

AgeLocker ransomware targets QNAP NAS devices, steals data

bleepingcomputer.com/news/security/agelocker-ransomware-targets-qnap-nas-devices-steals-data/

Lawrence Abrams

By

[Lawrence Abrams](#)

- September 23, 2020
- 03:37 PM
- 2

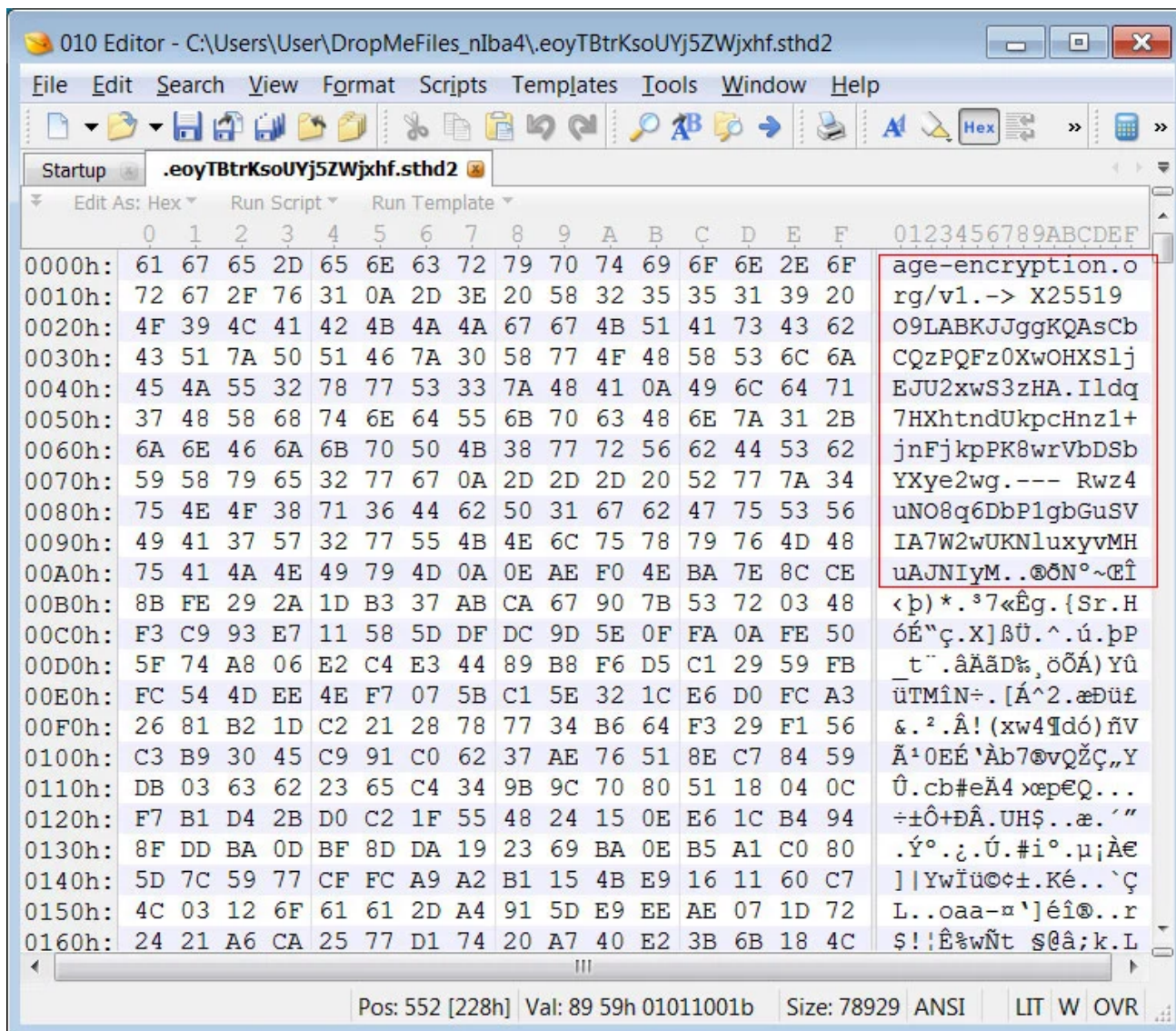


QNAP NAS devices are being targeted in attacks by the AgeLocker ransomware, which encrypts the device's data, and in some cases, steal files from the victim.

AgeLocker is ransomware that utilizes an encryption algorithm called Age (Actually Good Encryption) designed to replace GPG for encrypting files, backups, and streams.

In July 2020, we reported about a new ransomware called AgeLocker that was utilizing this algorithm to encrypt victims' files.

When encrypting files, it would prepend a text header to the encrypted data that starts with the URL 'age-encryption.org,' as shown below.



AGE encrypted file

AgeLocker now targets QNAP NAS devices

Since the end of August 2020, AgeLocker, or another ransomware utilizing the same encryption, has been targeting publicly exposed QNAP NAS devices and encrypting their files.

