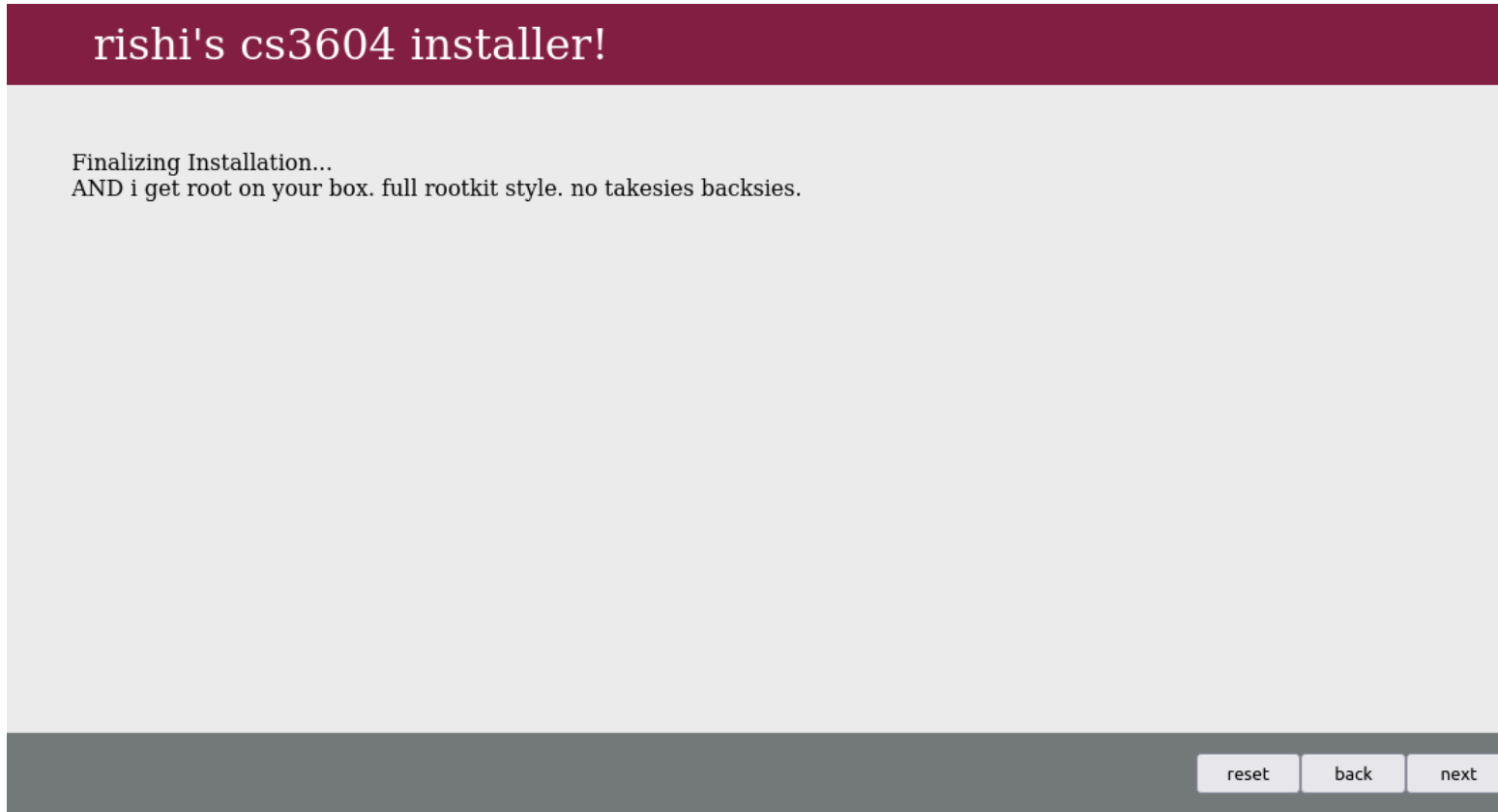


Figure 3: or this one

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

