

## Bolt-Recover

**Please read these instructions carefully so that you know what you are doing!**

In this writeup we will go through the whole process of recovering and renaming your data hit by the deadbolt ransomware. This tutorial works for QNAP and Asustor, we are working on a separate solution for TerraMaster devices.

Please be aware, that this ransomware is more advanced than Qlocker, a previous ransomware we worked on. We are very limited with our options to recover the files and rely on files being deleted before the attack. Please don't see this as a magical tool which will get all your data back. It will help you recovering what can be recovered, copy non affected files and it will show you which files you actually lost.

## You will need

- For Windows users: WSL (Windows subsystem for Linux)
- External HDD with a capacity of at least 2x your NAS, we recommend 3x bigger
- Connection to your NAS and to the internet
- the IP address of your PC (**ipconfig** / **all** on Windows cmd, **ip address** on Linux)

## Let's recover your data

First, we need to install WSL

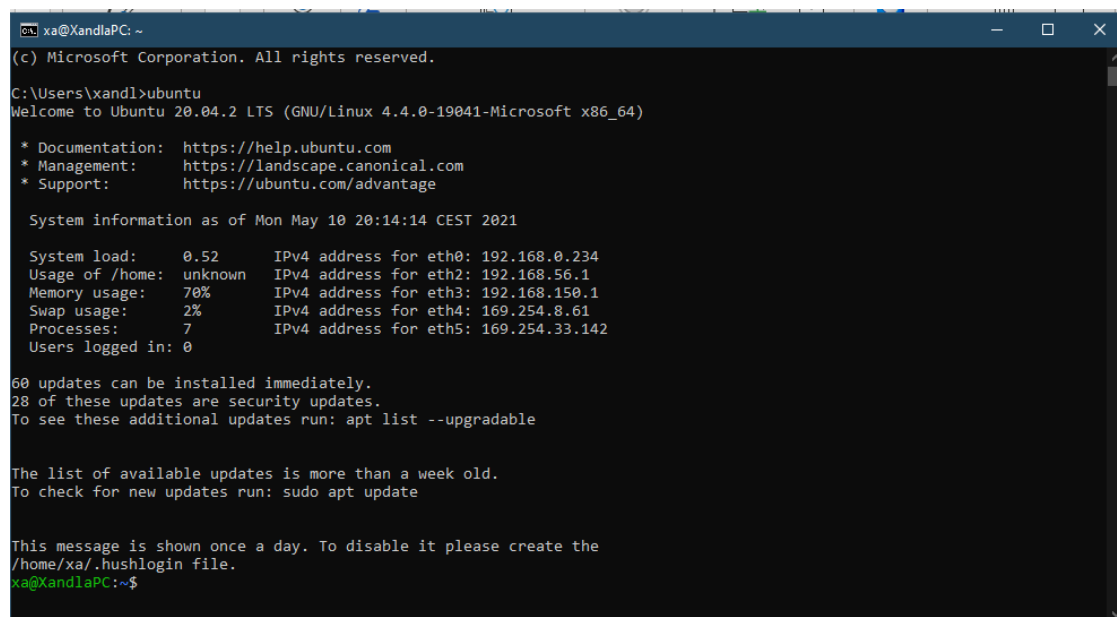
This will be our terminal where we will execute all commands.

Download it from the windows store and reboot after installation.

[Get Ubuntu - Microsoft Store](#)

Now open CMD by pressing **Win+R** and **cmd**, or just search for **cmd** in windows.

Type **ubuntu** in the command prompt which opened. It should look like this:



```
xa@XandlaPC: ~
(c) Microsoft Corporation. All rights reserved.

C:\Users\xandl>ubuntu
Welcome to Ubuntu 20.04.2 LTS (GNU/Linux 4.4.0-19041-Microsoft x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

System information as of Mon May 10 20:14:14 CEST 2021

System load:  0.52      IPv4 address for eth0: 192.168.0.234
Usage of /home: unknown  IPv4 address for eth2: 192.168.56.1
Memory usage: 70%      IPv4 address for eth3: 192.168.150.1
Swap usage:   2%        IPv4 address for eth4: 169.254.8.61
Processes:    7          IPv4 address for eth5: 169.254.33.142
Users logged in: 0

60 updates can be installed immediately.
28 of these updates are security updates.
To see these additional updates run: apt list --upgradable

The list of available updates is more than a week old.
To check for new updates run: sudo apt update

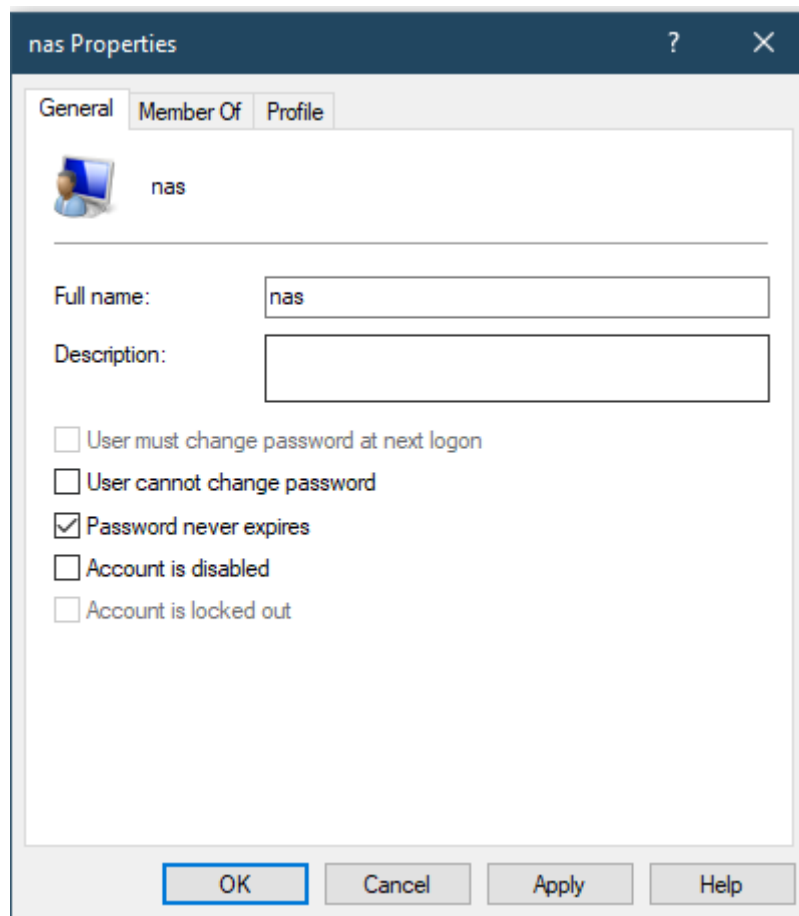
This message is shown once a day. To disable it please create the
/home/xa/.hushlogin file.
xa@XandlaPC:~$
```

- 1.) Now run these three commands:  
**sudo apt-get update**  
**sudo apt install rhash**

## Recover the Deleted Data with PhotoRec

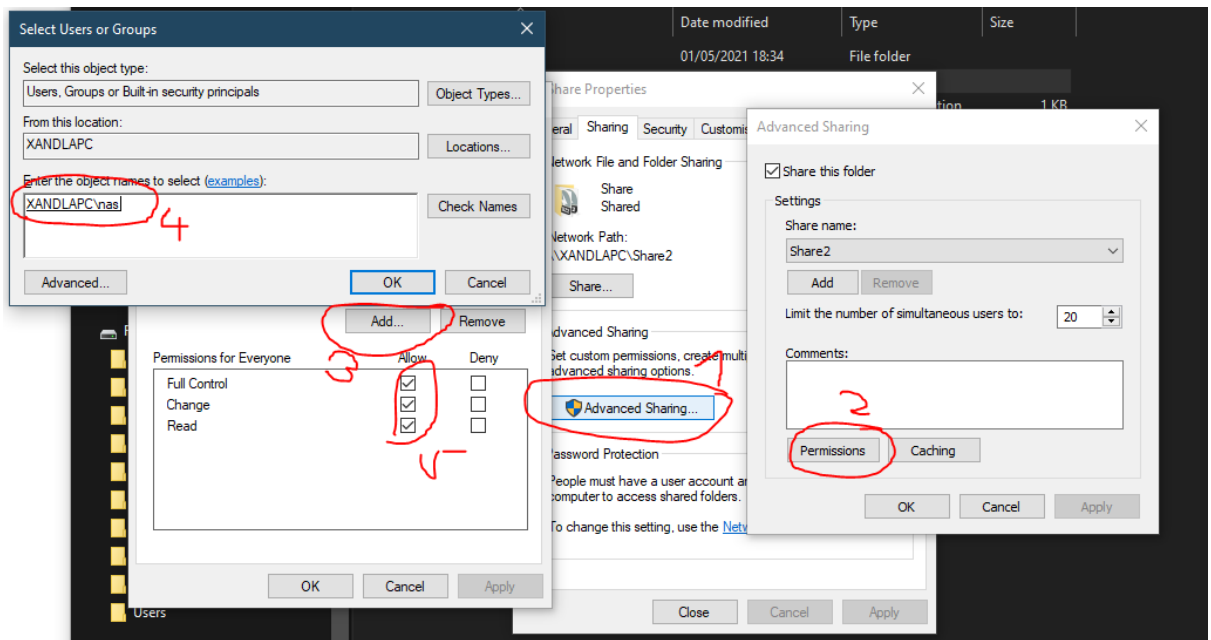
If you have already recovered your data with PhotoRec you can skip this part. This is basically the same as the tutorial from my other post, but I added some parts for completion.

- 2.) Connect an external hard drive to a PC which can be left turned on overnight. The size of the hard drive must be at least as big as the capacity of your NAS.
- 3.) On the harddisk create a folder called **Share**
- 4.) Create a new user called **nas** with the password **12345**:



Right click on **This PC** -> **Manage** -> **Local Users and groups** -> **Users**-> **new**

- 5.) Go back to the share folder you just created  
Right click on **Share** -> **Properties** -> go to sharing-tab **share** -> **advanced sharing** -> **permissions** -> **add** -> enter as user **nas**, password **12345** -> tick the box **full control**



- 6.) Download the data recovery tool PhotoRec.  
Note: There are two versions. We download both and determine later which one we need:

<https://www.cgsecurity.org/testdisk-7.2-WIP.arm-none-linux-gnueabi.tar.bz2>

Rename it to **testdisk-i.tar.bz2**

[https://www.cgsecurity.org/testdisk-7.2-WIP.linux26-x86\\_64.tar.bz2](https://www.cgsecurity.org/testdisk-7.2-WIP.linux26-x86_64.tar.bz2)

Rename it to **testdisk-x.tar.bz2**

- 7.) Move them to the **Share** folder  
8.) Go to your terminal window where you started **ubuntu**  
Connect to your NAS via SSH:

**ssh <user>@<IP-NAS>** (for example: **ssh admin@192.168.1.80**)

and enter the password of your user:

```
ka@XandlaPC:~$
ka@XandlaPC:~$ ssh admin@192.168.1.80
```

if successful this prompt should be visible:

[~]#

Maybe you have to leave the QNAP menu system by pressing **q** for quit and **y** for yes.

- 9.) Enter the following commands on your NAS prompt:

**mkdir /mnt/rescue-share**

**sudo mount -t cifs -o user=nas //192.168.1.2/Share /mnt/rescue-share**

(possibly replace **nas** with your user from above, **192.168.1.2** with the IP address of your PC, and **Share** with the name of the share you created)

**cd /mnt/rescue-share**

Troubleshooting: If you get the following error: "mount error(112): Host is down"

Please enable in SMB Windows

(<https://docs.microsoft.com/en-US/windows-server/storage/file-server/troubleshoot/detect-enable-and-disable-smbv1-v2-v3>)

- 10.) Determine the version of PhotoRec you need:

**uname -a**

```
xa@XandlaPC: ~  
[~] # uname -a  
[~] #
```

If the output is something with **x86\_64**:

```
tar -xvf testdisk-x.tar.bz2  
cd testdisk*  
chmod +x ./photorec_static  
sudo ./photorec_static
```

Else

```
tar -xvf testdisk-i.tar.bz2  
cd testdisk*  
chmod +x ./photorec  
sudo ./photorec
```

- 11.) Choose the **/dev/mapper/cachedev1** partition which should show up. Or choose the disk you stored your files at. Usually, it is the one with the highest capacity.  
Choose **ext2/3/4** file format  
Choose **ext2/ext3** option
- 12.) Choose **Free** (It took me about 24 hours. Don't be scared if it says it will take a long time, the estimation of the time is not very accurate.)
- 13.) Choose the **Shared** folder! Navigate to **..** (2nd from top). You could also create a new folder if you want to, but it must be within the Shared folder. Otherwise, it will not show up.  
If you choose a folder on your NAS by accident, you will overwrite the files you are trying to backup! Take care!
- 14.) After the undeleting process is completed, open your file explorer on windows and copy all files from your NAS to your external hard drive to the folder **Encrypted**. The folder must be at the same level as your **Share** folder.  
(You do not have to do this step, if you want to save space on your hard drive and feel confident enough to mount your nas as a drive like shown in step 18.a))

## Rename and copy your files with our script

You need three folders. One called **Share**, where all the data from PhotoRec is stored, another one called **Encrypted**, where all your files from your NAS are (the .deadbolt ones) and you need to create a new one called **Export**.

- 15.) You do not need to be connected to your NAS anymore. So, quit the ssh connection and return to the ubuntu shell:  
**exit**
- 16.) Download the **bolt-recover** script from: **xxx**  
Copy it to your external hard drive. It needs to be at the same level as your three folders.

Name	Date modified	Type	Size
Encrypted	12/03/2022 00:39	File folder	
Export	12/03/2022 00:39	File folder	
Share	12/03/2022 00:39	File folder	
bolt-recover	01/03/2022 10:29	File	8 KB

- 17.) Go to your ubuntu shell
- 18.) Mount your external hard drive so ubuntu can see and access it  
`sudo mkdir /mnt/f`  
`sudo mount -t drvfs <letterOfDrive>: /mnt/f`  
e.g.: `sudo mount -t drvfs d: /mnt/f`

18.a)

If you feel confident enough to mount your NAS directly, you can save a lot of space on your hard drive, as we do not need to copy the files to your drive as in step 14).

<https://www.qnap.com/en/how-to/knowledge-base/article/two-alternative-methods-to-map-the-shared-folder-as-the-network-drive-in-windows>

So, let's assume you mounted your NAS drive in Windows explorer to drive Z:

`sudo mount -t drvfs z: /mnt/z`

If you choose to do this, please make sure to adjust the path in step 21.)

- 19.) `cd /mnt/f`
- 20.) Check if files are there  
`ll`

```
drwxrwxrwx 1 as as 4096 Mar 12 00:39 ./
drwxrwxrwx 1 as as 4096 Mar 12 00:39 ../
drwxrwxrwx 1 as as 4096 Mar 12 00:39 Encrypted/
drwxrwxrwx 1 as as 4096 Mar 12 00:39 Export/
drwxrwxrwx 1 as as 4096 Mar 12 00:39 Share/
-rwxrwxrwx 1 as as 7415 Mar  1 10:29 bolt-recover*
```

- 21.) Change the paths in the script if needed:  
`vi bolt-recover`  
Navigate with your arrow keys down where the paths are specified.  
If you did step 18.a) please change "Encrypted" to: `Encrypted="/mnt/z"`

```
PhotoRec="/mnt/f/Share"
Encrypted="/mnt/f/Encrypted"
Restored="/mnt/f/Export"
StartDir=$(pwd)
```

If changes are needed press `i` to insert text.

If you are done, press `ESC` and enter `:wq` and press the enter key.

- 22.) After you closed the editor type

**chmod +x bolt-recover**

- 23.) Execute the script by entering

**./bolt-recover**

It will take a while. The script will display progress in 10% steps. Do not worry if it looks stuck. Depending on the number of files in Share and Encrypted folders it can take more than one day.

```
bolt-recover version 0.83d running...
Tue Mar  1 10:30:07 CET 2022

Total Files on Encryptd = 77040
Total crypted .deadbolt Count = 54971
Total unencrypted Count = 22069

Calculating Sizes...

RHash: /mnt/e/Share/recup_dir.258/f3705403096_Persbackup_ini.gz: Invalid argument
Making Directory Structure...
Directory Count = 3866
Creating files...
10% . 20% . 30% . 40% . 50% . 60% . 70% . 80% . 90% . 100% .

Created batch files (call in this order!):
recreate:   recreates directories on Export           // all directories from Encryptd
renamer:    copies * from PhotoRec to Export           // with matching size and file ext
redater:    changes * filedatetime in Export           // already processed with renamer
notcryp:    copies * from Encryptd to Export           // unencrypted files - not affected
notcrypdel: deletes * from Encryptd                   // unencrypted files - not affected
remover:    deletes processed deadbolt in Encryptd    // all deadbolt with matching size
duplicates: deletes processed * in PhotoRec           // and all with same size

What remains to be done:
In PhotoRec: files that were already deleted before deadbolt (maybe old but unencrypted)
In Encryptd: deadbolt files for which there was no recoverable deleted file (maybe so
ool)
notfound.csv contains them without ending .deadbolt (plus Count [usually
etime)

Tue Mar  1 16:49:46 CET 2022
Recoverable files: 3394 of 54971 (6%)
```

- 24.) After the first Script is completed, you will find that there will be other scripts on your drive. If you want to only use some functions, you can call the scripts individually or just enter the command from step 31) to execute everything in order.

- 25.) Creates the directory structure within Export:

**./recreate**

- 26.) Copying and renaming the recovered files to Export.

**./renamer**

- 27.) Deadbolt sometimes won't encrypt large files like videos. For this, use the following script to copy unaffected files to the Export folder.

**./notcryp**

- 28.) There will be files that our script cannot match as there will be files with the same size. It will create a .csv file with all missing files which can be manually searched if wanted. Just import the file into a spreadsheet program. It shows you the possible matches for one file and you can check your most important files manually.

**notfound.csv**

- 29.) If you want to delete the .deadbolt files from the hard drive run this. Only .deadbolt files that were used for renaming are deleted.  
**./remover**
- 30.) If you want to look for the remaining files manually run this command because it will remove all files we already recovered and do not need to be looked at again.  
**./duplics**
- 31.) If you want to use all functions:  
**./recreate; ./renamer; ./notcryp; ./remover; ./duplics**

What remains to be done after running all the scripts:

- 32.) In the **PhotoRec** directory tree (e.g. **/mnt/f/Share**) are recovered files that could not be matched with their original name. You may want to look through them manually.
- 33.) In the **Encrypted** directory tree (e.g. **/mnt/f/Encrypted** or **/mnt/z**) are .deadbolt files for which there was no recoverable deleted file. Please keep a copy of those remaining (i.e. unrecoverable) .deadbolt files because someday we might have the ability to decrypt them with a key. The file **notfound.csv** contains them without ending .deadbolt.
- 34.) If you are still missing files and you remember some unique contents of it, you can enable indexing in windows search and add your /Share folder to be indexed. Now you can search for bits and pieces you might remember. The reason for this step is, that there may be an older (un)deleted version of your file (that therefore has a different file size than the encrypted file and cannot be recovered automatically).  
<https://www.groovypost.com/howto/search-through-file-contents-windows-10/>  
<https://www.tenforums.com/tutorials/58756-add-remove-search-index-locations-windows-10-a.html>

Now all your data should show up in the folder **Export**.

I hope I could help you with this guide. If you have any questions, feel free to contact me at:  
[grecover.xandl@gmail.com](mailto:grecover.xandl@gmail.com)