

## QNAP warns of eCh0raix ransomware attacks, Roon Server zero-day

By Sergiu Gatlan

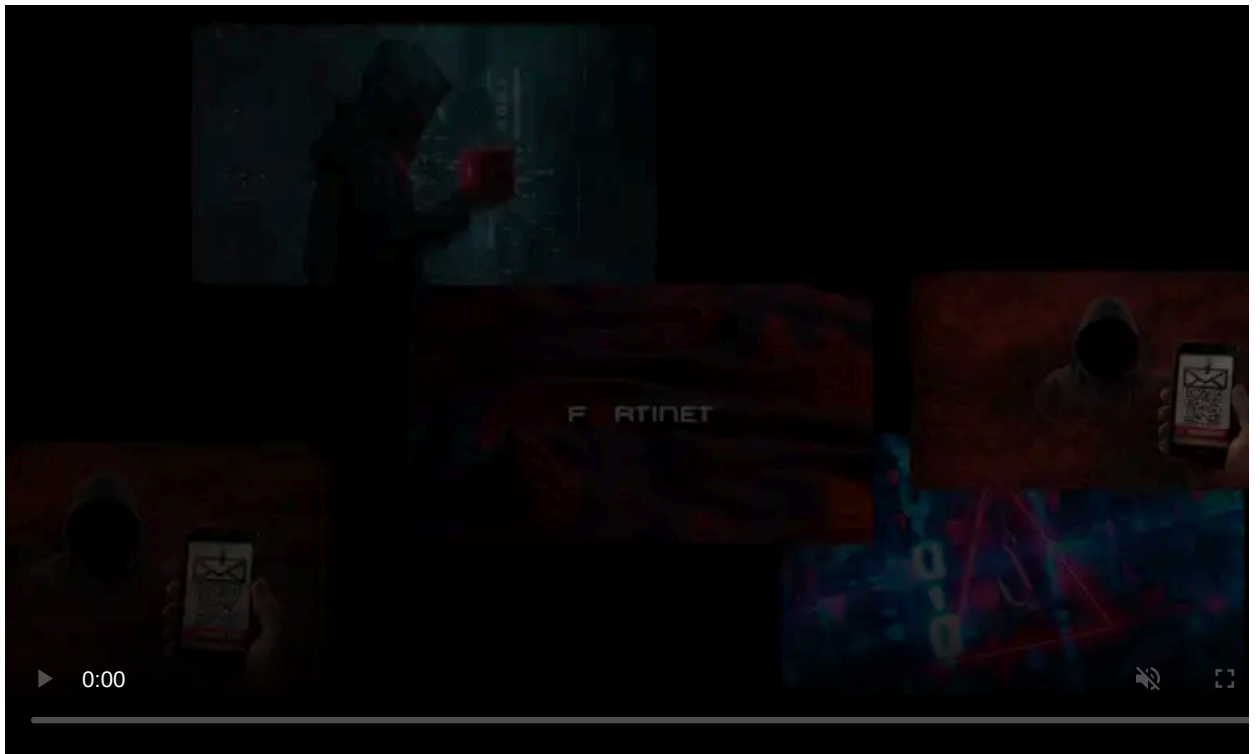
Published: 2021-05-14 · Archived: 2026-04-05 23:14:39 UTC



QNAP warns customers of an actively exploited Roon Server zero-day bug and eCh0raix ransomware attacks targeting their Network Attached Storage (NAS) devices.

This warning comes only two weeks after QNAP users were alerted of an ongoing AgeLocker ransomware outbreak.

The Taiwan-based NAS appliance maker says that it has received reports of devices impacted by eCh0raix ransomware in a security advisory published today.



Visit Advertiser website [GO TO PAGE](#)

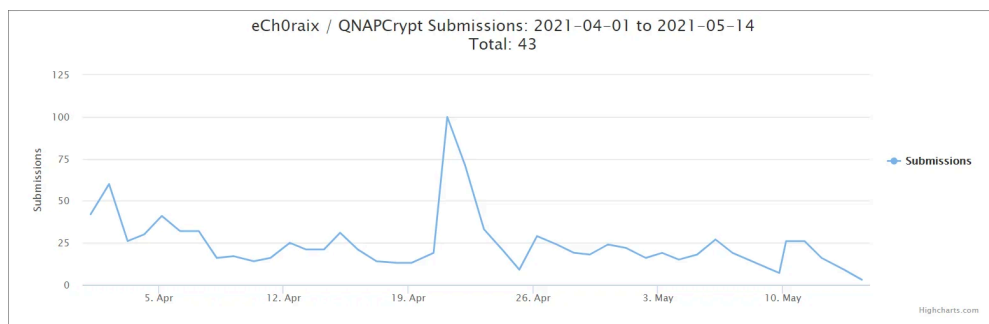
"The eCh0raix ransomware has been reported to affect QNAP NAS devices," the company said. "Devices using weak passwords may be susceptible to attack."

QNAP urged customers to "act immediately" to protect their data from potential eCh0raix attacks by:

- Using stronger passwords for your administrator accounts.
- Enabling IP Access Protection to protect accounts from brute force attacks.
- Avoiding using default port numbers 443 and 8080.

Detailed step-by-step instructions on changing your NAS password, enabling IP Access Protection, and changing the system port number are available in the [security advisory](#).

While QNAP doesn't mention how many reports it received from users directly affected by eCh0raix ransomware in the last weeks, BleepingComputer has seen an uptick in attack reports on the highly active [eCh0raix support topic](#).



*eCh0raix activity (ID Ransomware)*

## Actively exploited Roon Server zero-day

Today, although not making a direct connection with the eCh0raix attacks, QNAP also [warned of an actively exploited zero-day vulnerability](#) impacting Roon Labs' Roon Server 2021-02-01 and earlier versions.

The company recommends disabling the [Roon Server music server](#) and not exposing the NAS on the Internet to protect it from these active attacks until Roon Labs provides a security update.

To disable Roon Server on your NAS, you have to follow this procedure:

1. Log on to QTS as administrator.
2. Open the **App Center** and then click . A search box appears.
3. Type "Roon Server" and then press **ENTER**. Roon Server appears in the search results.
4. Click the arrow below the Roon Server icon.
5. Select **Stop**. The application is disabled.

QNAP also [fixed a command injection vulnerability in the Malware Remover app](#) on Thursday.

This security flaw would allow remote attackers to execute arbitrary commands on devices running vulnerable app versions.

## Heavily targeted by ransomware

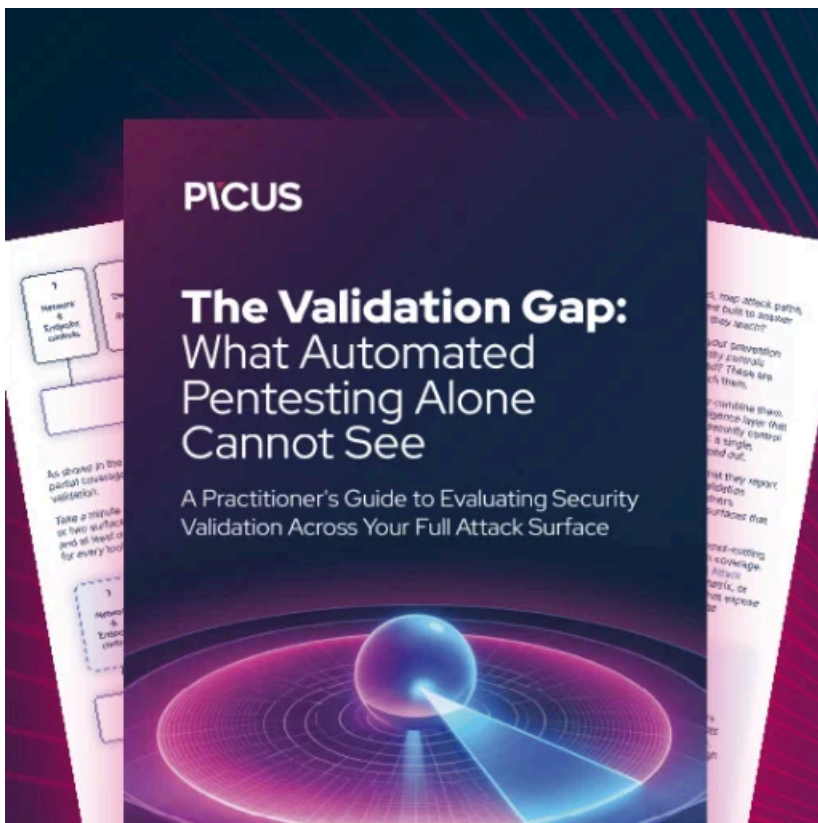
QNAP devices were previously targeted by eCh0raix ransomware (also known as QNAPCrypt) in [June 2019](#) and [June 2020](#).

A massive [Qlocker ransomware campaign](#) also hit QNAP devices starting mid-April, with the threat actors behind the attacks [making \\$260,000 in just five days](#) by remotely encrypting data using the 7zip archive program.

Additionally, QNAP removed a backdoor account (aka hardcoded credentials) in the HBS 3 Hybrid Backup Sync backup and disaster recovery app.

It was later [confirmed](#) that Qlocker ransomware operators used the removed backdoor account to hack into some QNAP customers' NAS devices and encrypt their files.

As mentioned in the beginning, [AgeLocker ransomware](#) also hit QNAP customers two weeks ago and in another campaign [targeting publicly exposed NAS devices](#) exploiting vulnerable Photo Station versions during September 2020.



### [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/qnap-warns-of-echo-raid-ransomware-attacks-roon-server-zero-day/>