The eCh0raix Ransomware

By Anomali Threat Research

Published: 2026-03-12 · Archived: 2026-04-05 20:54:27 UTC

Introduction

Anomali researchers have observed a new ransomware family, dubbed eCh0raix, targeting QNAP Network Attached Storage (NAS) devices. QNAP devices are created by the Taiwanese company QNAP Systems, Inc., and contain device storage and media player functionality, amongst others. The devices appear to be compromised by brute forcing weak credentials and exploiting known vulnerabilities in targeted attacks. The malicious payload encrypts the targeted file extensions on the NAS using AES encryption and appends .encrypt extension to the encrypted files. The ransom note created by the ransomware has the form shown below.

```
All your data has been locked(crypted). How to unclock(decrypt) instruction located in this TOR web
```

Note that there is a typo in the ransom note which may indicate that the actors behind this campaign are not native-English speakers.

QNAP Technical Breakdown

The malware is written and compiled in the Go programming language. The ransomware is very simple with its source code being fewer than 400 lines. A reconstruction of the source code tree is shown below. The functionality is standard for a ransomware: check if already encrypted, walk the file system for files to encrypt, encrypt the files, and produce the ransom note.

```
Package main: /home/user/go/src/qnap_crypt_worker File: main.go        getInfo Lines: 61 to 123 (6
```

Upon execution, the malware reaches out to the URL http://192.99.206[.]61/d.php?s=started and notifies the Command and Control (C2) that the encryption process has begun, as shown in Figure 1.

Checks if the instance is already running by reaching out to a C2 IP. If it is, exit process.
Figure 1 - Checks if the instance is already running by reaching out to a C2 IP. If it is, exit process.

Establishing C2 connection

The malware communicates to the C2 sg3dwqfpnr4sl5hh[.]onion via a SOCKS5 Tor proxy at 192.99.206[.]61:65000, as seen in Figures 2 and 3. Based on the analysis it is clear that the proxy has been set up by the malware author to provide Tor network access to the malware without including Tor functionality in the malware.


Port scan results on Proxy IP.
Figure 2 - Port scan results on Proxy IP.


Connects via SOCKS5 proxy
Figure 3 - Connects via SOCKS5 proxy

The malware retrieves the RSA public key and the ‘readme’ text content from the C2 server. One of the samples analyzed used the URL “http://sg3dwqfpnr4sl5hh[.]onion/api/GetAvailKeysByCampId/10”, that possibly suggests this was the 10th campaign run by the threat actor. The data returned by the C2 server is encoded in JSON and the malware unserializes the data into the following Go data struct:

```
type main.Info struct {         RsaPublicKey string         Readme string }
```

Encryption Module

The module generates a 32 character random string from the array “abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQRSTUVWXYZ!@#$%^&*()_+” to create an AES-256 key. By using this fixed set of characters, the effective key space is 192-bit. As can be seen in Figure 4, the malware initializes the math random page with the seed of the current time. Since it is using the math’s package to generate the secret key, it is not cryptographically random and it is likely possible to write a decryptor.


Set the math random seed with the current time.
Figure 4 - Set the math random seed with the current time.

The generated AES key is then encrypted with a public key which was either embedded in the malware sample or retrieved from the C2 server, depending on the version of the malware. The resulted string is then encoded with base64 and added to the README_FOR_DECRYPT.txt file.

Before the malware encrypts any files, it proceeds to kill the below list of processes. The processes are stopped on the infected NAS by issuing the commands “service stop %s” or “systemctl stop %s”.

- apache2
- httpd
- nginx
- mysqld
- mysql
- php-fpm
- php5-fpm
- postgresql

File Encryption

The files are encrypted with AES in Cipher Feedback Mode (CFB) with the secret key that was generated. When selecting files to encrypt, the ransomware skips any files where the absolute path for the file contain any of the strings listed below.

- /proc
- /boot/
- /sys/
- /run/
- /dev/
- /etc/
- /home/httpd
- /mnt/ext/opt
- .system/thumbnail
- .system/opt
- .config
- .qpkg

If the path does not contain any of the strings, it checks the file extension for the file. If the file extension is one of the extensions shown below, the ransomware encrypts the file. The encrypted data is written to a new file with the original name and file extension but the file extensions ".encrypt" is appended to the end. Once the file has been written, the original file is removed.

```
.dat.db0.dba.dbf.dbm.dbx.dcr.der.dll.dml.dmp.dng.doc.dot.dwg.dwk.dwt.dxf.dxg.ece.eml.epk.eps.erf.es
```

Once the entire encryption process is completed the malware reaches out to the URL http://192.99.206.61/d[.]php?s=done and sends the command "done" to notify the completion of encryption, Figure 5.


Send "done" to C2
Figure 5 - Send "done" to C2

C2 Analysis

The analyzed C2 URL (http://sg3dwqfpnr4sl5hh[.]onion) has partial directory listing enabled, and after browsing through the directories, Anomali researchers were able to find a sample named "linux_crypter". The sample was packed by UPX. Analysis of the unpacked sample confirmed that it is written in Go and had some modifications to the previously analysed sample. The sample found on C2, checks the locale of the infected NAS for Belarus, Ukraine, or Russia and exits without doing anything if a match is found. This technique is common amongst threat actors, particularly when they do not wish to infect users in their home country.

Analysis

The eCh0raix ransomware, named after a string found in the malware, is a ransomware used in targeted attacks. It appears to not be designed for mass distribution. The samples with a hardcoded public key appear to be compiled for the target with a unique key for each target. Otherwise the decryptor sold by the threat actor could be used for all victims. The samples that fetch the public key and ransom note from the C2 server, also send a request when it starts and when it is done. This is probably used to provide the threat actor with live feedback. The request does not include any identifiable information for the threat actor to discern multiple targets.

The threat actor targets QNAP NAS devices that are used for file storage and backups. It is not common for these devices to run antivirus products and currently the samples are only detected by 2-3 products on VirusTotal, Figure 6, which allows the ransomware to run uninhibited. It is not known how these devices are infected. According to a post on Bleeping Computer's forum, some infected systems were not fully patched and others reported detections of failed login attempts.

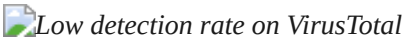
Low detection rate on VirusTotal

Figure 6 - Low detection rate on VirusTotal

> *"During my research, the nas pops me severals time with the message "HTTP Login Failed", like every second."*
> - zerocool64

> *"Seems all of us are using QNAP NAS, which version of QTS where you using at the time of the attack? Mine was 4.1.3"*
> - eggxpert

> *"I've found a lot of .encrypt files on my RAID 6 in my QNAP TS-459 Pro II with 4.2.6 firmware"*
> - alew1s3

> *"I've activated system registry and suddenly there are a lot of attempts to login via HTTP in my myqnapcloud by strange usernames and IPs so i totally disabled it"*
> - alew1s3

> *"Same as someone already explained: lot of login failed that day."*
> - lucagiroletti

Figure 7 - Content from BleepingComputer forum post

Source: https://www.anomali.com/blog/the-ech0raix-ransomware