

Massive Qlocker ransomware attack uses 7zip to encrypt QNAP devices

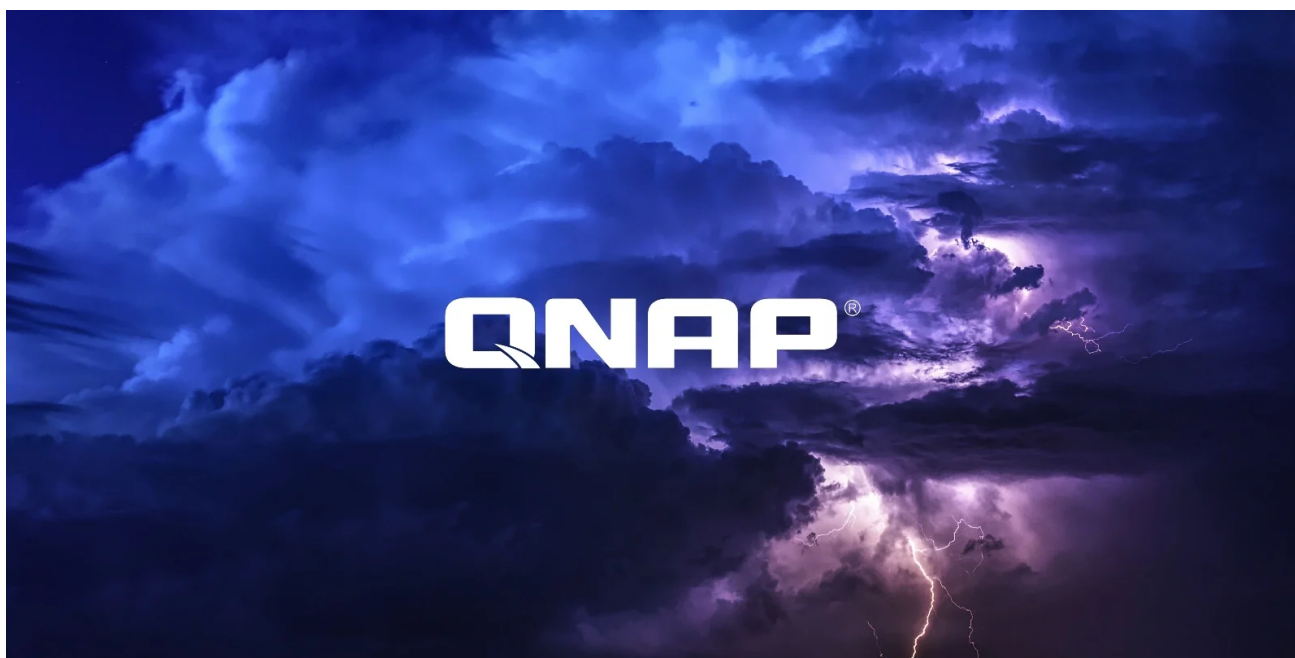
bleepingcomputer.com/news/security/massive-qlocker-ransomware-attack-uses-7zip-to-encrypt-qnap-devices/

Lawrence Abrams

By

[Lawrence Abrams](#)

- April 21, 2021
- 01:44 PM
- [482](#)

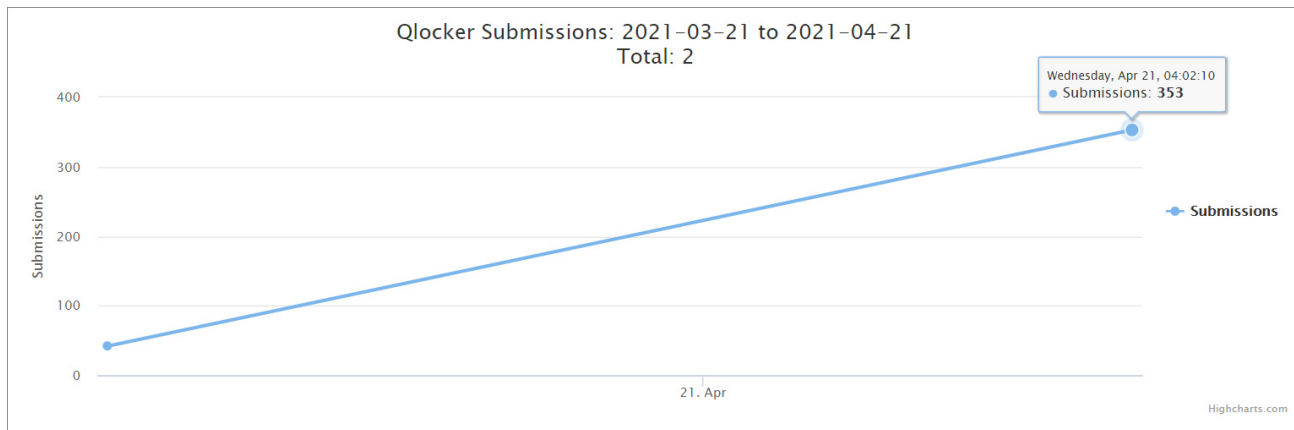


Update 4/22/21: A bug was discovered last night that allowed victims to recover their 7zip password for free but was fixed soon after being discovered. You can find more info in the update below.

Update 4/24/21: A [frequently asked questions](#) section has been added to the bottom of the article.

A massive ransomware campaign targeting QNAP devices worldwide is underway, and users are finding their files now stored in password-protected 7zip archives.

The ransomware is called Qlocker and began targeting QNAP devices on April 19th, 2021. Since then, there has been an enormous amount of activity in our support forum, and the [ID-Ransomware](#) ransomware identification site has seen a surge of submissions from victims.



ID-R submissions from Qlocker victims

According to reports from victims in a [BleepingComputer Qlocker support topic](#), the attackers use 7-zip to move files on QNAP devices into password-protected archives. While the files are being locked, the QNAP Resource Monitor will display numerous '7z' processes which are the 7zip command-line executable.

Control Panel
Resource Monitor

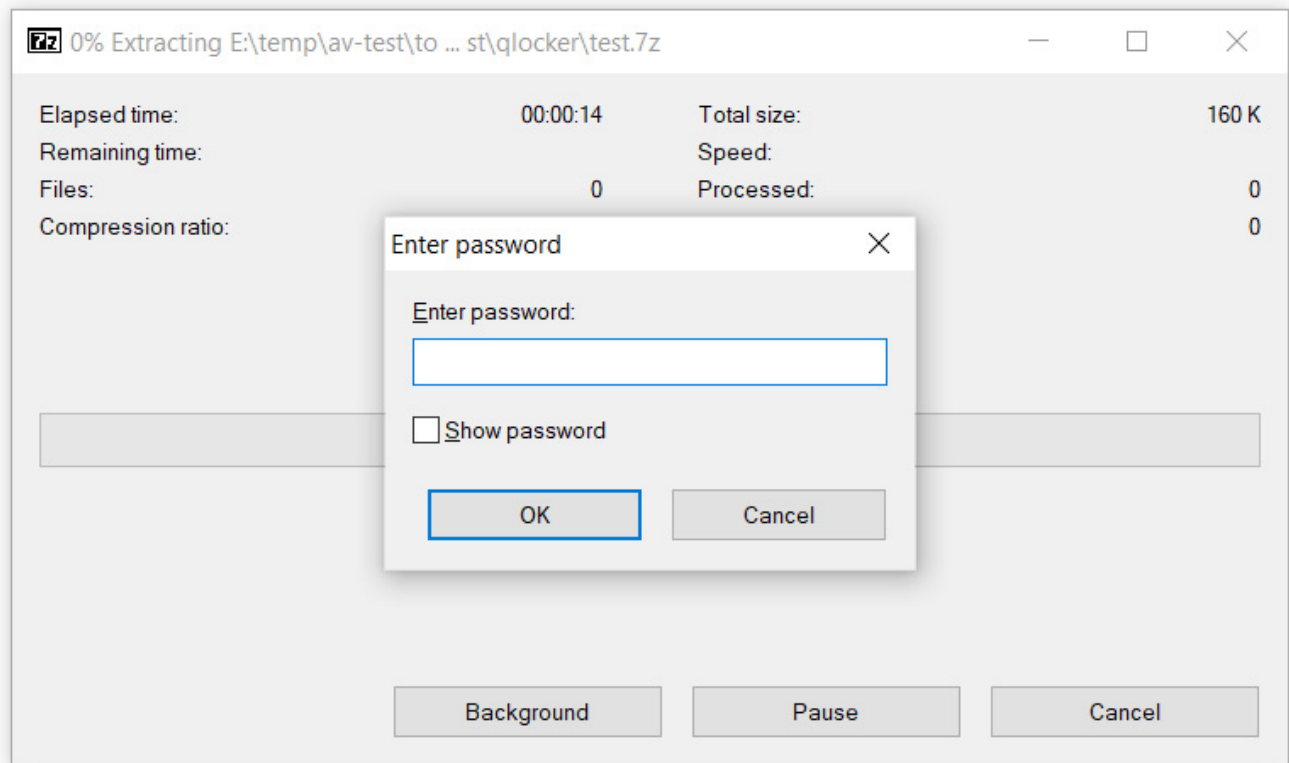
Resource Monitor

Processes Total:256 | Running:2 | Sleeping:250 | Uninterruptible:0 | Stopped:0 | Zombie:4

Process Name	User	PID
System Processes (80)	--	--
7z	admin	13243
chartReq.cgi	admin	13249
apache_proxy	admin	18383
appRequest.cgi	admin	13248
hal_daemon	admin	779
ncaas	admin	5749
gwd	admin	5911
manaRequest.cgi	admin	13193
rfsd	admin	14451
r.py	admin	17339
authn?	admin	20477

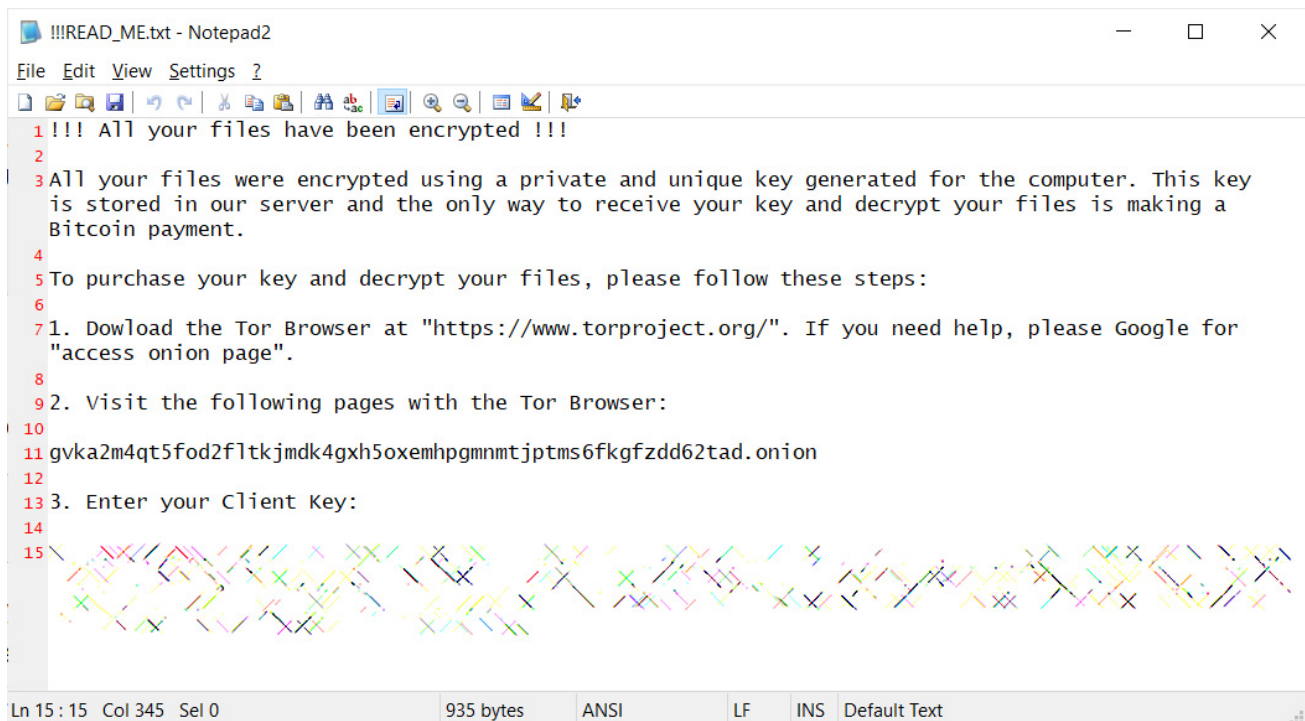
7zip seen running in the QNAP Resource Monitor

When the ransomware has finished, the QNAP device's files will be stored in password-protected 7-zip archives ending with the **.7z** extension. To extract these archives, victims will need to enter a password known only to the attacker.



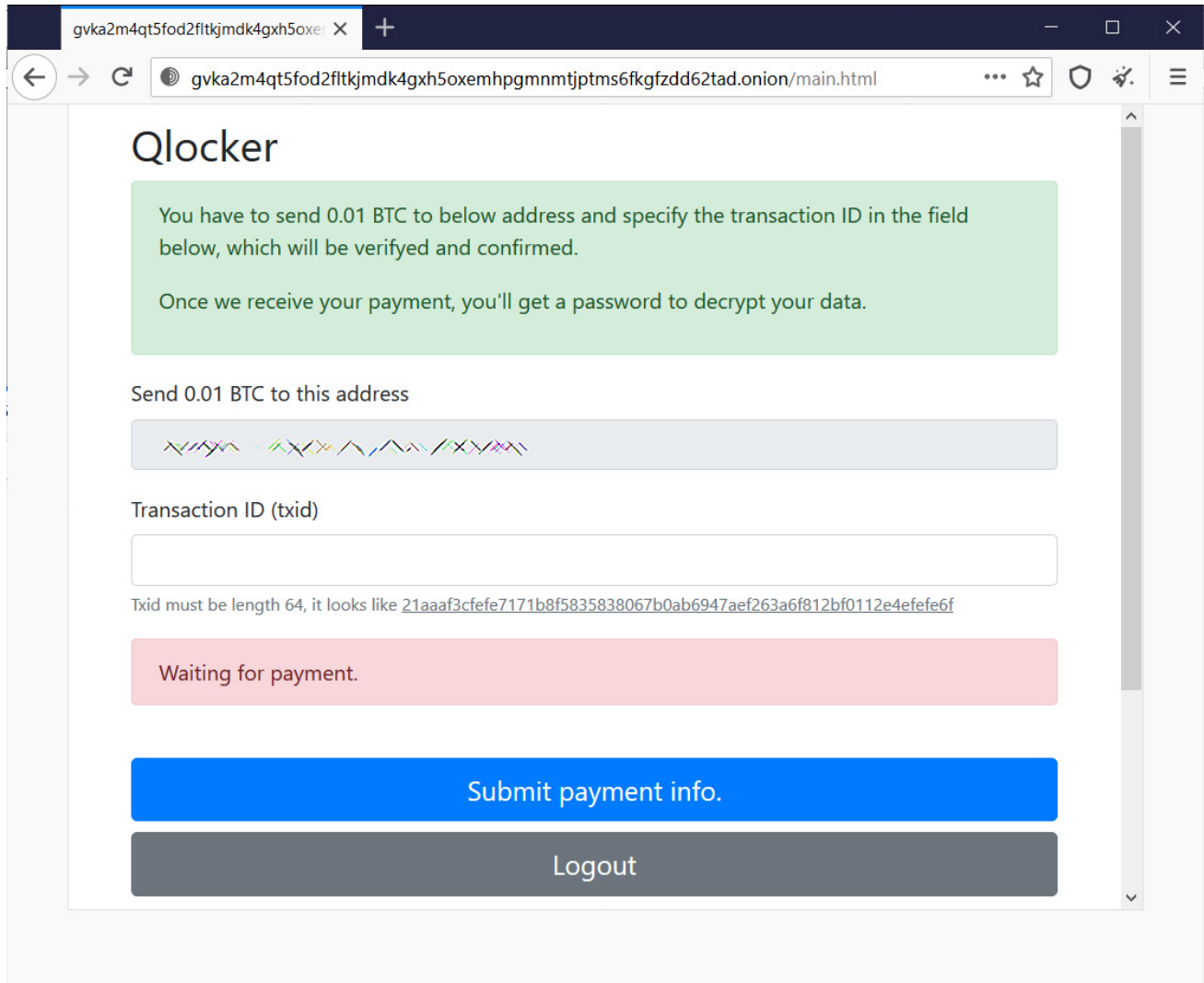
Password-protected 7zip archive

After QNAP devices are encrypted, users are left with a **!!!READ_ME.txt** ransom note that includes a unique client key that the victims need to enter to log into the ransomware's Tor payment site.



Qlocker ransom note

From the Qlocker ransom notes seen by BleepingComputer, all victims are told to pay 0.01 Bitcoins, which is approximately \$557.74, to get a password for their archived files.



Qlocker Tor payment site

After paying the ransom and entering a valid Bitcoin transaction ID, the Tor payment site will display the password for the victim's 7Zip archives, as shown below.

Qlocker

You have to send 0.01 BTC to below address and specify the transaction ID in the field below, which will be verified and confirmed.

Once we receive your payment, you'll get a password to decrypt your data.

Send 0.01 BTC to this address

Transaction ID (txid)

Txid must be length 64, it looks like `21aaaf3cfefe7171b8f5835838067b0ab6947aef263a6f812bf0112e4efefe6f`

You decrypt password is: **PL91KfUp4k5DtEWc5q6tYVB5UnZK8oX8**

Submit payment info.

The password displayed after a ransom is paid

This password is unique to the victim and cannot be used on other victims' devices.

Update 4/22/21 09:15 AM EST: Early this morning, BleepingComputer was contacted by security researcher Jack Cable about a bug he discovered in the Qlocker Tor site that allowed users to recover their 7zip passwords for free.

Using this bug, victims could take a Bitcoin transaction ID from a person who had already paid and slightly alter it. When they submitted the altered transaction ID into the Qlocker Tor site, it accepted it as payment and displayed the victim's 7zip password.

Last night, Cable had been privately helping people recover their passwords, and arrangements were being made with Emsisoft to create a help system to better exploit this weakness.

Sadly, an hour after we learned of the bug, the ransomware operators caught on and fixed it.

Update: it looks like this may have been fixed by the ransomware operators, unfortunately. I apologize if I was not able to get to yours before it was fixed. In total decrypted around 50 keys worth \$27k.

— Jack Cable (@jackhcable) April 22, 2021

At this point, there is no way to recover the files without a password, which can no longer be retrieved for free.

QNAP believes attackers are exploiting vulnerabilities

Recently QNAP resolved critical vulnerabilities that could allow a remote actor to gain full access to a device and execute ransomware.

QNAP fixed these two vulnerabilities on April 16th with the following descriptions:

More information about these vulnerabilities can be found in a [blog post](#) by the SAM Seamless Network research team, who disclosed the bugs to QNAP in October and November.

QNAP told BleepingComputer that they believe Qlocker exploits the CVE-2020-36195 vulnerability to execute the ransomware on vulnerable devices.

Due to this, it is strongly recommended to update QTS, Multimedia Console, and the Media Streaming Add-on to the latest versions.

"QNAP strongly urges that all users immediately install the latest Malware Remover version and run a malware scan on QNAP NAS. The Multimedia Console, Media Streaming Add-on, and Hybrid Backup Sync apps need to be updated to the latest available version as well to further secure QNAP NAS from ransomware attacks. QNAP is urgently working on a solution to remove malware from infected devices," QNAP stated in a [security advisory](#).

