

New DeadBolt ransomware targets QNAP devices, asks 50 BTC for master key

By Lawrence Abrams

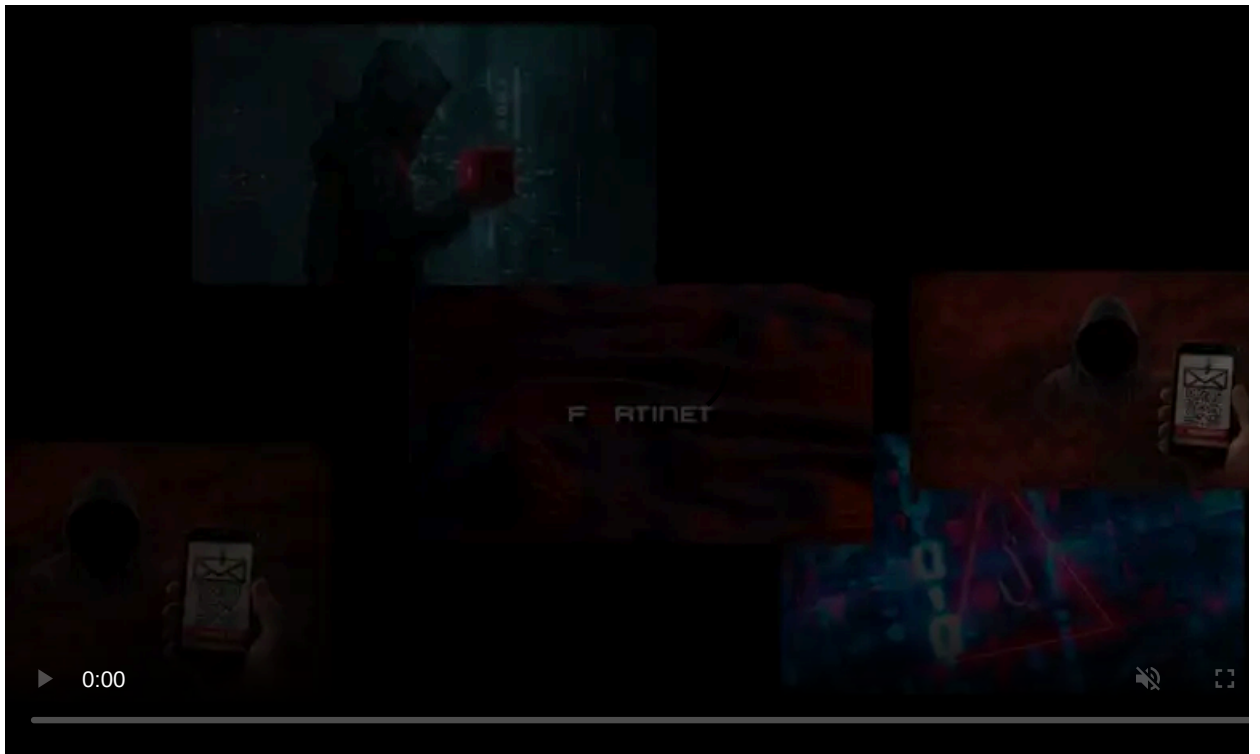
Published: 2022-01-26 · Archived: 2026-04-05 22:40:07 UTC



