FL|INT.

SEKOIA.IO

SEKOIA.IO THREAT **INTEL**LIGENCE **FLASH** REPORT

TLP WHITE

2022-016
11/03/2021

QNAP worm: who benefits from crime?

OBJECTIVES:
UNKNOWN

INTRUSION SET:
UNKNOWN

Summary

In January 2022, SEKOIA obtained from a trusted source several IOCs related to a worm which used compromised QNAP devices as command and control servers. This worm, which seems to be present in many networks around the globe, has been seen active in several french networks.

Even if its spreading method doesn't use any vulnerabilities, its main code is quite sophisticated and the infrastructure used is large. SEKOIA have been able to get one sample of the code and the analysis is ongoing to understand its the aim: cybercriminals playing around or more serious actors behind it?

Before having the full conclusions behind this threat, we wanted to share with our readers some network IOCs and a few rules related to this threat in order to hunt it inside your windows environments. We will be glad to have any feedback under TLP/NDA if you have seen this threat inside your IT systems or have more intelligence related to it.

Relaying on LNK files downloading an MSI

This worm is using LNK files taking the icons of removable devices to spread (eg. Network shares, USB devices). These LNK files are using well-known techniques in order to download

and execute from a compromised device an MSI package containing a malicious library.

Figure 1. Sample of LNKs used by the threat actor

At the time of writing, three execution chains using different obfuscation methods have been seen used in the wild when a victim click on the shortcut file:

- Use `msiexec` with the arguments -q (quiet) and -i (install) to download in HTTP and install the remote MSI package.
- Use wmic and the argument "`product call install`" to download in HTTP and install the remote MSI package.
- Call cmd.exe to start a binary blob which contains the malicious msiexec execution command, download and execute the malicious MSI and then execute explorer to open the removable service.

The compromised device seems to act as a reverse proxy and verifies if the right URL is provided by the client in order to send the malicious MSI package. If a wrong URL is provided, the server will respond by the QNAP default 404 page (Server: `http server 1.0`), otherwise it will respond with a "`Server: nginx`" header. Here is some URL patterns seen being used in the wild:

- `http://[domain]:8080/[token]/[computername]=[username]`
- `http://[domain]:8080/[token]/[computername]`
- `http://[domain]:8080/[token]/[computername]?[username]`

As the communication is in HTTP, it is quite easy to know which workstation and user have been compromised inside your Windows environment by just looking at the network flows.

SEKOIA.IO has been able to retrieve only one MSI package from the attacker infrastructure and we still don't know the logic behind the token generation and the other checks performed by the server.

The malicious downloaded MSI contains a heavily obfuscated DLL which is still under analysis by SEKOIA.IO. However, according to our source and analysis, this DLL exfiltrates environment execution data (Workstation name, Username, etc.) to a second infrastructure composed of QNAP servers, also on the port 8080. We share at the end of the FLINT the indicators related to this DLL.

QNAP infrastructure and beyond

At the beginning of the campaign, the MSI files were downloaded from compromised QNAP devices but since the DeadBolt ransomware attack, the operators seem to have diversified their infrastructure. New compromised devices have been seen, mostly Internet boxes in Germany. In fact, few of their C2 were targeted by the DeadBolt ransomware because of running vulnerable QNAP versions.

These QNAP - and the rest of the compromised infrastructure - are resolved by small domain names registered through few registrars such as Njalla (64), Registrar-servers (17), Ndns (5) and Flokinet (2) since september 2021. As of today, 90 domain names have been seen associated with this campaign, resolving 176 unique IP addresses.

