Protecting NAS Devices Against Evolving Threats

What You Need to Know

By Stephen Hilt and Fernando Mercês

Users and businesses have noticeably become more dependent on the internet of things (IoT) for connectivity and access to information. This dependence is accompanied by a demand for customized features and round-the-clock connection to the internet, a requirement that manufacturers of network-attached storage (NAS) devices have responded to over the years. Cybercriminals have taken notice of these developments and have pivoted their threats and attacks to compromise these connected gadgets, as we elaborate in our paper, "**Backing Your Backup: Defending NAS Devices Against Evolving Threats**."

Why are NAS devices a target?

NAS devices are targeted for two main reasons. First, the security measures that can be implemented in these devices are optional. Secondly, these devices contain valuable information since they are used for both storage and backup. Moreover, users and businesses unwittingly expose their vulnerable NAS devices to the internet for access, simultaneously making them easier for criminals to find.

What threats target NAS?

The following are some of the threats that we analyze as specifically focused on NAS devices:

- Ransomware, including notorious families REvil and Qlocker
- Botnets, notably StealthWorker
- Cryptominers, specifically UnityMiner and Dovecat
- Highly targeted attacks, such as QSnatch

How can I defend my NAS device?

As a vital component of storage and backup strategies for businesses and consumers, NAS devices can be protected from attackers with some basic best practices:

- Never connect NAS devices directly to the internet.
- Customize and regularly change access and security credentials of all connected devices. Never use devices' preset default passwords.
- Enable two-factor authentication (2FA) whenever available.
- Uninstall any services that are not in use, such as software and applications.
- Regularly check NAS manufacturers' online security guides for additional protection against attacks.

Read more of our analysis and security recommendations in our research, "**Backing Your Backup: Defending NAS Devices Against Evolving Threats**."

Read the full paper at **https://research.trendmicro.com/NASSecurity** for more on NAS devices and how to protect them against threats.

TREND MICRO | research