Quad7 : L'enquête!

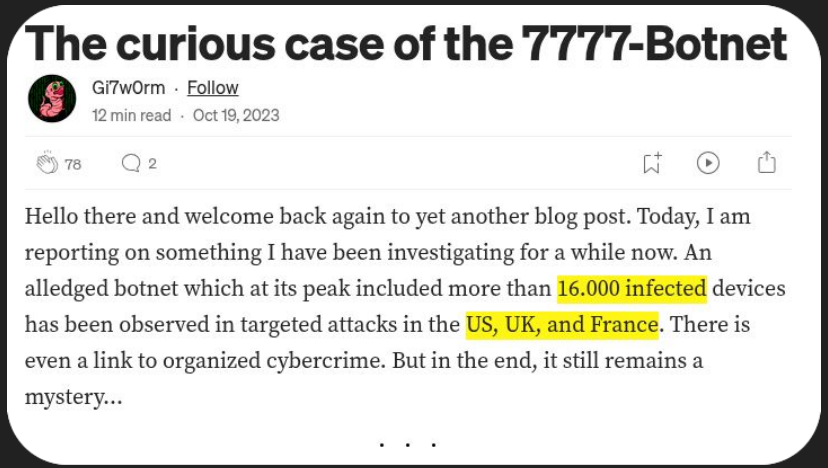
CoRIIN2025

Félix Aimé

Charles Meslay

sekoia

Publication originale



The curious case of the 7777-Botnet

Gi7w0rm · Follow
12 min read · Oct 19, 2023

78 2

Hello there and welcome back again to yet another blog post. Today, I am reporting on something I have been investigating for a while now. An alledged botnet which at its peak included more than 16.000 infected devices has been observed in targeted attacks in the US, UK, and France. There is even a link to organized cybercrime. But in the end, it still remains a mystery...

. . .

Publication originale

The curious case of the 7777-Botnet

Gi7w0rm · Follow
12 min read · Oct 19, 2023

78 2

Hello there and welcome back again to yet another blog post. Today, I am reporting on something I have been investigating for a while now. An alledged botnet which at its peak included more than 16.000 infected devices has been observed in targeted attacks in the US, UK, and France. There is even a link to organized cybercrime. But in the end, it still remains a mystery...

. . .

In recent months an unknown botnet has been observed brute forcing Microsoft Azure instances via Microsoft Azure PowerShell bruteforcing. The botnet has a unique pattern of opening port 7777 on infected devices, returning an "xlogin:" message. The botnet has been used for low-volume attacks against targets of all industry sectors at a global scale, almost exclusively targeting C-Level employee logins. Due to the very low volume of around 2–3 login requests per week, the botnet is able to evade most security

176.96.34.210 (host34-210.toop.pl)

GART-AS (197956) Kujawsko-Pomorskie, Poland

network-administration remote-access

1 Matched Service

11288/SOCKS

1 Other Service

7777/TELNET

Gitw0rm blogpost
Oct 2023

Intrinsec & Devices id.
Feb 2024

Hardware honeypot
Feb & March 2024

Intervention & Blogpost 1
June & July 2024

Blogpost 2
September 2024

...
February 2025

2023 | 2024 | 2025

Publication originale

The curious case of the 7777-Botnet

Gi7w0rm · Follow
12 min read · Oct 19, 2023

78 2

Hello there and welcome back again to yet another blog post. Today, I am reporting on something I have been investigating for a while now. An alledged botnet which at its peak included more than 16.000 infected devices has been observed in targeted attacks in the US, UK, and France. There is even a link to organized cybercrime. But in the end, it still remains a mystery...

. . .

