QNAP warns of new DeadBolt ransomware encrypting NAS devices

bleepingcomputer.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," the company said 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 detailed step-by-step guide 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 DeadBolt ransomware support topic on BleepingComputer's forum with more info on the attacks and with help from other QNAP users.

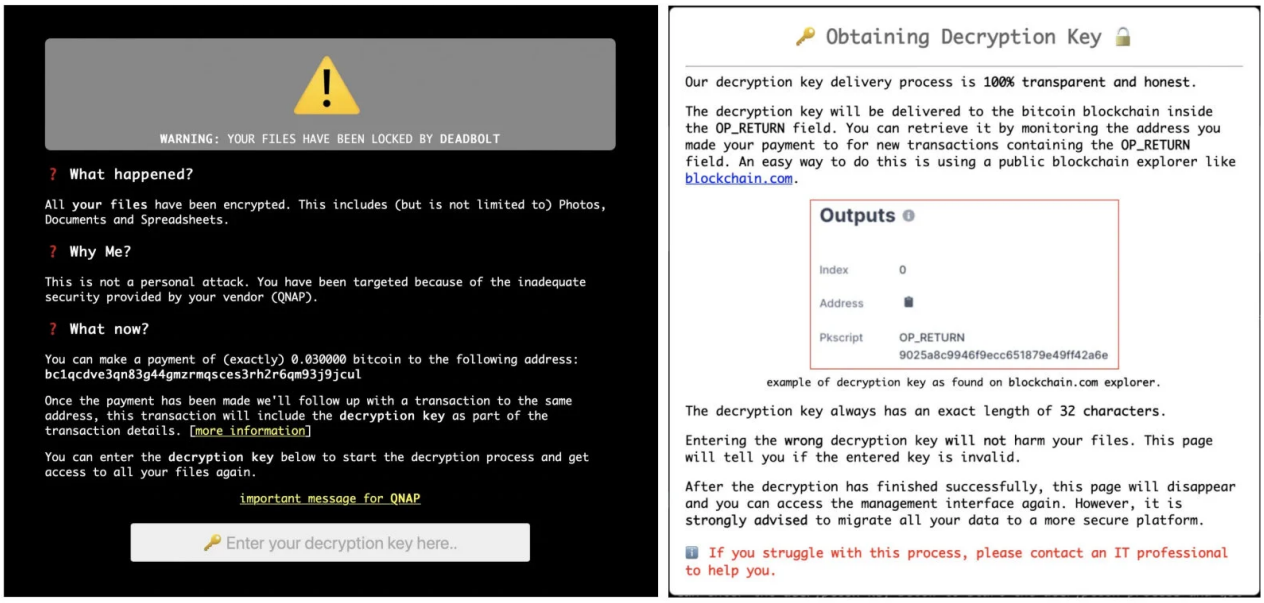
New DeadBolt ransomware surfaces

As BleepingComputer reported yesterday, the DeadBolt ransomware group started attacking QNAP users 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.



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 asking QNAP to pay 50 bitcoins (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 eCh0raix ransomware attacks in May and AgeLocker ransomware attacks in April.

The company also urged all QNAP NAS users to secure NAS devices exposed to Internet access on January 7th, at the same time alerting them of active ransomware and brute-force attacks.