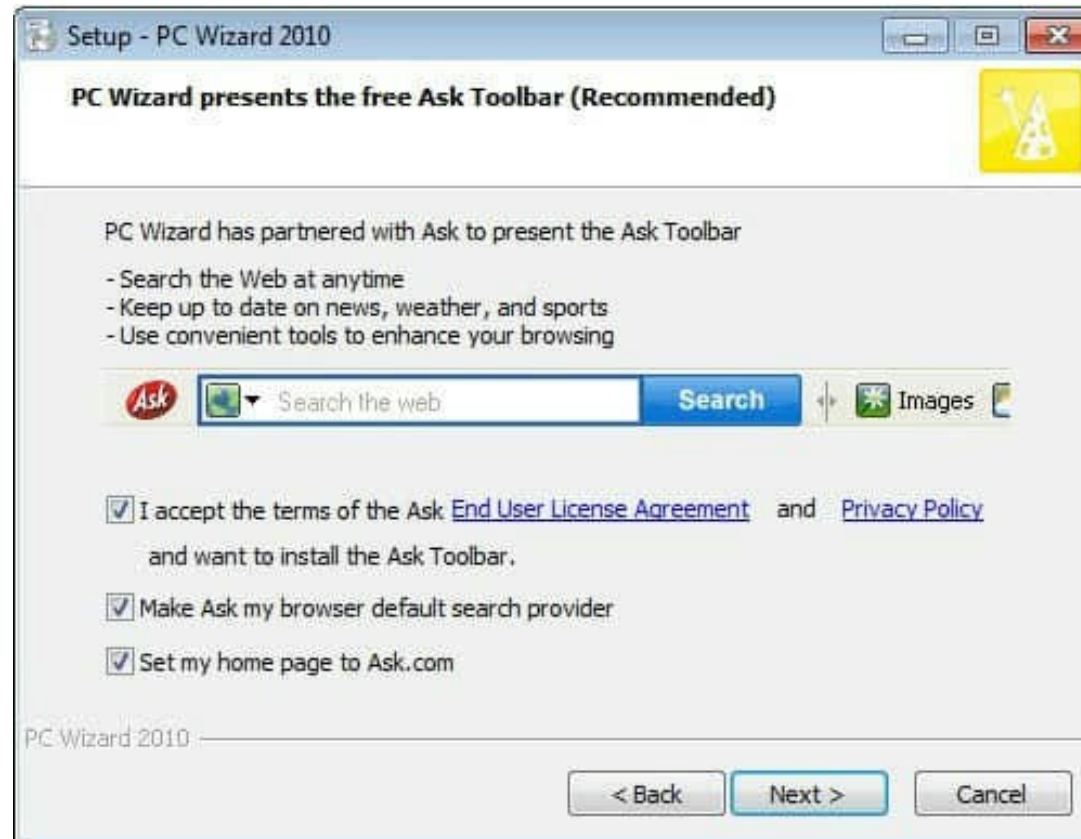


Figure 4: while you click through the installer, you accidentally agree to install something you don't want