After a [victim in the BleepingComputer forums](#) uploaded an encrypted file to ID Ransomware, [Michael Gillespie](#) could determine that it was encrypted with the Age encryption.

Gillespie also confirmed that AgeLocker had picked up in activity towards the end of August as they continued to target QNAP devices worldwide.



ID Ransomware submissions

When the ransomware encrypts files, it will leave behind a ransom note named **HOW_TO_RESTORE_FILES.txt** that tells the victim that their QNAP device was specifically targeted in the attack.

"Unfortunately a malware has infected your QNAP and a large number of your files has been encrypted using a hybrid encryption scheme."

```

HOW_TO_RESTORE_FILES.txt - Notepad2
File Edit View Settings ?
1 Hello,
2
3 Unfortunately a malware has infected your QNAP and a large number of your files has been encrypted using a hybrid
  encryption scheme.
4 File names were also encrypted.
5
6 You have to pay for decryption in Bitcoins. The price depends on how fast you write to us. After payment we will send
  you the tool that will decrypt all your files.
7
8 Send email to support@id-r.com with subject "ransomware" and we will talk.
9
10 Free decryption as guarantee
11
12 Before paying you can send us up to 5 files for free decryption.
13 The total size of files must be less than 4Mb (non archived), and files should not contain valuable information.
  (databases, backups, large excel sheets, etc.)
14
15 How to obtain Bitcoins
16
17 The easiest way to buy bitcoins is LocalBitcoins site. You have to register, click 'Buy bitcoins', and select the
  seller by payment method and price.
18 https://localbitcoins.com/buy_bitcoins
19
20 Also you can find other places to buy Bitcoins and beginners guide here:
21 http://www.coindesk.com/information/how-can-i-buy-bitcoins/
22
23 Attention!
24 Do not rename encrypted files.
25 Do not try to decrypt your data using third party software, it may cause permanent data loss.
26 Decryption of your files with the help of third parties may cause increased price (they add their fee to our) or you
  can become a victim of a scam.
27
28
29 If our email account is not working or no answer in 24 hours:
30 1. Download and install TOR Browser from https://www.torproject.org/download/
31 2. Copy url https://www.torproject.org/download/ and open in TOR
  Browser
32 3. You will find actual email address or/and instructions
33 4. If email is not working, or you have no answer in 24 hours, try to refresh page and find new contact

```

AgeLocker-QNAP Ransom Note

In one submission to ID-R, Michael Gillespie reports that the attackers state they first stole unencrypted files that contain "medical data, scans, backups, etc."

It is unknown how much they are demanding as a ransom or how the attackers are gaining access to the QNAP devices.

Unfortunately, there is no way to recover files encrypted by AgeLocker for free.

How to secure an encrypted QNAP NAS device


QNAP has previously been targeted by the [eCh0raix Ransomware](#), which exploited vulnerabilities in the device to encrypt data.

At the time, [QNAP provided the following steps](#) to make sure you are running the latest firmware and vulnerabilities have been patched:

1. Log on to QTS as administrator.
2. Go to **Control Panel > System > Firmware Update**.
3. Under **Live Update**, click **Check for Update**.
QTS downloads and installs the latest available update.

Tip: You can also download the update from the QNAP website. Go to **Support > Download Center** and then perform a manual update for your specific device.

QNAP also suggests users update the Photo Station software with the following steps:

1. Log on to QTS as administrator.
2. Open the **App Center**, and then click  .
A search box appears.
3. Type "Photo Station," and then press **ENTER**.
The Photo Station application appears in the search result list.
4. Click **Update**.
A confirmation message appears.
Note: The **Update** button is not available if you are using the latest version.
5. Click **OK**.
The application is updated.

Finally, all QNAP owners should go through the following checklist to further secure their NAS and check for malware:

- Change all passwords for all accounts on the device
- Remove unknown user accounts from the device
- Make sure the device firmware is up-to-date, and all of the applications are also updated
- Remove unknown or unused applications from the device
- Install QNAP MalwareRemover application via the App Center functionality
- Set an access control list for the device (Control panel -> Security -> Security level)

Related Articles:

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

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

[Industrial Spy data extortion market gets into the ransomware game](#)

[Quantum ransomware seen deployed in rapid network attacks](#)

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

- [AgeLocker](#)
- [Data Exfiltration](#)
- [NAS](#)
- [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



• [Andre_M](#) - 1 year ago

-
-

Did somebody has got their data back by paying ransom or somehow else?



• Andre_M - 1 year ago

-
-

hackers gave me decryptor after some negotiation.

After 48 hours (4TB of DATA) all QNAP Server was decrypted.

More details here: <https://www.bleepingcomputer.com/forums/t/726030/agelocker-ransomware-support-topic/?p=5091353>

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:
