QNAP warns of AgeLocker ransomware attacks against NAS devices

therecord.media/qnap-warns-of-agelocker-ransomware-attacks-against-nas-devices/

April 29, 2021

Taiwanese hardware vendor QNAP said today that its network-attached storage (NAS) devices are under attack by a ransomware operation known as AgeLocker.

In a security advisory, the Taiwanese company urged customers to immediately update their NAS operating system and any apps they have installed on the device to prevent the AgeLocker gang from getting a foothold on their systems and encrypting their files.

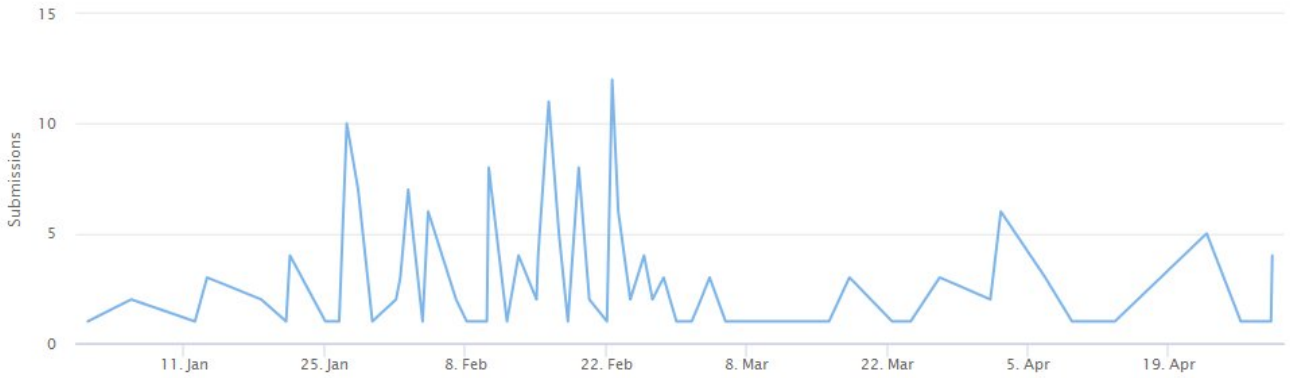
“To further secure your device, do not expose your NAS to the internet,” the company said. If you must connect your NAS to the internet, we highly recommend using a trusted VPN or a myQNAPcloud link.”

QNAP did not specify which vulnerabilities the AgeLocker gang was abusing.

It is unclear if the AgeLocker gang was hunting for QNAP NAS systems left unpatched or if they were targeting a recently patched vulnerability.

Today’s advisory comes after last week QNAP warned of similar attacks against its NAS systems from the Qlocker and eCh0raix ransomware strains.

According to statistics provided by the ID-Ransomware service, there doesn't seem to be a particular spike in activity from the AgeLocker group, which suggests these new AgeLocker attacks are not happening on the same scale as the Qlocker attacks from last week.



The AgeLocker ransomware was first spotted in the wild in July 2020 when it exploited bugs in the QNAP NAS firmware (known as QTS) and in a preinstalled app named PhotoStation.

The company warned of these attacks a few months later, in September 2020, when customer incidents started to rise.

AgeLocker is the fourth ransomware strain known to target QNAP NAS devices after Qlocker, eCh0raix, and Muhstik. AgeLocker's name comes from its use of the Actually Good Encryption (AGE) algorithm to encrypt files.

Besides ransomware, QNAP NAS devices have also been historically targeted by the Dovecat and UnityMiner crypto-miners and the QSnatch backdoor trojan.

Tags

- malware
- NAS
- network-attached storage
- QNAP
- Ransomware
- Taiwan

Catalin Cimpanu is a cybersecurity reporter for The Record. He previously worked at ZDNet and Bleeping Computer, where he became a well-known name in the industry for his constant scoops on new vulnerabilities, cyberattacks, and law enforcement actions against hackers.