QNAP warns that if a device's files have been encrypted, they should not reboot the device and instead immediately run the malware scanner.

"If user data is encrypted or being encrypted, the NAS must not be shut down. Users should run a malware scan with the latest Malware Remover version immediately, and then contact QNAP Technical Support at <https://service.qnap.com/>," advises QNAP.

While the malware scanner and security updates will not recover your files, they will protect you from future attacks using this vulnerability.

Qlocker frequently asked questions

Trying to follow all the information in this article's comments and the Qlocker support topics can quickly become overwhelming.

To help QNAP owners and Qlocker victims, we have put together this FAQ regarding the attack using various contributions from QNAP users who have posted comments to this article and the [Qlocker help topic](#).

How are my files get encrypted?

The Qlocker threat actors exploit vulnerabilities in QNAP devices that allow them to execute commands on your NAS device remotely.

While most ransomware operations deploy specially crafted malware programs, the Qlocker attackers are simply scanning for QNAP devices and using vulnerabilities to remotely launch the built-in 7zip archive utility to password-protect files.

With this type of attack, QNAP devices are not being infected with any malware but simply being abused by vulnerabilities taking advantage of software already bundled with the operating system.

It is unclear what vulnerabilities are being used, but it is believed to be one of the following, which QNAP fixed this month.

QNAP has told BleepingComputer that they believe it is the CVE-2020-36195 vulnerability that is being exploited.

Updates for all of these vulnerabilities were released earlier this month and should be installed immediately.

My files are being encrypted! What should I do?

If you see that your QNAP files are actively being encrypted, you should immediately disable myQNAPcloud and change the default web admin port from port 8080 to another port number.

These changes will effectively prevent the threat actors from issuing further 7zip commands to password-protect your files.

Now that the threat actors can no longer access your device remotely, you should terminate any active '7z' processes that may be running to stop any current encryption commands.

You can do this by logging into your QNAP device via SSH or Telnet using the [following guide](#).

Then issue the following command at the console to terminate all 7z processes.

```
kill -9 `ps |grep sbin/7z|grep -v grep|awk '{ print $1 }'`
```

Is there a way to get our passwords for free?

Tuesday night, security researcher Jack Cable discovered a method that tricked the ransomware payment site into thinking a payment was made and to display the victim's passwords.

Unfortunately, this bug was short-lived, and the bug no longer works.

For users who have not restarted their QNAP device since being encrypted, it may be possible to recover your password from the '7z.log' file using a command [offered by a victim](#).

The following command must be entered from the QNAP console when you are connected via SSH or Telnet.

```
cd /usr/local/sbin; printf '#!/bin/sh \necho $@\necho $@>>/mnt/HDA_ROOT/7z.log\nsleep 60000' > 7z.sh; chmod +x 7z.sh; mv 7z 7z.bak; mv 7z.sh 7z;
```

Once you execute the following command, you can look in the /mnt/HDA_ROOT/7z.log for a 7z command-line showing your password, as shown in the example below.

```
a -mx = 0 -sdel -pmFyBIvp55M46kSxxxxxYv4EIhx7r1TD [FOLDER PATH]
```

In the above case, the password is 'mFyBIvp55M46kSxxxxxYv4EIhx7r1TD.'

A [YouTube video](#) has been created to demonstrate how to perform this task.

If you have run QNAP's Malware Remover tool, the program will have moved the 7z.log to '[/share/CACHEDEV1_DATA/.qpkg/MalwareRemover/7z.log](#)'.

QNAP is [emailing customers instructions](#) with more information on possibly recovering a password from the 7z.log file.

Unfortunately, if you have previously restarted your device, the log file contents will be wiped.

In some cases, even if you have not restarted your device, the log file may be empty.

What has QNAP's response been?

In a [security advisory](#) released Tuesday, QNAP advises users not to restart their QNAP devices and to run the latest version of the Malware Remover to help protect against Qlocker.

When executed, Malware Remover will perform the following tasks:

- Rename /usr/local/sbin/7z to 7z.orig
- Replace /usr/local/sbin/7z to 7z.orig with [this script](#).
- The script will copy various data to the current 7z.log file and then copy that file to '[/share/CACHEDEV1_DATA/.qpkg/MalwareRemover/7z.log](#)'.
- Look for and quarantine the **/tmp/qnap/r.py** and **/tmp/qnap/re.sh** scripts to the /tmp/qnap folder. If you have these scripts, we would love to see them, and you can [submit them here](#).

In addition to running Malware Remover, QNAP is advising users to immediately update to the latest versions of **Multimedia Console**, **Media Streaming Add-on**, and **Hybrid Backup Sync** through the App Center.

After installing the latest updates, QNAP advises customers to review their guide on [best practices to enhance NAS security](#).

How to decrypt multiple files at once

If you found your passwords or paid the ransom, you can use the following command (thanks [ss1973](#)) to decrypt all of your files at once from within Windows.

```
SET source=C:\Users\thomb158\Downloads\5thKind\7z
FOR /F "TOKENS=*" %%F IN ('DIR /S /B "%source%\*.7z"') DO "C:\Program Files\7-
Zip\7z.exe" x -pPASSWORD "%~fF" -o"%~pF\"
EXIT
```

In the above command, ' `SET source=` ' is the path to your encrypted files, and `-p` is the password. You will also need to have installed the [7zip program](#).

If anyone has a command to perform these steps directly through the QNAP console, please [let me know](#).

Update 4/24/21: Added a frequently asked questions section.

Qlocker IOCs:

Associated Files:

```
!!!READ_ME.txt
```

Ransom note text:

```
!!! All your files have been encrypted !!!
```

```
All your files were encrypted using a private and unique key generated for the
computer. This key is stored in our server and the only way to receive your key and
decrypt your files is making a Bitcoin payment.
```

To purchase your key and decrypt your files, please follow these steps:

1. Download the Tor Browser at "<https://www.torproject.org/>". If you need help, please Google for "access onion page".

2. Visit the following pages with the Tor Browser:

```
gvka2m4qt5fod2f1tkjmdk4gxh5oxemhpgmnmjtptms6fkgfzdd62tad.onion
```

3. Enter your Client Key:

```
[client_key]
```

Related Articles:

[QNAP alerts NAS customers of new DeadBolt ransomware attacks](#)

[QNAP warns of ransomware targeting Internet-exposed NAS devices](#)

[QNAP urges customers to disable UPnP port forwarding on routers](#)

[QNAP warns severe OpenSSL bug affects most of its NAS devices](#)

[Windows 11 KB5014019 breaks Trend Micro ransomware protection](#)

- [7-Zip](#)
- [7zip](#)
- [Archive](#)
- [NAS](#)
- [QLocker](#)
- [QNAP](#)
- [Ransomware](#)

[Lawrence Abrams](#)

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- [Previous Article](#)
- [Next Article](#)

Comments



• [Charlie50mm](#) - 1 year ago

-
-

Hello, Sadly my qnap has been touch by this one... I'm able to go in the ssh console but I don't know how search the password of 7z file. Could you help me for this task please ?



Lawrence Abrams - 1 year ago

-
-

In the console type `ps -ef` and press enter.

Look for a `7z` command and if there is a readable password after the `-p` argument..



Charlie50mm - 1 year ago

-
-

I didn't find the command, but my NAS restart since the ransomware, so did I lost the previous command line ?



-

aston729 - 1 year ago

-
-

You have to exit the QNAP command line by typing "0"



-

mirror79 - 1 year ago

-
-

not by O but by Q!



-

aston729 - 1 year ago

-
-

Same problem here. I can log into the SSH but after typing ps -ef nothing happens



• Lawrence Abrams - 1 year ago

-
-

No output when you type the following command and press enter?

ps -ef



• aston729 - 1 year ago

-
-

Yes I already exit the Command to standard ssh comandline.

I typed ps -ef

and lookinf for 7z proccess, but it is something like this:

```
"/usr/local/sbin/7z a -mx=0 -sdel -p***** "
```



Lawrence Abrams - 1 year ago

-
-

OK then this method will not work unfortunately



Marchande - 1 year ago

-
-

please tel me that al those stars are NOT a 32 character pasword



sieci - 1 year ago

-
-

and like this: 20402 admin 4368 R /usr/local/sbin/7z a -mx=0 -sdel -
p***** /share/CACHEDEV1



• Marchande - 1 year ago

-
-

seems that I got nailed by this as well.. came here to monitor and see if there is ever a fix for it... sadly my nas rebooted and updated before the encryption was completed... thank the gods but there are still aLOT of files that did get hit... need to find a way to decrypt every thing... posting here in hopes that some one learns something new and has some ideas.



• ValiantThor - 1 year ago

-
-

Try this command:

```
cd /usr/local/sbin; printf '#!/bin/sh \necho $@\necho $@>>/mnt/HDA_ROOT/7z.log\nsleep 60000' > 7z.sh; chmod +x 7z.sh; mv 7z 7z.bak; mv 7z.sh 7z;
```

the encryption key would be stored in /mnt/HDA_ROOT/7z.log which you can then use to decrypt



Lawrence Abrams - 1 year ago

-
-

Be terrific if this works.



Twitterhd - 1 year ago

-
-

I just tried this option through a SSH connection, however, when trying to access the /mnt/HDA_ROOT/7z.log it tells me "permission denied". Is there another way to gain access?



• Darevx - 1 year ago

-
-

Yes, i used MobaXterm to access /mnt/HDA_ROOT/ and download 7z.log, i managed to recover password from that file. Just remember not to use the first p from that word.



• AirNelly - 1 year ago

-
-

"Yes, i used MobaXterm to access /mnt/HDA_ROOT/ and download 7z.log, i managed to recover password from that file. Just remember not to use the first p from that word."