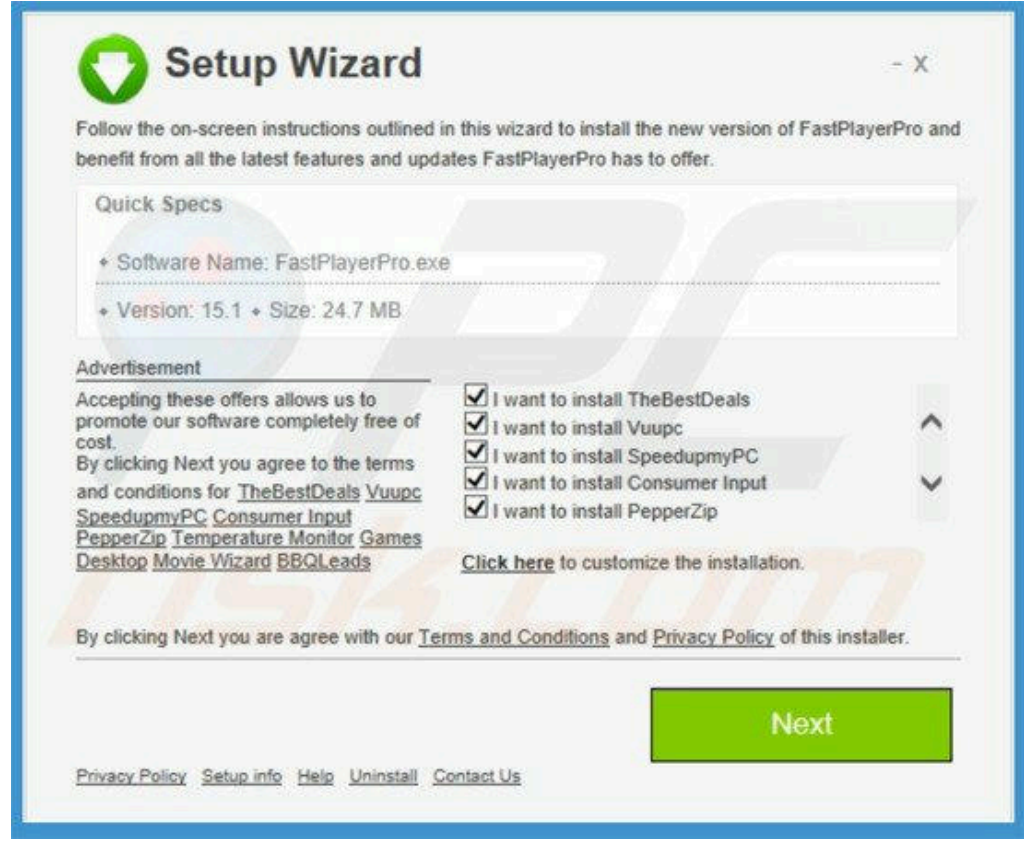


Figure 5: other software is subtly bundled with software you do want

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

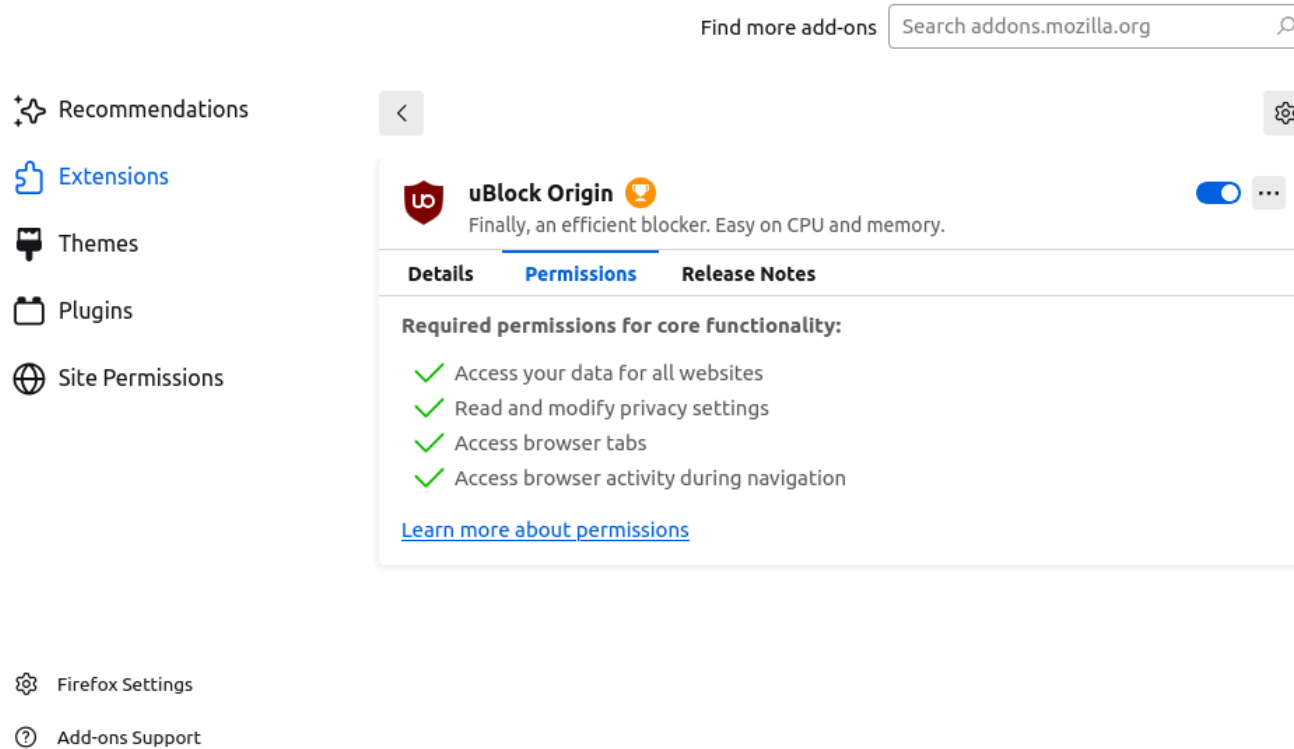


Figure 7: extensions added to your browser have the permission to edit web data without certificate errors

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 execution and installation
 - ▶ i.e. a rootkit