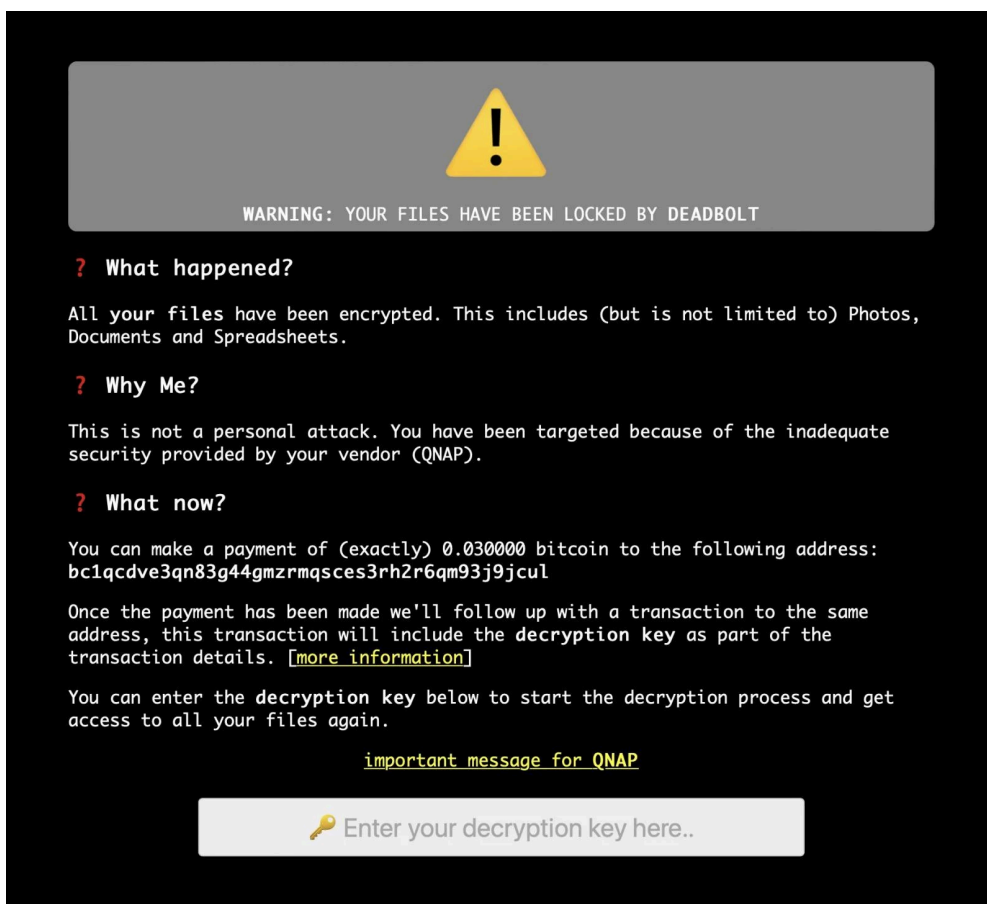
A new DeadBolt ransomware group is encrypting QNAP NAS devices worldwide using what they claim is a zero-day vulnerability in the device's software.

The attacks started today, January 25th, with QNAP devices suddenly finding their files encrypted and file names appended with a **.deadbolt** file extension.

Instead of creating ransom notes in each folder on the device, the QNAP device's login page is hijacked to display a screen stating, "WARNING: Your files have been locked by DeadBolt," as shown in the image below.



Visit Advertiser website [GO TO PAGE](#)



Ransom note on the hijacked QNAP login page

Source: [Twitter](#)

This screen informs the victim that they should pay 0.03 bitcoins (approximately \$1,100) to an enclosed Bitcoin address unique to each victim.

After payment is made, the threat actors claim they will make a follow-up transaction to the same address that includes the decryption key, which can be retrieved using the following instructions.

🔑 Obtaining Decryption Key 🔒

Our decryption key delivery process is **100% transparent and honest**.

The decryption key will be delivered to the bitcoin blockchain inside the OP_RETURN field. You can retrieve it by monitoring the address you made your payment to for new transactions containing the OP_RETURN field. An easy way to do this is using a public blockchain explorer like blockchain.com.



Outputs ⓘ	
Index	0
Address	📄
Pkscript	OP_RETURN 9025a8c9946f9ecc651879e49ff42a6e

example of decryption key as found on blockchain.com explorer.

The decryption key always has an exact length of 32 characters.

Entering the **wrong** decryption key will not harm your files. This page will tell you if the entered key is invalid.

After the decryption has finished successfully, this page will disappear and you can access the management interface again. However, it is strongly advised to migrate all your data to a more secure platform.