What is MobaXterm? Could you please provide some step by step instructions?
Thank you



• Marchande - 1 year ago

-
-

nothing showing in the HDA_ROOT folder labled anything .log



• LaurentH111 - 1 year ago

-
-

Not working ;-(



• Darevx - 1 year ago

-
-

Great job, I managed to recover the password for 3 devices in this way, but I had to download 7z.log locally to be able to open it, when I tried from the command line I received a permissions error.



• skiele - 1 year ago

-
-

There's no 7z.log in that folder unfortunately for me



• [micattack](#) - 1 year ago

-
-

What can I do when I already killed the encryption process. Will it come back after a reboot with the same password?

Currently I am leaving the qnap running and whatever the encryption was has not come back (stopped processes, disconnected from Internet, etc)



• [mirror79](#) - 1 year ago

-
-

THANK YOU!!! You saved me from many hours of restoring backups!!! It worked! To everybody: you must run the command from ValiantThor above, after this the 7z.log file will reveal, download it to your local PC and open it. You will find the password inside.



• [workfor747](#) - 1 year ago

-
-

Can you just guide me how you write the code step by step <

what You did After open ssh



• [Boonpot](#) - 1 year ago

-
-

Hi

Do I have to wait sleep 60000 finish ?



• [NewDayMedia](#) - 1 year ago

-
-

Sorry for my ignorance. when I try this command I get a series of permission errors:

```
-sh: 7z.sh: Permission denied
chmod: 7z.sh: No such file or directory
mv: can't rename "7z": Permission denied
mv: overwrite "7z"?
```

I am logged in with an administrator account. Am I doing something wrong?

Thanks.



• [keg415](#) - 1 year ago

-
-

It appears that as of 2021-04-11, Malware Remover now renames `/usr/local/sbin/7z` to `7z.orig` and replaces `7z` with a wrapper script that captures and logs info about the command and parent process. And if a password option is present, it delays for a few seconds before running `7z.orig`. So if you've replaced `7z` with the little `HDA_ROOT/7z.log` script, Malware Remover may have renamed it instead of the real `7z` and be calling it instead.

Note that on my QNAP TS-253D the log file is:

`/share/CACHEDEV1_DATA/.qpkg/MalwareRemover/7z.log`



Lawrence Abrams - 1 year ago

-
-

Keg, would you be able to send me the original `/usr/local/sbin/7z.orig` and the new helper script `/usr/local/sbin/7z`?

Would like to take a look and update the article with info.

Also, is this file readily accessible by anyone after they run the Malware Remover:

`/share/CACHEDEV1_DATA/.qpkg/MalwareRemover/7z.log`

Can users simply run the new version and open this file to get their password?

If you can PM so you can send me the files, it would be appreciated. I can be PMed at this URL:

<https://www.bleepingcomputer.com/forums/index.php?app=members&module=messaging§ion=send&do=form&fromMemberID=3>



• Pim65 - 1 year ago

-
-

Hi,

I have this problem to, but before I new. Did the update and restart 2 days ago. Now 80GB is encrypted I found this morning. I Have in user/local/sbin 7z.orig and 7z.so but cant decrypt them. Did someone found a solution to retrieve the password in this matter?



• n3xo - 1 year ago

-
-

Just logged to say thank you ValiantThor!



• Melissa81 - 1 year ago

-
-

n3x0 - hi! So you have just done this? Had you rebooted your QNAP prior?



n3xo - 1 year ago

- o
- o

no i didnt reboot buy the told me It rebooted itself After firmware update



keg415 - 1 year ago

- o
- o

"It appears that as of 2021-04-11, Malware Remover now renames `/usr/local/sbin/7z` to `7z.orig` and replaces `7z` with a wrapper script that captures and logs info about the command and parent process. And if a password option is present, it delays for a few seconds before running `7z.orig`. So if you've replaced `7z` with the little `HDA_ROOT/7z.log` script, Malware Remover may have renamed it instead of the real `7z` and be calling it instead.

Note that on my QNAP TS-253D the log file is:


```
/share/CACHEDEV1_DATA/.qpkg/MalwareRemover/7z.log"
```

I've not tested this, but rebooting the QNAP should restore the original `/usr/local/sbin/7z` executable, which Malware Remover will then rename to `7z.orig` and install the `7z` wrapper script.

The command:

```
more "`getcfg MalwareRemover Install_Path -f /etc/config/qpkg.conf`/7z.log"
```

will show the wrapper script log, and (hopefully) the encryption key.

-  nshimin Photo
[nshimin](#) - 1 year ago

-
-

"It appears that as of 2021-04-11, Malware Remover now renames /usr/local/sbin/7z to 7z.orig and replaces 7z with a wrapper script that captures and logs info about the command and parent process. And if a password option is present, it delays for a few seconds before running 7z.orig. So if you've replaced 7z with the little HDA_ROOT/7z.log script, Malware Remover may have renamed it instead of the real 7z and be calling it instead.

Note that on my QNAP TS-253D the log file is:

`/share/CACHEDEV1_DATA/.qpkg/MalwareRemover/7z.log`"

I have actually followed these and actually found more 7z files located here.

`usr\local\sbin`

The 7z files are:

7z.so

7z.orig

7z.bak

7z

Unfortunately, no 7z.log files are shown. Is there someone who might know how to get a .log file based on the 4 files I've found? Or perhaps something I should do to these 4 files.



Tweeterhd - 1 year ago

-
-

I would like to thank ValientThor for a quick and helpful response in creating the 7z.log and everyone else in this comment thread who worked to help us try to overcome this issue. Thanks to the advice given here, commands to try, and shared youtube video links I have seen several people who have been able to retrieve their passwords and begin work on extracting their files. You have provided a great service to combat what feels like terrorism. For those of you who haven't been able to retrieve your files yet, hopefully as things progress you will have your opportunity. By the way, has anyone seen files like these 3 on their NAS? ".wfm_upload_7htO7Z" ; ".wfm_upload_dSrQl1" ; ".wfm_upload_ez5d8Z". I stumbled across these suspicious looking files while looking through the slew of my encrypted files and wondered if this has anything to do with the 7z ransomware (be gentle, a lot of this is new to me).



Tweeterhd - 1 year ago

-
-

[duplicate]



• [Splay](#) - 1 year ago

-
-

Another victim here. It got pretty much all of the small files on my business's NAS. I'm not a programmer so if someone does find a fix or potential solution to decrypt the files, please post in layman terms. I'm not totally unfamiliar with using command lines in Windows, but I'm not as proficient on the QNAP system. Thanks in advance for anyone looking into this.



• [LaurentH111](#) - 1 year ago

-
-

Hi. I've got 2 devices impacted among 20 and i've found a piece of sh... in /root
-rwxr-xr-x 1 admin administrators 242 2021-04-21 13:35 re.sh*

I think that's the part deleting snapshots :

more re.sh

#!/bin/sh

```
export PATH="/bin:/sbin:/usr/bin:/usr/sbin:/usr/bin/X11:/usr/local/sbin:/usr/local/bin"
```

```
df | grep mapper | grep snap | while read line; do umount $line; done
```

```
find /dev/vg* -name snap* | while read line; do lvremove -f $line; done
```

Found only on those 2 infected Qnaps



• Marchande - 1 year ago

-
-

where are you finding this at. looking in root on mine not seeing any .sh file. possible it was removed when I did the firmware update?



• LaurentH111 - 1 year ago

-
-

found at /root. Not yet upgraded. Will do and report if still present



• Marchande - 1 year ago

-
-

thanks... my last backup failed I have a qddf file to read from but its sadly corrupted and unreadable by the q dedupe software that qnap provides.. both on the server and off. so im looking for any sliver lining that I might be able to latch on to.



Razorblade - 1 year ago

-
-

There's another suspicious file:
./mnt/ext/opt/apps/backup.php



Lawrence Abrams - 1 year ago

-
-

Can you send me the backup.php so I can take a look and possibly update the article?

You can submit it here:

<https://www.bleepingcomputer.com/submit-malware.php?channel=3>

Thanks



• Razorblade - 1 year ago

-
-

I deleted it, but it had just one line with "php eval POST cmd" (with the missing characters). Funny because Microsoft Defender detects that file as Backdoor:PHP/Remoteshell.B, but the QNAP Malware Remover does not detect it.



• MeanE - 1 year ago

-
-

Ooof. People let their QNAP be internet facing?



• ttanxu - 1 year ago

-
-

It's UPnP that exposes QNAP. UPnP is usually by default on routers. It's necessary to discover devices in the same network (e.g. printer & myQNAPCloud), but it opens up a lot of attacking surfaces for exploitation.

The truth is your home network is a lot more open to the Internet as you might have imagined. It's especially the case if your ISP and your router have IPv6 support (and they should).



• LaurentH111 - 1 year ago

-
-

After upgrade/reboot it's gone. Hope it's not coming back !



• cricker - 1 year ago

-
-

ps -ef revealed; 3504 admin 2564 S /bin/sh /usr/local/sbin/7z x -so ./data.tar.xz

I found the log via SSH in the folder /mnt/HDA_ROOT/7z.log

I moved it to another location and opened to reveal these contents, the same as above, "x -so ./data.tar.xz"



• aston729 - 1 year ago

-
-

so there is no possibility to decrypt the log file?



•
ss1973 - 1 year ago

-
-

has anyone had any luck decrypting their data. Or worse case has any one paid the ransom successfully?



•
Marchande - 1 year ago

-
-

I imagine its going to be a little more difficult, since its using 7zip for the encryption, and its appearing to be a 32 character password wich means that brute forcing it using any of the avalable tools out will be a little challenging... ive been searching all evening for something Im holding out hope that those that are far more versed in this than I am are able to find a solution....



Lawrence Abrams - 1 year ago

-
-

See update at top of article.



ttanxu - 1 year ago

-
-

I seriously doubt CVE-2020-36195 is the vulnerability the attacker used. I am a victim of this attack (with 7z files created at 4/21 1AM PDT), while the QuLog center on my affected device showed it installed Multimedia Console 1.3.4 on 3/2, Media Streaming Addon 500.0.0.1 on 3/2 and updated its firmware to 4.5.2.1630 Build 20210406 on 4/8. They all are above the patched version QNAP announced and yet the incident still happened.