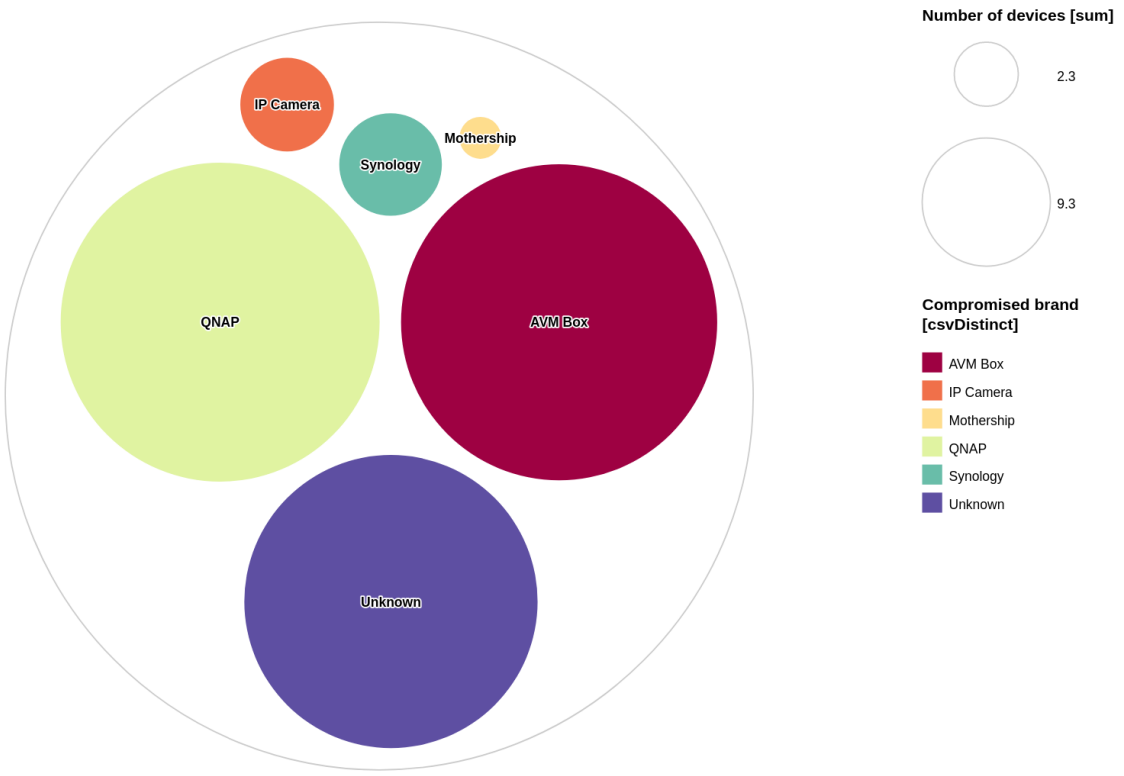

Figure 2. C2 by brands of compromised devices

In the chart above, a server named “mothership” is present. This server (`185.55.243[.]109`) is the only-one C2 which is not a compromised device in this infrastructure. We named it “mothership” because it is resolved by many domain names. Moreover, we think with a medium confidence that the network redirections from the compromised devices are made to it.

One other questions remain unanswered today regarding the targeting: what vulnerabilities do they use to compromise at least 13 different models of QNAP devices with firmware versions varying from 4.2.6 to 5.0.0? Moreover, by plotting the whole C2 lists - including the QNAP devices - on a map or via the autonomous systems we can clearly see a specific targeting in Europe, especially German networks.