📌 If you struggle with this process, please contact an IT professional to help you.

Decryption key instructions

Source: [landski at BleepingComputer](#)

This decryption key can then be entered into the screen to decrypt the device's files.

QNAP has told BleepingComputer that users can bypass the ransom screen and access their admin page by using the http://nas_ip:8080/cgi-bin/index.cgi or https://nas_ip/cgi-bin/index.cgi URLs.

BleepingComputer is aware of at least fifteen victims of the new DeadBolt ransomware attack, with no specific region being targeted.

As with all ransomware attacks against QNAP devices, the DeadBolt attacks only affect devices accessible to the Internet.

As the threat actors claim the attack is conducted through a zero-day vulnerability, it is strongly advised that all QNAP users disconnect their devices from the Internet and place them behind a firewall.

QNAP further told us that their Product Security Incident Response Team (PSIRT) is investigating the attack vectors now and that [owners should follow these steps](#) to protect their data and NAS.

With QNAP owners being targeted by ongoing attacks from two other ransomware families known as [Qlocker](#) and [eCh0raix](#), all owners should follow [these steps](#) to prevent future attacks.

BleepingComputer has created a [DeadBolt ransomware support topic](#) that can be used to discuss the attacks and potentially receive help from other QNAP owners.

Attackers demand 50 bitcoin for master key

On the main ransom note screen, there is a link titled "important message for QNAP," that when clicked, will display a message from the DeadBolt gang specifically for QNAP.

On this screen, the DeadBolt ransomware gang is offering the full details of the alleged zero-day vulnerability if QNAP pays them 5 Bitcoins worth \$184,000.

They are also willing to sell QNAP the master decryption key that can decrypt the files for all affected victims and the zero-day info for 50 bitcoins, or approximately \$1.85 million.

"Make a bitcoin payment of 50 BTC to bc1qnju697uc83w5u3ykw7luujzupfyf82t6tr1nd8," the threat actors wrote in a message to QNAP.

"You will receive a universal decryption master key (and instructions) that can be used to unlock all your clients their files. Additionally, we will also send you all details about the zero-day vulnerability to security@qnap.com."

⚠ Important Message for QNAP ⚠

All your affected customers have been targeted using a zero-day vulnerability in your product. We offer you two options to mitigate this (and future) damage:

1) Make a bitcoin payment of 5 BTC to
bc1qnju697uc83w5u3ykw7luujzupfyf82t6tr1nd8:

You will receive all details about this zero-day vulnerability so it can be patched. A detailed report will be sent to **security@qnap.com**.

2) Make a bitcoin payment of 50 BTC to
bc1qnju697uc83w5u3ykw7luujzupfyf82t6tr1nd8:

You will receive a universal decryption master key (and instructions) that can be used to unlock all your clients their files. Additionally, we will also send you all details about the zero-day vulnerability to **security@qnap.com**.

Upon receipt of payment for either option, all information will be sent to you in a timely fashion.

There is no way to contact us.
These are our only offers.
Thanks for your consideration.

Greetings,
DEADBOLT team.

Message from threat actors for QNAP

Source: [Twitter](#)

The ransomware gang further states that there is no way to contact them other than through Bitcoin payments.

This method of communication is a very different approach than other ransomware attacks that usually provide some form of communication, whether through a dedicated Tor website, email, or messaging platforms.

QNAP force updates to

On January 26th, QNAP began [force-updating customers' NAS devices](#) to firmware version 5.0.0.1891, which is the latest universal firmware released on December 23rd, 2021.

QNAP told BleepingComputer that they forced-installed this update as they believe the threat actors are using a [remote code execution vulnerability](#) fixed in the [5.0.0.1891 firmware](#) version.

However, a customer posted to the QNAP forum stating that they were encrypted even when they had this firmware version installed, indicating that the threat actors are likely exploiting a different vulnerability.

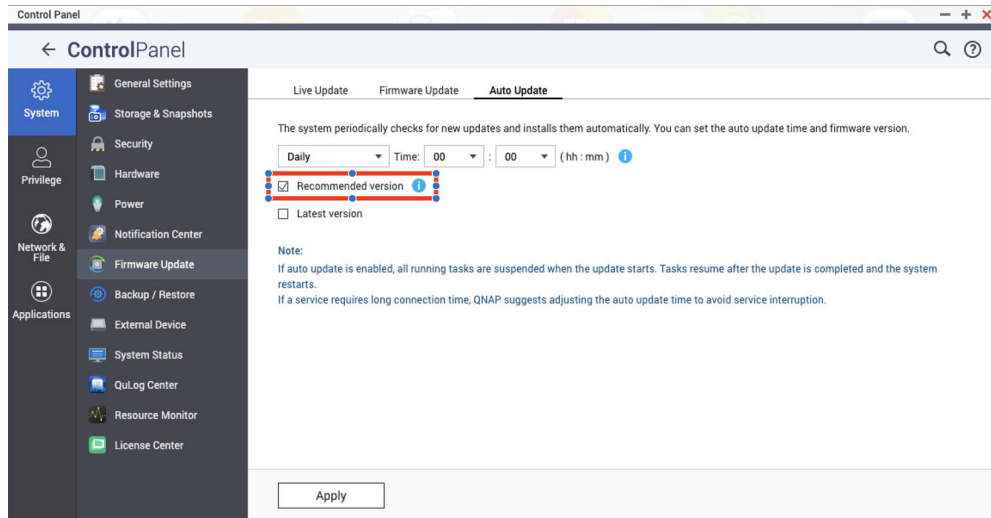
"Confirmed getting hit with deadbolt while using 5.0.0.1891 build 20211221 on a tvs-1282t3," the NAS owner [posted](#) to the QNAP forums.

After asking for a comment on this, QNAP conceded that it could be another vulnerability exploited by the threat actors.

"All the information we have shows DEADBOLT could be prevented with the build. Theoretically, we cannot exclude the possibility that there is the other vulnerability exploited. We are also interested in the user's observation," QNAP told BleepingComputer.

"If possible, we would suggest users with similar situation could submit a ticket to Technical Support."

QNAP also told BleepingComputer that the update should only have been installed by those with the 'Recommended version' setting enabled in the Auto Updates settings, as shown below.



QNAP auto update settings

QNAP asks customers to contact technical support if they are still receiving updates with that setting unchecked.

DeadBolt technical details

When a QNAP NAS device is compromised, the threat actors will install the DeadBolt malware executable as a randomly named file in the `/mnt/HDA_ROOT/` folder. For example, the DeadBolt ransomware executable could be located at `/mnt/HDA_ROOT/27855`.

Ransomware expert Michael Gillespie told BleepingComputer that ransomware is initially launched with a config file, which likely contains various data, including an encryption key used to encrypt files.

The initial command to encrypt files is:

```
[random_file_name] -e [config] /share
```

The `/share` folder is where QNAP NAS devices store user folders and files.

When encrypting files, the ransomware will only target files with the following file extensions:

```
.3dm, .3ds, .3fr, .3g2, .3gp, .3pr, .ab4, .accdb, .accdc, .accde, .accdr, .accdt, .ach, .acr, .act, .adb, .ads, .agdl, .a
```

Gillespie says the files are encrypted with AES128 encryption and will have the `.deadbolt` extension appended to file names. For example, `test.jpg` will be encrypted and renamed to `test.jpg.deadbolt`.

DeadBolt will also replace the `/home/httpd/index.html` file so that when victims access the device, they will see the ransom screen demanding a ransom of 0.03 bitcoins to a specified bitcoin address.

If a ransom is paid, the threat actors will create a bitcoin transaction to the same bitcoin ransom address that contains the decryption key for the victim. The decryption key is located under the `OP_RETURN` output, as shown below.