I don't think it was affected even on 4/19, so it can't be the attacker who changed the modified date of those 7z files. I don't think attackers were interested in changing the software update log either.



• [Veyabilc11](#) - 1 year ago

-
-

May i know how the Qlocker got in?



• [micattack](#) - 1 year ago

-
-

I am also wondering how it came in. Just 2 days ago I checked and firmware was current. I have the suspicion that it came in through Adguard Home (docker - container station) but cannot prove it. Stopped some scripts with "mana..." in the name with "kill -9"

It got 2787 files on my qnap :-)

check via ssh with "find /share -type f -name "*.7z"|wc -l"

to see the affected directories that have encrypted files do "find /share -type f -name '*.7z' | sed -r 's|/[^\|]+\$||' |sort |uniq"

so: what do we know of the attack vector and where the scripts are hiding?



• [Veyabilc11](#) - 1 year ago

-
-

How do we know that it's there already and running? Is it the 7z that shows in the Resource Monitor?



• [micattack](#) - 1 year ago

-
-

i used "top" and saw some fishy looking things - as explained with "mana" in the name and I just killed those in my panic (kill -9 <process-id-number>)

There might be a 7z task running as well but I didnt see that and dont remember. For now I stopped everything in the web front-end via app-center that might be running and am working on the ssh console to debug

UPDATE: What I did probably had no effect at all. It looks like the encryption stopped on its own at about 4:33 am CET (6-7 hours ago) so that is also why I didnt see a 7z process running



• krysc4d - 1 year ago

-
-

Hi Guys. I am a victim as well. I am completely newbie in terms of NAS. Can someone advice me what to do now? How to get rid of this ransomware? I've turned the QNAP off at this moment...



• stook_84 - 1 year ago

-
-

i'm in via ssh, but the 7z.log is empty :(

<https://ibb.co/KFV8n7c>



• Darevx - 1 year ago

-
-

Run the following command: `cd /usr/local/sbin; printf '#!/bin/sh \necho $@\necho $@>>/mnt/HDA_ROOT/7z.log\nsleep 60000' > 7z.sh; chmod +x 7z.sh; mv 7z 7z.bak; mv 7z.sh 7z;`

After that, right click on 7z.log - select download and save the file on your computer. Now you can open the file from your computer. Use the password without first "p".



• matteocalle - 1 year ago

-
-

Hi Darevx,

I tried with the command you suggested, but in the folder where I should find the log, I find nothing. My client turned off QNAP after being attacked. Could this be the cause of the missing log? Can the decryption password possibly be traced in some other way?

Thanks in advance.

Matteo



• cnwong - 1 year ago

-
-

Hello Darevx,

I managed to find the file and I downloaded it on my computer. But when I opened it the file is completely blank - no letters or words at all. Any advice? Thanks very much.



• Boonpot - 1 year ago

-
-

Hi

I got the same problem ., there is nothing on 7z.log
Pelse help



• Melissa81 - 1 year ago

-
-

this command is not showing as available in the run program. any other ideas



• [Koluschki](#) - 1 year ago

-
-

Hello Darvex,

i tried your command

```
cd /usr/local/sbin; printf '#!/bin/sh \necho $@\necho
```

```
$@>>/mnt/HDA_ROOT/7z.log\nsleep 60000' > 7z.sh; chmod +x 7z.sh; mv 7z 7z.bak;  
mv 7z.sh 7z;
```

but the 7z.log file not exists. i hope you can help me. The QNAP is since 24 days on



• [icetealight](#) - 1 year ago

-
-

I just registered to thank @Lawrence Abrams for all the work he is doing ... what a hero.

I leave my QNAP turned off and untouched until later today when the update comes out from Bleepingcomputer.

Since it is personal file storage - I dont REALLY need the files and as soon as there is hope that the files can be recovered - I am patient.



Lawrence Abrams - 1 year ago

-
-

Thank you :) Just wish we could have utilized that bug longer and recovered all of your keys.



perarg - 1 year ago

-
-

I have a NAS-473 and i am a victim of Qlocker too. I have two volumes in a storage pool. Only the one volume's files have been encrypted.

I tried the command

```
cd /usr/local/sbin; printf '#!/bin/sh \necho $@\necho $@>>/mnt/HDA_ROOT/7z.log\nsleep 60000' > 7z.sh; chmod +x 7z.sh; mv 7z 7z.bak; mv 7z.sh 7z;
```

But there is no file 7z.log at all at /mnt/HDA_ROOT. This may happens because of the two volumes?



thetaga - 1 year ago

- o
- o

i am a victim of Qlocker too.

I tried `cd /usr/local/sbin; printf '#!/bin/sh \necho $@\necho`

`$@>>/mnt/HDA_ROOT/7z.log\nsleep 60000' > 7z.sh; chmod +x 7z.sh; mv 7z 7z.bak;`
`mv 7z.sh 7z;`

But it comes back to me like this:

```
[bobisnotadmin@NAS3D733E sbin]$ cd /usr/local/sbin; printf '#!/bin/sh \necho
```

```
$@\necho $@>>/mnt/HDA_ROOT/7z.log\nsleep 60000' > 7z.sh; chmod +x 7z.sh; mv
```

```
7z 7z.bak; mv 7z.sh 7z;
```

```
-sh: 7z.sh: Permission denied
```

```
chmod: 7z.sh: No such file or directory
```

```
mv: unable to rename `7z': Permission denied
```

```
mv: overwrite `7z'? y
```

```
mv: unable to rename `7z.sh': No such file or directory
```

I am using a different user than admin, since I have disable to avoid other attacks for the time being. What should I do?



Alexspiteri - 1 year ago

- o
- o

I also have been hit with this attack and have all files encrypted.

Any possible way of a workaround for laypersons and Mac users.

thank you in advance



• [Miniman01](#) - 1 year ago

-
-

I have followed the same command and cannot locate the file.

```
cd /usr/local/sbin; printf '#!/bin/sh \necho $@\necho $@>>/mnt/HDA_ROOT/7z.log\nsleep 60000' > 7z.sh; chmod +x 7z.sh; mv 7z 7z.bak; mv 7z.sh 7z;
```

7z.log

I have 3 QNAPS with same issue. All have been shutdown and rebooted to access ssh. Any help please; Also contacted QNAP Support as to why and if there is going to be a new update firmware security for QLOCKER.



• [janwozniak](#) - 1 year ago

-
-

It looks strange for me, I have two QNAPs at home, one encrypted, the other not, for clients from 10, some encrypted part not.

Interestingly - packed files are without a password. At the moment, I have turned off all that I had access to and I am waiting for information on what to do next.

Two-step verification doesn't matter how I've seen.



• Miniman01 - 1 year ago

-
-

There are 2 on our network, 1 encrypted and 1 not. strange to see how this has been targeted. Waiting for remote support by QNAP.



• MartinMe - 1 year ago

-
-

Hello all, I've tried your steps. I've used command: `cd /usr/local/sbin; printf '#!/bin/sh\nnecho $@\nnecho $@>>/mnt/HDA_ROOT/7z.log\nsleep 60000' > 7z.sh; chmod +x 7z.sh; mv 7z 7z.bak; mv 7z.sh 7z;`

looks it go through smoothly but I cannot find any log file in /mnt/HDA_ROOT/ folder. Is there a way to find and open those files manually let say with WinSCP or so?

I've also tried to use `ps -ef` command. But I cannot see there any line with 7z.

Thanks for your help guys.



• perarg - 1 year ago

-
-

Same thing here. No 7z.log file there.



• mirror79 - 1 year ago

-
-

Do it like this: https://youtu.be/aq_cldY_ksQ



• ss1973 - 1 year ago

-
-

Has any one paid the ransom and regained access to their files successfully?



• [PhR34k](#) - 1 year ago

-
-

"Has any one paid the ransom and regained access to their files successfully?"

I saw someone on Reddit or Qnapforum that had paid and succesfully managed to unlock the files. Its a headache thou to open all the files. I dont know how to manage that but there are tools for it I hope.



• [PhR34k](#) - 1 year ago

-
-

"Has any one paid the ransom and regained access to their files successfully?"

I saw someone on Reddit or Qnapforum that had paid and succesfully managed to unlock the files. Its a headache thou to open all the files. I dont know how to manage that but there are tools for it I hope.



• [scrumpers](#) - 1 year ago

-
-

We paid the ransom got the password and then used peazip to unlock all the files to their current places and its working



• lamAdverb - 1 year ago

-
-

Would you mind sharing you peazip command line? I would appreciate it.

TIA

Adverb



• Tony-OZ - 1 year ago

-
-

Hallow - Another victim here from Down-under (Sydney)

My office QNAP got hit badly with this rotten Qlocker - it is world wide alright.

Lawrence, you are the only source of information on this to date, I cant thank you enough for your prompt and clever presentation. You described the problem exactly. I got all my files locked up and I had to shutdown my entire practice today.

Qnap here in Melbourne must have gone in a meltdown, I phoned them at 9am Sydney time and it is past 10:30PM and have not heard from them yet.

I got image files, DBF files, RTF files, excel files all locked for a ransom.

I will be waiting in anticipation for the news and updates

Thanks Lawrence



r2d2c3po - 1 year ago

-
-

I see on the top!

Update 4/22/21 12:44 AM: A weakness may have been found that could potentially allow victims to recover their files for free. We are still investigating this and will post an update around 10 AM EST, or possibly earlier..

Give's new informations?



klaun1979 - 1 year ago

-
-

hello a question to all users who are affected of this attack:
is open to the qnap http or https port?



wydo91 - 1 year ago

-
-

http set on 8080 but not NAT on Router.
Https forced.
Https open with NAT.



• [wydo91](#) - 1 year ago

-
-

Hi,

One more, near Paris, France.

Try to figure out with 7z.log but there is not such file.

Maybe file was deleted after finishing encryption.

Still waiting for another potentially recover method.



• [PhR34k](#) - 1 year ago

-
-

About the 7z.log file.

What i have gatherd from reddit and qnap forum is that the encrpytion needs to still be active to see this file.

Like for me the encryption is done so i cant find these file.

Lets hope Lawrence has some good news for us.



• [perarg](#) - 1 year ago

-
-

It seems that if someone made a reboot to the system, the option to get the 7z.log file has been lost. I made the same "mistake", i run a firmware update and then reboot the machine so now the 7z.log is not present in the system



• [PhR34k](#) - 1 year ago

-
-

"It seems that if someone made a reboot to the system, the option to get the 7z.log file has been lost. I made the same "mistake", i run a firmware update and then reboot the machine so now the 7z.log is not present in the system"

I have not made a reboot on the system and still can not see the file. I think its a matter wether the encrpytion is done or not.



• salvo981 - 1 year ago

-
-

hi, I also have the usual problem the only thing is that if I give the command:
`cd /usr/local/sbin; printf '#!/bin/sh \necho $@\necho $@>>/mnt/HDA_ROOT/7z.log\nsleep 60000' > 7z.sh; chmod +x 7z.sh; mv 7z 7z.bak; mv 7z.sh 7z;`
it returns me the error : no such file or directory
the file 7z.log it's no present
Tank you



• AirNelly - 1 year ago

-
-

This has happened to me too here in North Carolina. I'm fairly new to network storage and QNAP and use this for my video editing and have a lot of important video footage that is now encrypted. I'm using an iMac and have tried using the command suggested in terminal but get "no such file". My QNAP requested an update last night which I performed. Any help would be tremendously appreciated. Did not know things like this could happen



[vincentw2622](#) - 1 year ago

-
-

it's 9:33 am est now, i stayed up all night and hitting my f5 over 10k times and it's almost broken but the solution hasn't been shared yet



[TacticalLynx](#) - 1 year ago

-
-

Lost all my stuff. I panicked because this is my work NAS and reset everything. I couldn't let a ransomware get to my work computer and mess up that server as well. Sucks.. I had sooo much stuff on this NAS for work.



[Boydy81](#) - 1 year ago

-
-

Yep I have also been hit by the qlocker on my qnap here in Melbourne Aus anxiously waiting a fix as mine is off now !



PhR34k - 1 year ago

-
-

Jack Cable was able to pass thru the ransomware but seems that these has been stoped by the Qlocker team.

I hope this is not the "fix" Lawrence was hoping/talking about... :(

<https://twitter.com/jackhcable/status/1385064776435310593>



Lawrence Abrams - 1 year ago

-
-

It was unfortunately :(



• Jimac1888 - 1 year ago

-
-

Tried the 7z.log which probably would have worked great had i not rebooted and stopped the service in a panic before hand.

Thankfully it was only small files that i have lost but all my kids school work is now gone,

If anyone has paid to get the key could you post what it consists of for example

32 characters upper and lowercase with numbers and or symbols, i ask as i would like to try some brute force attacks to decrypt and if everyone's keys are similar format it would give a good start point.

Can't believe QNAP has let this happen, disgusted to read about all the work places affected by this, cyber terrorism.



•
[wtutwiler70](#) - 1 year ago

-
-

I too am a victim, one of my two QNAP NAS was hit. I just read the recent update (which is disappointing), and I also shut down both units, so using the mentioned commands to find the password is unlikely an option for me either, when I do turn them back on.

I had just done the firmware update a couple of days ago, but unfortunately, at the time, I did not check the QNAP admin page for potential software updates.

The majority of the files on my QNAP were backups, so it will be possible to rebuild it, if necessary (which it is sounding more and more likely), but it will take DAYS and I will still have lost a good portion of data.

I don't use ANY of the multimedia apps on the QNAP, would uninstalling/disabling them all help prevent this?



•
[wtutwiler70](#) - 1 year ago

-
-

Ironically, when looking on the QNAP website for information on this, and possible preventative measures, I only find articles about using the NAS to safeguard from ransomware, and nothing (recent) about if the NAS itself was the target.



• janwozniak - 1 year ago

-
-

<https://www.qnap.com/en/news/2021/response-to-qlocker-ransomware-attacks-take-actions-to-secure-qnap-nas?ref=jorma> official



• wtutwiler70 - 1 year ago

-
-

Ah, thanks, I had only found the article from 2019 before.



• krysc4d - 1 year ago

-
-

Funny enough, I've run this scan on mine and this didn't find any ransomware in data log...



• salvo981 - 1 year ago

◦

◦

file 7z.log no present



• marco1982 - 1 year ago

◦

◦

My qnap is inaccessible from both ssh and https after reboot. Is there any way to get it back?

•  SARASA Photo

SARASA - 1 year ago

◦

◦

Hello, I got caught in ransomware in Korea.

I came here looking for a solution.

It's too difficult.



• AirNelly - 1 year ago

-
-

Guess I'm going to have to pay this ransom, plan on selling my QNAP after I get all my 60TB of data off of it. No more network storage for me.



• SARASA Photo
SARASA - 1 year ago

-
-

I thought it would be safe, but I feel betrayed.



• z4kir0v - 1 year ago

-
-

So this problem was known to QNAP for at least 4 month. And it's been 2 weeks since publication with enough details to re-implement the attack.

And only 3 days since an update with mentioned NO information about security problems it's closing.

<https://securingsam.com/new-vulnerabilities-allow-complete-takeover/>



oblong - 1 year ago

-
-

That explains a lot. Thanks for sharing



mirror79 - 1 year ago

-
-

Hi everybody, I made a video how to do it. Hope it helps. This is how I found the password for all my 7z files created using this ransomware:

https://youtu.be/aq_cldY_ksQ



aston729 - 1 year ago

-
-

Do you have any idea when the file 7z.log is empty?



• [vincentw2622](#) - 1 year ago

-
-

You mean there's nothing in the log file?



• [aston729](#) - 1 year ago

-
-

"You mean there's nothing in the log file?"

Yes exaclly



• [vincentw2622](#) - 1 year ago

-
-

Did you reboot your nas?



• aston729 - 1 year ago

-
-

"Did you reboot your nas? "

I shut it down during encrypting and it started on its own today morning. I didn't notice that... Probably the encryption has been finished



• aston729 - 1 year ago

-
-

Do you have any idea when the file 7z.log is empty?



• MartinMe - 1 year ago

-
-

Hi, I've did the same what you and still cannot see that log file. Do you think that it may be as hidden file? I am using WinSCP.



• Jimac1888 - 1 year ago

-
-

I see you still have the attack going on with the failed log ins, i tried unzipping a file in file station, now my log has only that info so if you have restarted or updated you might be out of luck like me, i have re connected to the internet and added some new files hopefully to receive another attack



• aston729 - 1 year ago

-
-

"I see you still have the attack going on with the failed log ins, i tried unzipping a file in file station, now my log has only that info so if you have restarted or updated you might be out of luck like me, i have re connected to the internet and added some new files hopefully to receive another attack"

I don't know if it's working like this :/



• Jimac1888 - 1 year ago

-
-

""I see you still have the attack going on with the failed log ins, i tried unzipping a file in file station, now my log has only that info so if you have restarted or updated you might be out of luck like me, i have re connected to the internet and added some new files hopefully to receive another attack"

I don't know if it's working like this :/"

You could be right sadly, i have the failed log in messages again but my newly added files are still good, will leave for a few hours i have nothing left to lose now



• matteocalle - 1 year ago

-
-

I did everything exactly as you said but i can't find any .log files in the given directory :(



• Bursat - 1 year ago

-
-

we can not read scripts u write coz of resolution. is it possible to copy paste your script here so we can read it



• sirvanux - 1 year ago

-
-

I have more than 10 QNAP Clients. 3 of them are affected. I want the unaffected clients to keep working locally. What steps do you recommend to disable all Internet Features or internet access while this thing gets clarified?



• Bursat - 1 year ago

-
-

we can not read scripts u write coz of resolution. is it possible to copy paste your script here so we can read it



• mi_w - 1 year ago

-
-

(duplicate)



• aston729 - 1 year ago

-
-

Is there any chance that the second disk was not infected? RAID 1



• nogaret - 1 year ago

-
-

This is fresh information I just received from QNAP support:

<https://www.qnap.com/en/news/2021/response-to-qlocker-ransomware-attacks-take-actions-to-secure-qnap-nas>

Unfortunately, that only applies if you're NAS did not restarted.



• lukaszromczyk - 1 year ago

-
-

They wrote everything and nothing. I've always updated apps on my NAS, and system scanned everyday night at 3 AM. And at all I have the same problem just as i were not doing anything



• [ss1973](#) - 1 year ago

-
-

So, after Qnap tech support looked at my drives, they said their is nothing they can do to decrypt data. They suggest I pay the ransom if I need the data.



• [AirNelly](#) - 1 year ago

-
-

"So, after Qnap tech support looked at my drives, they said their is nothing they can do to decrypt data. They suggest I pay the ransom if I need the data. "

F QNAP!! They owe me \$550 and they need to buy back this POS NAS that I won't be able to resale because no one will want to buy their \$h*t anymore.



• [iKooza](#) - 1 year ago

-
-

It seems that the SSH method mentioned above works only if the ransomware is still running and using the 7z program. As soon as you update or restart the NAS (which I did as soon as I saw the issue) - the 7z process is no longer active and the method does not work. Is there a way (for whoever knows how to do that) to start the ransomware manually on the QNAP again to generate the log file and retrieve the password?



• [remy99c](#) - 1 year ago

-
-

I saw the !!README.txt file on a single folder on my nas but none of my files are affected. i turned my nas off as soon as i noticed this morning, Now in the evening i read that qnap pushed firmware and app updates to fix this but my TS-453B is already on latest firmware although that one is from 2021-03-02. Should i still be worried or is all fine and am i safe?



• [Bursat](#) - 1 year ago

-
-

Has anyone received a password after making a ransom payment?



• lukaszromczyk - 1 year ago

-
-

If you'll send money never receive the code for sure. Never negotiate with terrorists.



• Bursat - 1 year ago

-
-

You are absolutely right. Thanks.



• lukaszromczyk - 1 year ago

-
-

The same problem. Anyone resolved the problem? I've tried description of @ValiantThor , but probably too late. File 7z.log, not created at all, so virus creator for sure improved fixes to the virus script.



• [charlespig](#) - 1 year ago

-
-

If a 7z.log file was created on the HDA_ROOT and was deleted, is it possible to recover it with some utility?



• [lukaszromczyk](#) - 1 year ago

-
-

I'm not sure if it was created at all. Command didn't receive any errors, but file wasn't created



• [yesman686](#) - 1 year ago

-
-

Got the ransomware as well. i unplug the network and power. should i connect it back and check the log file? I tried the web portal before unplug which doesn't work.



• [yesman686](#) - 1 year ago

-
-

I have plug in everything back like network cable and power. however. the log file was not there under: /mnt/HDA_ROOT
any help?



• [Redbeard77](#) - 1 year ago

-
-

Is there any indication of data being accessed or stolen by a third party in the case of QLocker?



• [janwozniak](#) - 1 year ago

-
-

I looked through all the logs from the week, there is neither proper login nor file copying, so I would be confident about that - just a quick action to get rich by looking for a hole in the whole.



•
oblong - 1 year ago

-
-

I'd like to thank everyone around here for the amazing input. The internet is an amazing place!

I've too been affected. I'm a professional photographer and use my nas as my main archive. Following good advice I have a second one at home that backs up all data every night — which luckily was not affected (probably because it's not always on, it boots up on a schedule and does its tasks, then shuts down again).

While eating breakfast this morning I was wondering why my backup was still running (the nas sits atop my refrigerator). In the office I canceled the running backup. It was only later today that I discovered what shenanigans caused my massive 400GB backup job.

Thankfully my archive is approaching 10TB of data – it does take a considerable amount of time to encrypt this much data. Before I shut the whole thing down and then found this wonderful forum I did check my more important folders and nothing was encrypted. There were these text-notes here and there but most things were still working — probably because my files tend to be large, well above 20MB. The main machine is powered off for now.

This evening I did inspect my backup machine. Luckily it was not affected, but it did back up the files that were encrypted on the main machine (Mostly stuff from 10 years ago – have to check my main machine soon). I'm glad my backups never delete anything so now I have both – original file + encrypted backup ;)

I'm super mad about these f***s. So much unnecessary hassle. I wish those pesky hacking ransom wankers die a slow and painful death from covid combined with ebola, aids and cancer. The internet is such a rotten place!



•

ss1973 - 1 year ago

-
-

OK, So I paid the Ransom and received the Key immediately and it works. The shitty part is I need to figure out how to batch extract in 7z. the directories are not compressed so I have to go into each folder and select the encrypted files. If any one knows how to batch extract with in a directory please share.... So I can maintain the original file structure



•

Marchande - 1 year ago

-
-

how many characters was the password they gave you?



• [PhR34k](#) - 1 year ago

-
-

"OK, So I paid the Ransom and received the Key immediately and it works. The shitty part is I need to figure out how to batch extract in 7z. the directories are not compressed so I have to go into each folder and select the encrypted files. If any one knows how to batch extract with in a directory please share.... So I can maintain the original file structure"

When did you pay? Did you pay recently?

Im thinking of paying but i dont now what Bitcoin site to use so i can send them their money.



• [ss1973](#) - 1 year ago

-
-

I did it with in the hour and instantly received key. I ended up going to a bitcoin ATM to purchase bitcoin



janwozniak - 1 year ago

-
-

All the QNAPs I maintain have the latest software and the latest application updates

"For details, please refer to the QNAP security advisory QSA-21-11 (<https://qnap.to/3eq7hy>) and QSA-21-13 (<https://qnap.to/3dygse>)."

Much newer than here, QNAP proposes, but unfortunately most of the US were hit, after contacting the store (early Central European hours), the recommendations were - to turn off the US.

QNAP releases in the late afternoon that it is bad and not to shut down the servers.

And here I am surprised because I say about 12 devices, half of which on average is encrypted (some only partially), turned off for now but what next? Despite the recommendations of QNAP, unfortunately it does not work as we would like, and most do not intend to pay the ransom.

I went the way: https://www.youtube.com/watch?v=aq_cldY_ksQ but on 2 tested devices there are no such files after switching off.

And now a question for those who paid - after paying you can decrypt everything or each file individually. We are not talking about a flat structure, but a tree.



• LogicNode - 1 year ago

-
-

I manage about 8 QNAP devices right now. Yesterday I fully patched them all with the latest firmware and also updated all of the applications. I confirmed last night that that were all 100% up to date and secure.

Today 4 of those devices have been subject to this ransomware attack.

I can see from the time stamps on the 7z files that the attack took place some 12 hours after I updated the QNAPs!

I have being using 2FA, with super secure passwords. All unnecessary services switched of etc. So have followed industry recommended hardening recommendations.

Checking all the devices again now they are still all reporting up to date. No further updates released by QNAP since I applied the fixes yesterday.

So how is it, that fully patched and updated systems are still being hacked? Could it be that QNAP has not yet correctly identified the vulnerability the hackers are using? Are we all still at risk?



•
[wtutwiler70](#) - 1 year ago

-
-

In case any of you haven't seen this other thread, there is some good info on (1) how to grab the password IF the 7z process is still running; (2) steps to take to lock down all your QNAPs (without necessarily denying yourself access via the Internet, if that is necessary for you - as it is for me); and (3) How to retrieve the deleted, pre-encrypted files, so you don't have to go through the hassle of [paying and] extracting all those files - but it gives you a different pain of renaming and returning the files to their proper places.

Anyway, that thread is here:

<https://www.bleepingcomputer.com/forums/t/749247/qlocker-qnap-nas-ransomware-encrypting-with-extension-7z-read-metxt/page-24#entry5171519>



•
[ChrisBurchett](#) - 1 year ago

-
-

Our developers are currently working on changing one of our brute force tools and are hoping that a couple of people who have successfully decrypted anything / received their password may be willing to share one of their encrypted zip files and their received password. Note the file should be something that does not contain any confidential information, something like a program readme file or any other random file is fine as long as it can be decrypted, we need to validate a couple of things. If anyone is willing please PM me.



Lawrence Abrams - 1 year ago

-
-

Out of curiosity, why are you creating a decryptor for this when the password works with 7zip?



ChrisBurchett - 1 year ago

-
-

Updated, thank you, We have a distributed brute force tool that has had some luck in the past, just passing on the request from our developers here to the community.



Lawrence Abrams - 1 year ago

-
-

Ahh...looking forward to learning more about the tool. Hope we see good success with it.



jj2134 - 1 year ago

-
-

Ok, I need the pictures of my kids back. What's the best wallet and place to purchase bitcoins to send?



• ChrisBurchett - 1 year ago

-
-

"Shakepay" phone app works well if in canada, if not I have heard coinbase but have never used them.



• Xandl - 1 year ago

-
-

If you want you could try this before you make a payment:

It worked for me!

<https://www.bleepingcomputer.com/forums/t/749751/qlocker-full-guide-how-to-get-your-data-back-qnap-nas-hack/>

Cheers



• AirNelly - 1 year ago

-
-

I've sent the BTC and I'm getting the message "Waiting for confirmations (confirm:1, must>=2)" transaction has completed on Coinbase and did so 20 minutes ago.

Anyone else with any insight on how long it took after sending payment??



•

ss1973 - 1 year ago

-
-

are you using 7zip to extract them?



•

AirNelly - 1 year ago

-
-

No but I just tried to download and it looks like it only works on Windows and I'm on a Mac



•

AirNelly - 1 year ago

-
-

Finally got the code but when I double click a Final Cut Pro file for example it asks me to enter password and I do and nothing happens. What do I do??



• ChrisBurchett - 1 year ago

-
-

You will need 7-zip installed to open the file, <https://www.7-zip.org/>

You can also try copying the file to the local desktop, test with a file with a small file size first.



• AirNelly - 1 year ago

-
-

"You will need 7-zip installed to open the file, <https://www.7-zip.org/>

You can also try copying the file to the local desktop, test with a file with a small file size first."

Looks like it only works on Windows, any idea how to do this on a mac??



• ChrisBurchett - 1 year ago

-
-

Possibly this?

<https://osxdaily.com/2010/12/13/open-7z-files-on-a-mac/>



• AirNelly - 1 year ago

-
-

The Unarchiver seems to be duplicating the files properly but when I go into Final Cut Pro and open the affected library my library is empty. Nothing in it



• ChrisBurchett - 1 year ago

-
-

There are likely support files for the project around the decrypted files that are not opening, make sure all files have been decrypted before opening projects and that they are in the same folders as the originals.



• [ss1973](#) - 1 year ago

-
-

Its crazy because I am still seeing constant failed Admin login attempts as we speak. I am batch decrypting my files as fast as possible to get them backed up.



• [Eegy](#) - 1 year ago

-
-

Can anyone tell me if there is a risk of stopping the 7z process when doing a 3 second reset to reset the admin password. I can't find any information anywhere about whether this will reboot the NAS.

Thanks in advance



•
[wtutwiler70](#) - 1 year ago

-
-

@Fugy, I mentioned this in the other forum, but just to restate here:

Due to the nature of the attack, changing the password would be ineffective to stop it. Creating another admin account (without the name 'admin') and disabling the default one MAY help, but unlikely on its own. Both of these things CAN be done without rebooting, though.



•
[rolextec](#) - 1 year ago

-
-

I want to buy the 0.01 bt, but I am from Peru, some support, I need to recover the information.

The password is successful, I have windows 10??????



• cavez - 1 year ago

-
-

Hey guys, affected by this here in Ireland too. Thankfully I only recently began to use a NAS (needless to say I regret choosing QNAP!) and I only 'dumped' files on it and I still have the HDD with them. I managed to salvage something before it got encrypted and I've only lost a few recent files that I can live without. I wouldn't mind finding a password though. I shut down the NAS and rebooted it so the help from Mirror 79 here https://www.youtube.com/watch?v=aq_cldY_ksQ&ab_channel=LinusTechTips might not be an option for me. Also I'm using mac and I see that there are other issues. Hope it gets solved quickly and that those f**%*ers die a slow really painful death



• Melissa81 - 1 year ago

-
-

How has this not reached the news yet?! This is massive! It should be everywhere! What are we to do? Will it be possible to bring back our files? Thankfully I am not a business that has had my files encrypted but I do have 200 000 files of work and personal life on there. Will there be a chance of re-fixing this?



• [davisdd](#) - 1 year ago

-
-

This may sound obvious to some but try and unzip the encrypted files to verify it is actually password protected. My QNAP was very recently patched. I assumed the .7z files were Password protected after finding this article and started the process to try and grab the password using the suggestion mentioned here. I decided to check a few of the files after an unsuccessful attempt. No Password! I was able to extract all of the files!



• [Melissa81](#) - 1 year ago

-
-

when I right click on an image it doesn't come up with an option to unzip it



• [davisdd](#) - 1 year ago

-
-

you will need to download and install 7zip



• denmcca - 1 year ago

-
-

Any chance there might be a list of valid passwords for analysis?



• ChrisBurchett - 1 year ago

-
-

Seconded, have been asking all day and no one seems to be sharing ;)



• denmcca - 1 year ago

-
-

CcrP7PCP1euF0MBjD2C866YYi388m9jD

Taken from https://youtu.be/aq_cldY_ksQ?t=533

At least we know the password is ascii-based.

Mix of upper and lower-case letters, numbers, and 32 characters long.



ChrisBurchett - 1 year ago

-
-

Looks like an md5 of something,

If you go to the web address and look at the data page (right click on page and view source to see the background code)

<http://gvka2m4qt5fod2fltkjmdk4gXH5oxemhpgmnmTjptms6fkfzdd62tad.onion/data.php>

There is an info block that comes back that we are looking into.



Lawrence Abrams - 1 year ago

-
-

I updated the article with an example of another password displayed after making a payment.



• Tony-OZ - 1 year ago

-
-

has anyone thought of combing the files from more than one "QCRAP" NAS system so as to share the cost of the ransom. if this works then 2 will pay 50% and 3 will pay 1/3 of the cost and so on.

Will this work?



• Tony-OZ - 1 year ago

-
-

has anyone thought of combing the files from more than one "QCRAP" NAS system so as to share the cost of the ransom. if this works then 2 will pay 50% and 3 will pay 1/3 of the cost and so on.

Will this work?



• ChrisBurchett - 1 year ago

-
-

The ransom is generated per device so this will not work.



•

Tony-OZ - 1 year ago

-
-

Yes I know but I mean copy the files of one device into the other, so you'll end up with one device rather than two. will this work?



•

jj2134 - 1 year ago

-
-

How do you get the password if you pay the ransom?



•

ChrisBurchett - 1 year ago

-
-

The password would be placed on the same page where you input the transaction ID



• MFR73 - 1 year ago

-
-

after entering the transaction Id. How long does it take for confirmation and password?



• ChrisBurchett - 1 year ago

-
-

Usually About an hour



• vincentw2622 - 1 year ago

-
-

What if i close the page by accident after paying? Can i still get the password entering the page next time?



ChrisBurchett - 1 year ago

-
-

Yes just re enter the id string they gave you and it should show



Lawrence Abrams - 1 year ago

-
-

If you pay, you can always see the password again by logging into their Tor system with your "client key".

From my tests, you do not have to enter the transaction ID again.



• [jj2134](#) - 1 year ago

-
-

I'm not able to edit the transaction ID field after entering my key. Any help? I can't delete it or type.



• [imalek](#) - 1 year ago

-
-

Got nabbed by this this morning. Files started converting around 4 am EST (4/22/21). I was using my laptop at my office and luckily happened to be looking in our archive folders (main purpose of NAS besides camera DVR) and actively saw files being replaced.

immediately unplugged everything and shutdown the NAS.

Luckily for me only local network devices had started propagating the new files and I was able to use a remote PC as a source for the originals after updating, cleaning and restoring everything.

IMMEDIATELY Bought a backup drive for our backup server and will be taking weekly snapshots off-site from now on. It was an eye-opening experience. (our files are mostly docs and PDFs and a 3yr archive is only about 100 gb)

I wish I could turn off ALL outside access, but unfortunately one of the main purposes of our QNAP was the ability for remote cloud service and IP cam DVR w/ remote viewing (Everything thing else is disabled except qcloud.....)

Shout out to ValiantThor for a awesome command for getting the password, I just wish I caught it an hour earlier while 7z was still running)

BEST of luck to all those affected, and my hopes for a full recovery of all your stuff



• [jhy](#) - 1 year ago

-
-

Could the password be in the client key? Might help if those who paid the ransom post their password and client key.



• [imalek](#) - 1 year ago

-
-

Update 4/22/21 09:15 AM EST: Early this morning, BleepingComputer was contacted by security researcher Jack Cable about a bug he discovered in the Qlocker Tor site that allowed users to recover their 7zip passwords for free.

Using this bug, victims could take a Bitcoin transaction ID from a person who had already paid and slightly alter it. When they submitted the altered transaction ID into the Qlocker Tor site, it accepted it as payment and displayed the victim's 7zip password.

Last night, Cable had been privately helping people recover their passwords and arrangements were being made with Emsisoft to create a help system to better exploit this weakness.

Sadly, an hour after we learned of the bug, the ransomware operators caught on and fixed it.



• [ss1973](#) - 1 year ago

-
-

If you decide to pay the ransom, make sure immediately change passwords and back up your files. You are still a target for another attack. Paying the ransom does not make you safe from falling a victim again. I have been constantly getting failed Admin access attempts. Protect your self.



• [ss1973](#) - 1 year ago

-
-

If you decide to pay the ransom, make sure immediately change passwords and back up your files. You are still a target for another attack. Paying the ransom does not make you safe from falling a victim again. I have been constantly getting failed Admin access attempts. Protect your self.



• [ss1973](#) - 1 year ago

-
-

If you decide to pay the ransom, make sure immediately change passwords and back up your files. You are still a target for another attack. Paying the ransom does not make you safe from falling a victim again. I have been constantly getting failed Admin access attempts. Protect your self.



• [AirNelly](#) - 1 year ago

-
-

I've turned off uPnP port forwarding but I'm getting constant admin login failed notifications. I'm trying to get all my files off my QNAP and will need it to run overnight but I don't want them to hack my NAS again. What can I do to ensure they can't access my NAS? I've updated everything



• wtutwiler70 - 1 year ago

-
-

@AlrNelly

Have you tried creating a different account with administrator privileges, and disabling the default admin account? This seemed to take care of the login failures for me, as it is no longer a valid account to log in with.



• ss1973 - 1 year ago

-
-

I created a new admin with a different username and password. A friend of mine had me change my port numbers. And turn on secured https. This has been a stressful 2 days I pray their is some kind of class action suit against QNAp.



• Marchande - 1 year ago

-
-

so now that we know that the password is 32 characters long, I wonder if it would be possible to either generate a dictionary file using just 32 character ascii passwords and run it through hascat and see if its possible to brute force it... thought not sure how long something like that could take to both compile and or brute force ...



• salvo981 - 1 year ago

-
-

hi, but if i pay the ransom to recover my files can i take legal action against qnap since this problem was caused by them?



• ozstar - 1 year ago

-
-

I have got PuTTY on my Win 10x64 (which I have never used before) and given it my admin and pwd for the NAS but what do I do now? The cursor just blinks.



• vincentw2622 - 1 year ago

-
-

try this out and dont reboot your nas

https://youtu.be/aq_cldY_ksQ



•

salvo981 - 1 year ago

-
-

hi, unfortunately I find myself forced to pay as I can to make a transaction in their favor in bitcoin.



•

Tony-OZ - 1 year ago

-
-

what did it cost you pal ?



•

matteocalle - 1 year ago

-
-

Hi Salvo, After making the payment they give your password successfully?



• [polarbear616](#) - 1 year ago

-

-

Nevermind



• [Chris10eS](#) - 1 year ago

-

-

I was affected by the attack as well (the Netherlands). Noticed that not all files were encrypted. But unfortunately the business ones were all. Luckily I had switched off the backup possibility, by turning off the main NAS straight away, My backup files are all okay. No 7z or read me text to be found.



• [Chris10eS](#) - 1 year ago

-

-

I was affected by the attack as well (the Netherlands). Noticed that not all files were encrypted. But unfortunately the business ones were all. Luckily I had switched off the backup possibility, by turning off the main NAS straight away, My backup files are all okay. No 7z or read me text to be found.



• [Boydy81](#) - 1 year ago

-
-

Ok so I have an interesting story I noticed yesterday that I was hit by the qlocker as I was working on an After effects file and the file all of a sudden didn't show up, I looked closer as the 7z file was on the end, this brought me to this thread. The NAS had to be turned off due to Electrical works being done at my house, after looking into this further and from QNAP support themselves they pretty much said that because the NAS has been turned off it useless now, (who is unless you say?) So I have recently turned the NAS back on for a quick look at the files and noticed all my larger files are still there Pics are not however I have had the Edited ones backed up on Dropbox. Can someone recommend how I get the Malware off ? or should I just get the Videos etc off and start again. Just to add to this I do a lot of my Business stuff through dropbox so lucky not off my NAS.

[View all 482 comments](#)

Post a Comment [Community Rules](#)

You need to login in order to post a comment

Not a member yet? [Register Now](#)

You may also like:
