Alert: Potential legacy risk from malware targeting QNAP NAS devices
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.

\(\text{1} \) https://www.zdnet.com/article/thousands-of-qnap-nas-devices-have-been-infected-with-the-qsnatch-malware/

\(\text{2} \) 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]

**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.

- **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)*

<table>
<thead>
<tr>
<th>SH Samples (SHA256)</th>
</tr>
</thead>
<tbody>
<tr>
<td>09ab3031796bea1b8b79fcfd2db86dac8f38b1f95f0fcee6bd259036fd6cd6764</td>
</tr>
<tr>
<td>3c38e7bb004b000bd9ad9446437096f46140292e138bf9f7e44dc136bac8d</td>
</tr>
<tr>
<td>8fd16e639f99cdaa7a2b730fc9af34a203c41fb353eaa250a536a09caf78253b</td>
</tr>
<tr>
<td>473c5df2617ce5a1f73880c2d466ad9668eeb2e6c0c6a9e3375797639d1a</td>
</tr>
<tr>
<td>55b5671876f463f2f75db423b188a1d478a466c5e68e6f9df340396f6558b9f</td>
</tr>
<tr>
<td>9526ccdeb9b7fc9d93d290db49ab6a6acefc17bfff0e859dbbb4cca89b0dc</td>
</tr>
<tr>
<td>4b514278a3ad03f5efb9488f41585458c7d42d0028e48f6e45c944047f3a15e</td>
</tr>
<tr>
<td>fa3c2f8e3309ee67e7684abc6602eaa01d85d799a266209ce5494974269346</td>
</tr>
<tr>
<td>18a4f2e7847a2c4e3c9a949cc610044bde319184ef1f4d23a8053e5087a641b</td>
</tr>
<tr>
<td>9791c5f567838f1705bd468e80e38e2e9f3400c353c2bf55a9fa9f130f3f077</td>
</tr>
<tr>
<td>a569332b52d484f40b910f2f0763b13c0285c7d93dcd7cea0e8a3e3366ba5d</td>
</tr>
<tr>
<td>a9364f3fa77a1c5b1b7035738cbd5e7438721b9d2be120e46b5f3b23c6c18</td>
</tr>
<tr>
<td>62426146b8fcaef6abb24d2453c63745f51e06c32206ccb9042350b832ea8</td>
</tr>
<tr>
<td>5cb5dce0a1e03fc4d3f8c831e4a356bce80e928423b374fc80ee997e962d3f8</td>
</tr>
<tr>
<td>5130282cd4b4e371b59257e6c992fbb7c121432b2511a6d4185eaf0faa0e0a3a6</td>
</tr>
<tr>
<td>15892206207fde1fa60af17684ea18bcaaa534a1c7bda65f460bb69abec0bdc</td>
</tr>
<tr>
<td>3cb052a7ada6cda9609c32b5bafa11b76c2bb0f74b61277feca464dc0baead0e</td>
</tr>
<tr>
<td>13f3ea4783a6c8d5ecb0d342dcd90de668694b9c1b533ce640ae4571f6bf63c</td>
</tr>
</tbody>
</table>
### 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 must run a full factory reset on the device prior to completing the firmware upgrade** to ensure the device is not left vulnerable.

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.
- Block external connections when the device is intended to be used strictly for internal storage.

---