Index	2
Address	
Pkscript	OP_RETURN 5f144b4c18e8794587b60c8f60c49372

Bitcoin transaction's OP_RETURN output containing decryption key

Source: *BleepingComputer*

When you enter this key into the ransom note screen, the web page will convert it into a SHA256 hash and compare it to the SHA256 hash of the victim's decryption key and the SHA256 hash of the master decryption key.

The SHA256 hash for the master decryption key

is **93f21756aeeb5a9547cc62dea8d58581b0da4f23286f14d10559e6f89b078052**.

If the decryption key matches either SHA256 hash, it will decrypt the files using the following command:

```
/mnt/HDA_ROOT/[encryptor_name] -d "[decryption_key]" /share
```

Multiple victims have reported paying the ransom and receiving a decryption key that has successfully decrypted their files.

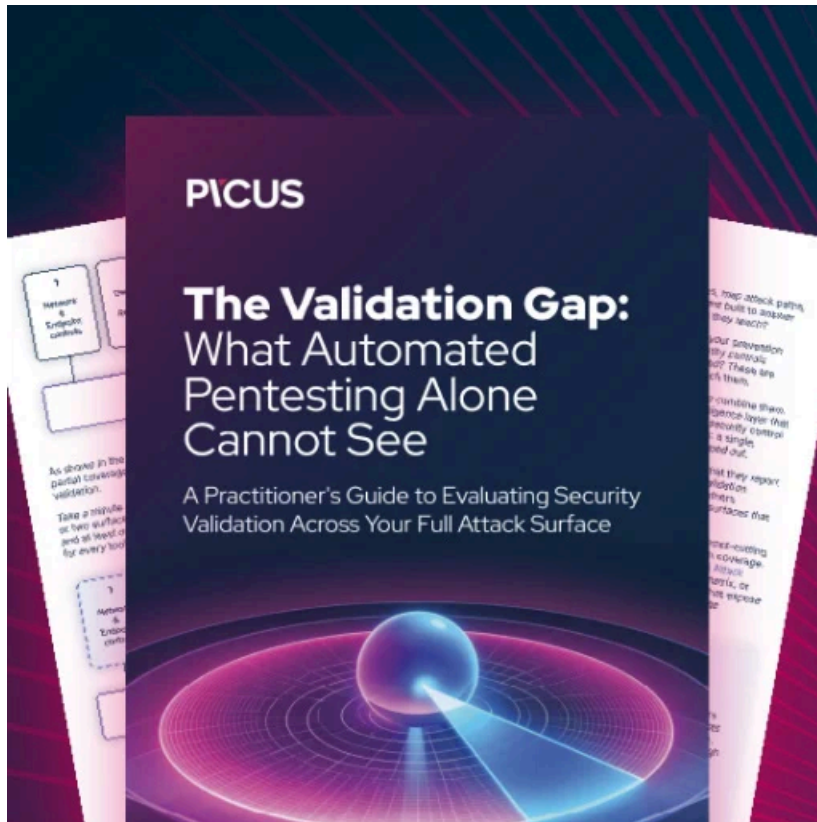
However, QNAP's forced firmware updates are causing the executable and index.html ransom screen to be deleted from the device, which prevents the decryption of files.

Gillespie has created a free Windows decryptor that can be [downloaded from Emsisoft](#) and decrypt files without needing the ransomware executable. However, users will still need a valid decryption key, which QNAP owners can only obtain at this time by paying a ransom.

Update: Added further information on how the decryption key will be retrieved.

Update 1/26/22: Added further information from QNAP

Update 1/28/22: Added technical details, information on exploited vulnerabilities, and number of victims.



[Automated Pentesting Covers Only 1 of 6 Surfaces.](#)

Automated pentesting proves the path exists. BAS proves whether your controls stop it. Most teams run one without the other.

This whitepaper maps six validation surfaces, shows where coverage ends, and provides practitioners with three diagnostic questions for any tool evaluation.

Source: <https://www.bleepingcomputer.com/news/security/new-deadbolt-ransomware-targets-qnap-devices-asks-50-btc-for-master-key/>