National Cyber Security Centre
a part of GCHQ

CISA
CYBER+INFRASTRUCTURE

Alert: Potential legacy risk from malware targeting QNAP NAS devices

Version 1.1

10 August 2020

About this document

This report provides details of the malware Qsnatch (also known as ‘Derek’) from NCSC, CISA and industry partner analysis.

It includes indicators of compromise as well as detection and mitigation advice.

Disclaimer

This report draws on information derived from multiple sources. Any NCSC findings and recommendations made have not been provided with the intention of avoiding all risks, and following the recommendations will not remove all such risk. Ownership of information risks remains with the relevant system owner at all times.

This is a joint alert from the United Kingdom's National Cyber Security Centre (NCSC) and the Cybersecurity and Infrastructure Security Agency (CISA) in the United States.

Introduction

The NCSC and CISA are investigating a strain of malware called QSnatch (also known as 'Derek'), which attackers used in late 2019 to target Network Attached Storage (NAS) devices manufactured by the firm QNAP.

All QNAP NAS devices are potentially vulnerable to QSnatch malware if not updated with the latest security fixes. The malware, documented in open-source reports,[1] has infected thousands of devices worldwide with a particularly high number of infections in North America and Europe.[2] Further, once a device has been infected, attackers can prevent administrators from successfully running firmware updates.

This alert summarises the findings of NCSC,CISA and industry partner analysis and provides mitigation advice.

Details

Campaigns

The NCSC and CISA have identified two campaigns of activity for QSnatch malware. The first campaign likely began in early 2014 and continued until mid-2017, while the second started in late 2018 and was still active in late 2019. The two campaigns are distinguished by the initial payload used as well as some differences in capabilities. This alert focuses on the second campaign as it is the most recent threat.

It is important to note that infrastructure used by the malicious cyber actors in both campaigns is not currently active, but the threat remains to unpatched devices.

Although the identities and objectives of the malicious cyber actors using QSnatch are currently unknown, the malware is relatively sophisticated, and the cyber actors demonstrate an awareness of operational security.

Global distribution of infections

Analysis shows a significant number of infected devices. In mid-June 2020, there were approximately 62,000 infected devices worldwide; of these, approximately 3,900 were in the UK and 7,600 were in the US. Figure 1 below shows the location of these devices in broad geographic terms.

[1] https://www.zdnet.com/article/thousands-of-qnap-nas-devices-have-been-infected-with-the-qsnatch-malware/
[2] Ibid

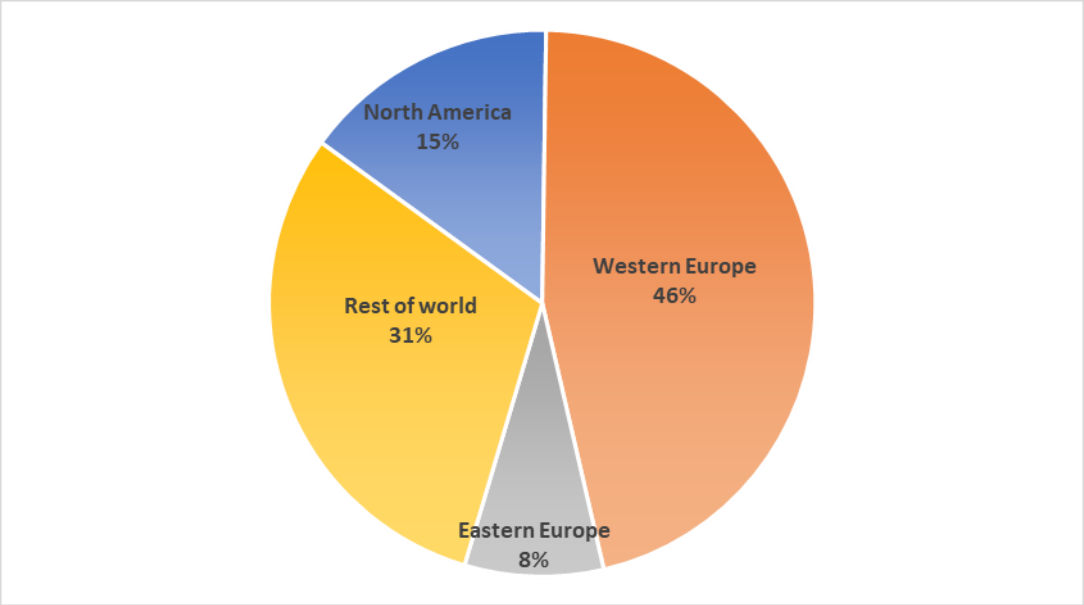

Figure 1: Location QNAP NAS devices infected by QSnatch

Delivery and exploitation

The infection vector has not been identified, but QSnatch appears to be injected into the device firmware during the infection stage, with the malicious code subsequently run within the device, compromising it. The attacker then uses a domain generation algorithm (DGA) to establish a command and control (C2) channel that periodically generates multiple domain names for use in C2 communications, using the following HTTP GET request:

```
HTTP GET https://[generated-address]/qnap_firmware.xml?=t[timestamp]
```
[3]

Malware functionalities

Analysis shows that QSnatch malware contains multiple functionalities, such as:

- **CGI password logger**
  - This installs a fake version of the device admin login page, logging successful authentications and passing them to the legitimate login page.
- **Credential scraper**
- **SSH backdoor**
  - This allows the cyber actor to execute arbitrary code on a device.
- **Exfiltration**
  - When run, QSnatch steals a predetermined list of files, which includes system configurations and log files. These are encrypted with the actor's public key and sent to their infrastructure over HTTPS.