3. mitigations

```
rishi@transformer: ~  
File Edit View Search Terminal Help  
rishi@transformer:~$ apt install thunderbird  
[sudo] password for rishi:  
Reading package lists... Done  
Building dependency tree... Done  
Reading state information... Done  
The following packages were automatically installed and are no longer required:  
  python3-cliapp python3-ttystatus  
Use 'sudo apt autoremove' to remove them.  
The following packages will be upgraded:  
  thunderbird  
1 upgraded, 0 newly installed, 0 to remove and 173 not upgraded.  
Need to get 65.6 MB of archives.  
After this operation, 21.4 MB of additional disk space will be used.  
Get:1 http://security.debian.org bullseye-security/main amd64 thunderbird amd64 1:128.4.0esr-1~deb11u1 [65.6 M  
B]  
Fetched 65.6 MB in 4s (15.6 MB/s)  
(Reading database ... 707328 files and directories currently installed.)  
Preparing to unpack .../thunderbird_1%3a128.4.0esr-1~deb11u1_amd64.deb ...  
Unpacking thunderbird (1:128.4.0esr-1~deb11u1) over (1:115.15.0-1~deb11u1) ...  
Setting up thunderbird (1:128.4.0esr-1~deb11u1) ...  
Skipping profile in /etc/apparmor.d/disable: usr.bin.thunderbird  
Processing triggers for desktop-file-utils (0.26-1) ...  
Processing triggers for hicolor-icon-theme (0.17-2) ...  
Processing triggers for gnome-menus (3.36.0-1) ...  
Processing triggers for man-db (2.9.4-2) ...  
Processing triggers for mailcap (3.69) ...  
rishi@transformer:~$
```

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

Filename	Folder	Comparison result	Left Date	Right Date	Extension
> ArchiveSupport		Folders are different	10/24/2024 8:12:54 PM	* 10/24/2024 8:13:11 PM	
> Docs		Folders are different	10/24/2024 8:12:55 PM	* 10/24/2024 8:13:12 PM	
> Externals		Folders are different	10/24/2024 8:15:44 PM	* 10/24/2024 8:15:54 PM	
> Filters		Folders are different	10/24/2024 8:15:45 PM	* 10/24/2024 8:15:55 PM	
> Installer		Folders are different	10/24/2024 8:15:46 PM	* 10/24/2024 8:15:56 PM	
> Plugins		Folders are different	10/24/2024 8:15:54 PM	* 10/24/2024 8:16:02 PM	
> ShellExtension		Folders are different	10/24/2024 8:15:55 PM	* 10/24/2024 8:16:03 PM	
> Src		Folders are different	10/24/2024 8:12:42 PM	* 10/24/2024 8:16:12 PM	
> Common	Src	Folders are different	10/24/2024 8:12:41 PM	* 10/24/2024 8:16:11 PM	
BCMenu.cpp	Src\Common	Text files are different	4/27/2018 11:06:13 PM	* 10/28/2018 11:47:48 PM	cpp
BCMenu.h	Src\Common	Text files are different	4/27/2018 11:06:13 PM	* 10/28/2018 11:47:48 PM	h
Bitmap.cpp	Src\Common	Text files are identical	4/27/2018 11:06:13 PM	* 10/28/2018 11:47:48 PM	cpp
Bitmap.h	Src\Common	Text files are identical	4/27/2018 11:06:13 PM	* 10/28/2018 11:47:48 PM	h
Clipboard.cpp	Src\Common	Text files are different	4/27/2018 11:06:13 PM	* 10/28/2018 11:47:48 PM	cpp
Clipboard.h	Src\Common	Text files are different	4/27/2018 11:06:13 PM	* 10/28/2018 11:47:48 PM	h
CMoveConstraint.cpp	Src\Common	Text files are different	4/27/2018 11:06:13 PM	* 10/28/2018 11:47:48 PM	cpp
CMoveConstraint.h	Src\Common	Text files are different	4/27/2018 11:06:13 PM	* 10/28/2018 11:47:48 PM	h
ColorButton.cpp	Src\Common	Text files are different	4/27/2018 11:06:13 PM	* 10/28/2018 11:47:48 PM	cpp
ColorButton.h	Src\Common	Text files are different	4/27/2018 11:06:13 PM	* 10/28/2018 11:47:48 PM	h
coretools.cpp	Src\Common	Text files are identical	4/27/2018 11:06:13 PM	* 10/28/2018 11:47:48 PM	cpp
coretools.h	Src\Common	Text files are different	4/27/2018 11:06:13 PM	* 10/28/2018 11:47:48 PM	h

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 deceived?



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 deceived?
- ▶ 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 deceived?
- ▶ 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 background 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