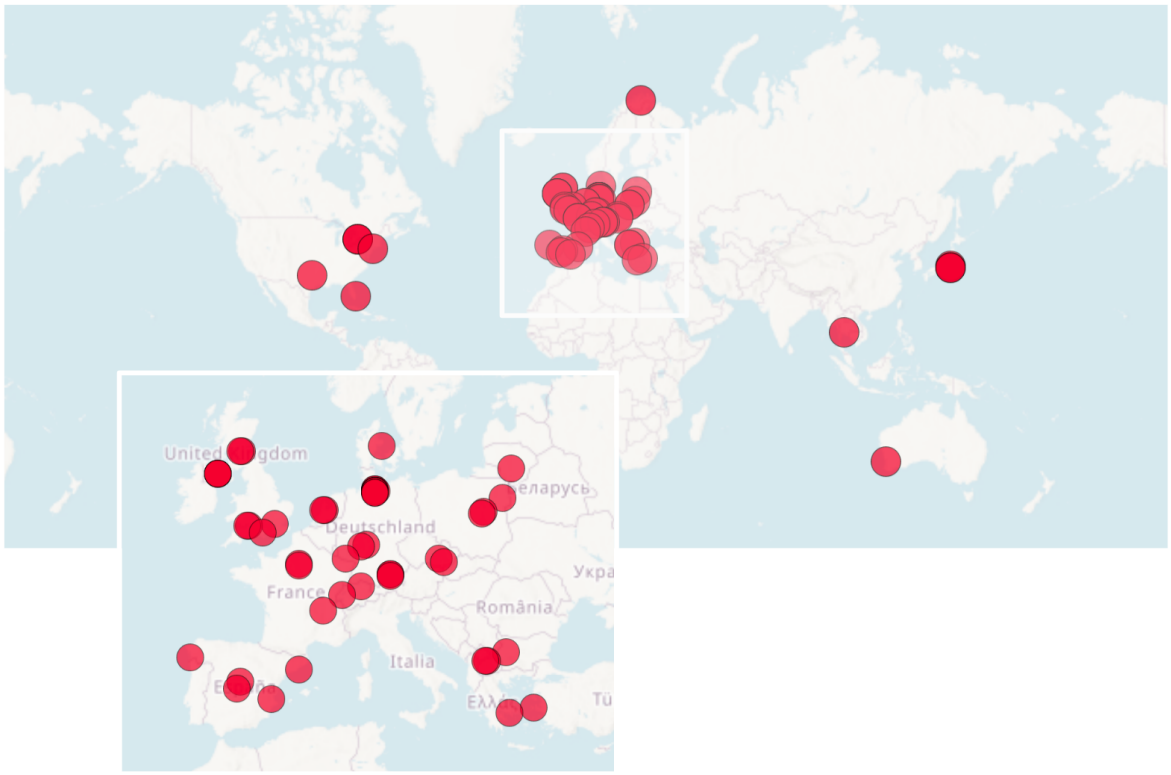

Figure 3. C2 by brands of compromised devices

This campaign raises more questions than answers. We are constantly monitoring the infrastructure to follow any changes from it and we hope to finish the analysis of the worm in the next few weeks. In the meantime, please find attached to this FLINT the network IOCs related to this campaign.

Course Of Actions

Filter Network Traffic - Use network appliances to filter ingress or egress traffic and perform protocol-based filtering. Configure software on endpoints to filter network traffic.

Restrict File and Directory Permissions - Restrict access by setting directory and file permissions that are not specific to users or privileged accounts

Limit Hardware Installation - Limit the use of USB devices and removable media within a network.

IOCs & Technical Details

Hashes

```
6fad3552f6b6cefcc27be589c3a687b2 (MSI Archive)
e8f0d33109448f877a0e532b1a27131a (Executed DLL)
80f8291c0b707e1bf4c8d2fcb06e2101 (LNK variant 1)
660dd9de83da1046ff76115f54730404 (LNK variant 2)
94414cc9a9a7907bd7e7fbabc07e4421 (LNK variant 3)
```

Second infrastructure

77.233.110[.]97
77.131.246[.]80
72.84.118[.]132

Mothership server

185.55.243[.]109

C2 domains

glnj[.]nl
zk5[.]co
j2[.]gy
nzm[.]one
jjl[.]one
pjz[.]one
wak[.]rocks
0dz[.]me
jrtz[.]re
3h[.]wf
lgf[.]pw
mnem[.]wf
qmpo[.]art
aij[.]hk
t7[.]nz
6w[.]re
msix[.]pm
r6[.]nz
c4z[.]pl
lwxa[.]eu
mirw[.]wf
mwgq[.]net
1j[.]pm
uqw[.]futbol
n5[.]ms
tz6[.]org
vn6[.]co
gz3[.]nl
u0[.]pm
zbs[.]is
mzjc[.]is
kr4[.]xyz
j4r[.]xyz
gloa[.]in
ri7[.]biz
j68[.]info
0t[.]yt
c7[.]lc
z7s[.]org
w4[.]wf
j4z[.]co
l9b[.]org
jzm[.]pw
euya[.]cn
kjaj[.]top
s8[.]cx
getmyfile[.]click
6y[.]re
getmyfile[.]link
j8[.]si
nt3[.]xyz
k5j[.]one
xjam[.]hk
ue2[.]eu
omzk[.]org

```
b8x[.]org
r4e[.]pl
bpyo[.]in
3e[.]pm
2j4[.]xyz
l5k[.]xyz
skqv[.]eu
w6[.]nz
doem[.]re
k6j[.]pw
yuiw[.]xyz
i49[.]xyz
g4[.]wf
k6c[.]org
p9[.]tel
2yd[.]eu
p3[.]ms
5qw[.]pw
f0[.]tel
k5m[.]co
kj1[.]xyz
kglo[.]link
uoej[.]net
b9[.]pm
oj8[.]eu
egso[.]net
krrz[.]pm
i6n[.]xyz
4q[.]pm
fz[.]ms
trzx[.]eu
q2[.]rs
v0[.]cx
lwip[.]re
m0[.]wf
```

TTPs (ATT&CK)

User Execution: Malicious File (T1204.002
Replication Through Removable Media (T1091)
Compromise Infrastructure: Virtual Private Server (T1584.003)
Windows Management Instrumentation (T1047)
Exfiltration Over C2 Channel (T1041)
Compromise Infrastructure (T1584)

CONFIDENCE
MEDIUM

REFERENCES

- [Intelligence Center] New USB Worm with QNAP C2s
- [Intelligence Center] New DeadBolt ransomware targeting QNAP NAS devices worldwide


SEKOIA.IO
You can now access all FLINT reports and associated IOCs on our SEKOIA.IO Intelligence Center web portal.
https://app.sekoia.io