[3] https://www.kyberturvallisuuskeskus.fi/en/news/qsnatch-malware-designed-qnap-nas-devices

- **Webshell functionality for remote access**

Persistence

The malware appears to gain persistence by preventing updates from installing on the infected QNAP device. The attacker modifies the system host's file, redirecting core domain names used by the NAS to local out-of-date versions so updates can never be installed.

Samples

The following tables provide hashes of related QSnatch samples found in open-source malware repositories. File types fall into two buckets: (1) shell scripts (see table 1) and (2) shell script compiler (SHC)-compiled executable and linking format (ELF) shell scripts (see table 2). One notable point is that some samples intentionally patch the infected QNAP for Samba remote code execution vulnerability CVE-2017-7494.

Table 1: QSnatch samples – shell scripts

SH Samples (SHA256)
09ab3031796bea1b8b79fcfd2b86dac8f38b1f95f0fce6bd2590361f6dcd6764
3c38e7bb004b000bd90ad94446437096f46140292a138bfc9f7e44dc136bac8d
8fd16e639f99cdaa7a2b730fc9af34a203c41fb353eaa250a536a09caf78253b
473c5df2617cee5a1f73880c2d66ad9668eeb2e6c0c86a2e9e3375976391d1a
55b5671876f463f2f75db423b188a1d478a466c5e68e6f9d4f340396f6558b9f
9526ccdeb9bf7cfd9b34d290bdb49ab6a6acefc17bff0e85d9ebb46cca8b9dc2
4b514278a3ad03f5efb9488f41585458c7d42d0028e48f6e45c944047f3a15e9
fa3c2f8e3309ee67e7684abc6602eea0d1d18d5d799a266209ce594947269346
18a4f2e7847a2c4e3c9a949cc610044bde319184ef1f4d23a8053e5087ab641b
9791c5f567838f1705bd46e880e38e21e9f3400c353c2bf55a9fa9f130f3f077
a569332b52d484f40b910f2f0763b13c085c7d93dcdc7fea0aeb3a3e3366ba5d
a9364f3faffa71acb51b7035738cbd5e7438721b9d2be120e46b5fd3b23c6c18
62426146b8fcaeaf6abb24d42543c6374b5f51e06c32206ccb9042350b832ea8
5cb5dce0a1e03fc4d3ffc831e4a356bce80e928423b374fc80ee997e7c62d3f8
5130282cdb4e371b5b9257e6c992fb7c11243b2511a6d4185eafc0faa0e0a3a6
15892206207fdef1a60af17684ea18bcaa5434a1c7bdca55f460bb69abec0bdc
3cb052a7da6cda9609c32b5bafa11b76c2bb0f74b61277fecf464d3c0baeac0e
13f3ea4783a6c8d5ec0b0d342dcdd0de668694b9c1b533ce640ae4571fdbf63c

Table 2: QSNATCH samples - SHC-compiled ELF shell scripts

SH Samples (SHA256)
18a4f2e7847a2c4e3c9a949cc610044bde319184ef1f4d23a8053e5087ab641b
3615f0019e9a64a78ccb57faa99380db0b36146ec62df768361bca2d9a5c27f2
845759bb54b992a6abcbca4af9662e94794b8d7c87063387b05034ce779f7d52
6e0f793025537edf285c5749b3fcd83a689db0f1c697abe70561399938380f89

Mitigation

As stated above, once a device has been infected, attackers have been known to make it impossible for administrators to successfully run the needed firmware updates. This makes it extremely important for organisations to ensure their devices have not been previously compromised. **Organisations that are still running a vulnerable version should take the following steps prior to completing the firmware upgrade to ensure the device is not left vulnerable:**

- **Scan the device with the latest version of Malware Remover**, available in QNAP App Center, to detect and remove QSnatch or other malware.
    - If the installation via App Center fails, manually install Malware Remover following this QNAP tutorial, or contact QNAP Technical Support for further assistance.
- **Run a full factory reset on the device.**
- **After the removal of malware, update the firmware to the latest version.**

The usual checks to ensure that the latest updates are installed still apply. **To prevent reinfection, this recommendation also applies to devices previously infected with QSnatch but from which the malware has been removed.**

To prevent QSnatch malware infections, the NCSC and CISA strongly recommend that organisations take the recommended measures in QNAP's November 2019 advisory.[4]

The NCSC and CISA also recommend organisations consider the following mitigations:

- Verify that you purchased QNAP devices from reputable sources.
    - If sources are in question then, in accordance with the instructions above, **scan the device with the latest version of the Malware Remover and run a full factory reset on the device prior to completing the firmware upgrade**. For additional supply chain recommendations, see CISA's tip on Securing Network Infrastructure Devices.
- Block external connections when the device is intended to be used strictly for internal storage.

[4] https://www.qnap.com/en/security-advisory/nas-201911-01