Synology warns of malware infecting NAS devices with ransomware

bleepingcomputer.com/news/security/synology-warns-of-malware-infecting-nas-devices-with-ransomware/

Sergiu Gatlan

By
Sergiu Gatlan

- August 9, 2021
- 09:12 AM
- 0

Taiwan-based NAS maker Synology has warned customers that the StealthWorker botnet is targeting their network-attached storage devices in ongoing brute-force attacks that lead to ransomware infections.

According to Synology's PSIRT (Product Security Incident Response Team), Synology NAS devices compromised in these attacks are later used in further attempts to breach more Linux systems.

"These attacks leverage a number of already infected devices to try and guess common administrative credentials, and if successful, will access the system to install its malicious payload, which may include ransomware," Synology said in a security advisory.

"Devices infected may carry out additional attacks on other Linux based devices, including Synology NAS."

The company is coordinating with multiple CERT organizations worldwide to take down the botnet's infrastructure by shutting down all detected command-and-control (C2) servers.

Synology is working on notifying all potentially impacted customers of these ongoing attacks targeting their NAS devices.

How to defend against these attacks

The NAS maker urges all system admins and customers to change weak administrative credentials on their systems, to enable account protection and auto block, and to set up multi-factor authentication where possible.

Synology rarely issues security advisories warning of active attacks against its customers. The last alert regarding ransomware infections following successful large-scale brute-force attacks was published in July 2019.

The company advised users to go through the following checklist to defend their NAS devices against attacks:

- Use a complex and strong password, and **Apply password strength rules** to all users.
- Create a new account in the administrator group and disable the system default "admin" account.
- Enable **Auto Block** in **Control Panel** to block IP addresses with too many failed login attempts.
- Run **Security Advisor** to make sure there is no weak password in the system.

"To ensure the security of your Synology NAS, we strongly recommend you enable Firewall in Control Panel and only allow public ports for services when necessary, and enable 2-step verification to prevent unauthorized login attempts," the company added.

"You may also want to enable Snapshot to keep your NAS immune to encryption-based ransomware."

Synology provides more information on defending your NAS device against ransomware infections here.

Brute-force malware targeting Windows and Linux machines

While Synology did not share more information regarding the malware using in this campaign, the shared details line up with a Golang-based brute forcer discovered by Malwarebytes at the end of February 2019 and dubbed StealthWorker.

Two years ago, StealthWorker was used to compromise e-commerce websites by exploiting Magento, phpMyAdmin, and cPanel vulnerabilities to deploy skimmers designed to exfiltrate payment and personal information.

However, as Malwarebytes noted at the time, the malware also has brute force capabilities that enable it to log into Internet-exposed devices using passwords generated on the spot or from lists of previously compromised credentials.

Starting with March 2019, StealthWorker operators switched to a brute force-only approach scanning the Internet for vulnerable hosts with weak or default credentials.

Once deployed on a compromised machine, the malware creates scheduled tasks on both Windows and Linux to gain persistence and, as Synology, warned deploys second-stage malware payloads, including ransomware.

While the NAS maker didn't issue a security advisory, customers reported in January that they had their devices infected with Dovecat Bitcoin cryptojacking malware [1, 2] starting with November 2020, in a campaign that also targeted QNAP NAS devices.

---

*Update August 10:*A Synology spokesperson sent BleepingComputer the following statement:

> We originally became aware of this attack at the end of July. Over the 2-3 weeks since then we've received under 50 reports from our customers. Considering the amount of Synology devices out there (over 8 million active deployments) we feel the number of devices exposed to this attack is very low. Our team has also noticed a slowdown in these attacks over the last few days.
>
> At this point, we're still actively investigating this malware attack and the scripts used. Currently, we believe the botnet engages in brute-forcing the "admin" account using common password combinations. At this time we have not seen the malware try to target any other user accounts.
>
> As mentioned previously our customers first reported this attack at the end of July. We've since sent a notice to affected customers and sent an additional notice to all Synology users advising them of our best practices and tips on how to secure their NAS.

Related Articles:

QNAP warns of ransomware targeting Internet-exposed NAS devices

Microsoft detects massive surge in Linux XorDDoS malware activity

QNAP alerts NAS customers of new DeadBolt ransomware attacks

Microsoft: Sysrv botnet targets Windows, Linux servers with new exploits

New cryptomining malware builds an army of Windows, Linux bots