QNAP warns of new DeadBolt ransomware encrypting NAS devices

Optimized bioepingcomputer.com/news/security/qnap-warns-of-new-deadbolt-ransomware-encrypting-nas-devices



QNAP is warning customers again to secure their Internet-exposed Network Attached Storage (NAS) devices to defend against ongoing and widespread attacks targeting their data with the new DeadBolt ransomware strain.

"DeadBolt has been widely targeting all NAS exposed to the Internet without any protection and encrypting users' data for Bitcoin ransom," <u>the company said</u> in a statement issued today.

"Your NAS is exposed to the Internet and at high risk if there shows 'The System Administration service can be directly accessible from an external IP address via the following protocols: HTTP' on the dashboard."

All QNAP users are urged to "immediately update QTS to the latest available version" to block incoming DeadBolt ransomware attacks.

The NAS maker also advises customers to immediately disable Port Forwarding on their router and the UPnP function of the QNAP NAS using the following steps:

• **Disable the Port Forwarding function of the router:** Go to the management interface of your router, check the Virtual Server, NAT, or Port Forwarding settings, and disable the port forwarding setting of NAS management service port (port 8080 and 433 by default).

 Disable the UPnP function of the QNAP NAS: Go to myQNAPcloud on the QTS menu, click the "Auto Router Configuration," and unselect "Enable UPnP Port forwarding."

You can also use this <u>detailed step-by-step guide</u> to toggle off SSH and Telnet connections, change the system port number and device passwords, and enable IP and account access protection.

There is also a <u>DeadBolt ransomware support topic</u> on BleepingComputer's forum with more info on the attacks and with help from other QNAP users.

New DeadBolt ransomware surfaces

As BleepingComputer reported yesterday, the <u>DeadBolt ransomware group started</u> <u>attacking QNAP users</u> on January 25th, encrypting files on compromised NAS devices and appending a .deadbolt file extension.

The attackers are not dropping ransom notes on encrypted devices but, instead, they are hijacking the login pages to display warning screens saying "WARNING: Your files have been locked by DeadBolt."

The ransom screen asks the victims to pay 0.03 bitcoins (roughly \$1,100) to a unique Bitcoin address generated for each victim, claiming that the decryption key will be sent to the same blockchain address in the OP_RETURN field once the payment goes through.

At the moment, there are no confirmations that the threat actors will actually deliver on their promise to send a working decryption key after paying the ransom.

<u>.</u>	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
WARNING: YOUR FILES HAVE BEEN LOCKED BY DEADBOLT What happened? All your files have been encrypted. This includes (but is not limited to) Photos, Documents and Spreadsheets.	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 <u>blockchain.com</u> .
 ? Why Me? This is not a personal attack. You have been targeted because of the inadequate security provided by your vendor (QNAP). ? What now? You can make a payment of (exactly) 0.030000 bitcoin to the following address: bc1qcdve3qn83q44gmzrmqsces3rh2r6qm93j9jcul 	Index 0 Address Pkscript OP_RETURN 9025a8c9946f9ecc651879e49ff42a6e example of decryption key as found on blockchain.com explorer.
Once the payment has been made we'll follow up with a transaction to the same address, this transaction will include the decryption key as part of the transaction details. [more information] You can enter the decryption key below to start the decryption process and get access to all your files again. <u>important message for QNAP</u> <u>P Enter your decryption key here.</u>	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.

DeadBolt ransom note and instructions (BleepingComputer)

These ongoing DeadBolt ransomware attacks only impact exposed NAS devices and, given that the attackers also claim to use a zero-day bug, it's advised to disconnect them from the Internet just as QNAP recommended in today's warning.

The DeadBolt gang is also <u>asking QNAP to pay 50 bitcoins</u> (around \$1.85 million) for the zero-day and a master decryption key to decrypt files for all affected victims.

Today's warning is the third one QNAP issued to alert customers of ransomware attacks targeting their Internet-exposed NAS devices in the last 12 months.

They were previously warned of <u>eCh0raix ransomware</u> attacks in May and <u>AgeLocker</u> <u>ransomware</u> attacks in April.

The company also <u>urged all QNAP NAS users to secure NAS devices exposed to Internet</u> <u>access</u> on January 7th, at the same time alerting them of active ransomware and bruteforce attacks.