QSnatch - Malware designed for QNAP NAS devices | NCSC-FI

Published: 2019-10-25 · Archived: 2026-04-05 23:01:33 UTC

NCSC-FI received reports via the Autoreporter service during mid October of infected devices attempting to communicate to specific command and control (C2) servers. Originally the malware was designated as Caphaw, which is targeted to Windows-operating systems, but the parameters used in the C2 traffic had strong indications towards QNAP-devices, and an investigation was started.

About the malware functionality

When investigating the related domain names and the requests performed by the malware the functionality and features of the malware were found in depth. The original infection method remains unknown, but during that phase malicious code is injected to the firmware of the target system, and the code is then run as part of normal operations within the device. After this the device has been compromised. The malware uses domain generation algorithms to retrieve more malicious code from C2 servers. The retrieval method is "HTTP GET https://<generated-address>/qnap_firmware.xml?=t<timestamp>", and this request is a strong indicator of compromise.

The retrieved code will then be executed within the operating system with system rights. At this phase at least the following will be done:

- Operating system timed jobs and scripts are modified (cronjob, init scripts)
- Firmware updates are prevented via overwriting update sources completely
- QNAP MalwareRemover App is prevented from being run
- All usernames and passwords related to the device are retrieved and sent to the C2 server
- The malware has modular capacity to load new features from the C2 servers for further activities
- Call-home activity to the C2 servers is set to run with set intervals

The malware was named QSnatch based on the target system and the "snatching" activity the malware performs.

Cleansing an infected device

The malware can be removed from an infected device with two possible methods: performing a full factory reset (effectively destroying all stored data within the device). Another unconfirmed method is to apply an update provided by the vendor (see link below). NCSC-FI has not been able to confirm whether the update actually removes the malware, and this is also acknowledged by the manufacturer. After cleansing the device further steps are required:

- Change all passwords for all accounts on the device
- Remove unknown user accounts from the device
- Make sure the device firmware is up-to-date and all of the applications are also updated
- Remove unknown or unused applications from the device

- Install QNAP MalwareRemover application via the App Center functionality
- Set an access control list for the device (Control panel -> Security -> Security level)

In case of further assistance we recommend contacting QNAP support (see link below).

NCSC-FI recommends that NAS devices are categorically not exposed to the internet without firewalling to prevent external attacks. Additionally constant updates will provide protection against vulnerabilities found within the systems.

Update Nov 4th 2019

QNAP has released updated instructions and a version of their MalwareRemover app for detecting and cleaning up infected devices.

NCSC-FI would like to thank Doina Cosovan of SecurityScorecard for providing us with the initial information and collaboration in investigating this threat.