176.96.34.210 (host34-210.toop.pl)

GART-AS (197956) Kujawsko-Pomorskie, Poland

network-administration remote-access

1 Matched Service

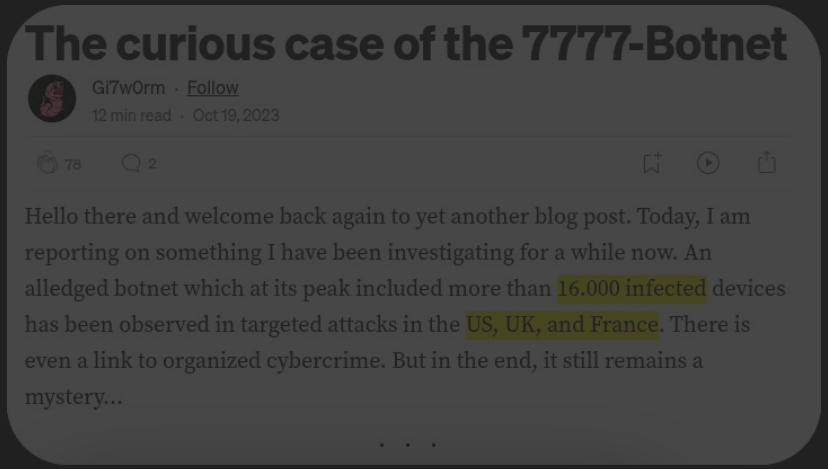
11288/SOCKS

1 Other Service

7777/TELNET

In recent months an unknown botnet has been observed brute forcing Microsoft Azure instances via Microsoft Azure PowerShell bruteforcing. The botnet has a unique pattern of opening port 7777 on infected devices, returning an “xlogin:” message. The botnet has been used for low-volume attacks against targets of all industry sectors at a global scale, almost exclusively targeting C-Level employee logins. Due to the very low volume of around 2–3 login requests per week, the botnet is able to evade most security

Publication originale



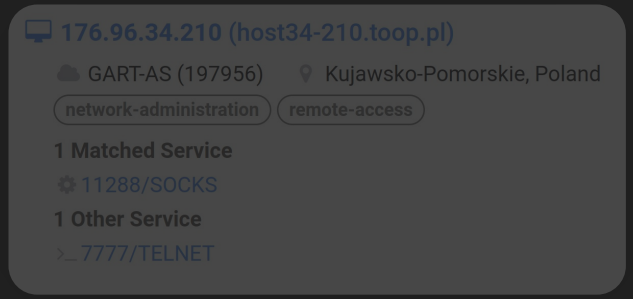
The curious case of the 7777-Botnet

Gi7w0rm · Follow
12 min read · Oct 19, 2023

78 2

Hello there and welcome back again to yet another blog post. Today, I am reporting on something I have been investigating for a while now. An alledged botnet which at its peak included more than 16.000 infected devices has been observed in targeted attacks in the US, UK, and France. There is even a link to organized cybercrime. But in the end, it still remains a mystery...

. . .



176.96.34.210 (host34-210.toop.pl)

GART-AS (197956) Kujawsko-Pomorskie, Poland

network-administration remote-access

1 Matched Service

11288/SOCKS

1 Other Service

7777/TELNET

In recent months an unknown botnet has been observed brute forcing Microsoft Azure instances via Microsoft Azure PowerShell bruteforcing. The botnet has a unique pattern of opening port 7777 on infected devices, returning an “xlogin:” message. The botnet has been used for low-volume attacks against targets of all industry sectors at a global scale, almost exclusively targeting C-Level employee logins. Due to the very low volume of around 2–3 login requests per week, the botnet is able to evade most security

Gitw0rm blogpost
Oct 2023

Intrinsec & Devices id.
Feb 2024

Hardware honeypot
Feb & March 2024

Intervention & Blogpost 1
June & July 2024

Blogpost 2
September 2024

...
February 2025

2023 | 2024 | 2025

Publication originale

The curious case of the 7777-Botnet

Gi7w0rm · Follow
12 min read · Oct 19, 2023

78 2

Hello there and welcome back again to yet another blog post. Today, I am reporting on something I have been investigating for a while now. An alledged botnet which at its peak included more than 16.000 infected devices has been observed in targeted attacks in the US, UK, and France. There is even a link to organized cybercrime. But in the end, it still remains a mystery...

. . .

In recent months an unknown botnet has been observed brute forcing Microsoft Azure instances via Microsoft Azure PowerShell bruteforcing. The botnet has a unique pattern of opening port 7777 on infected devices, returning an “xlogin:” message. The botnet has been used for low-volume attacks against targets of all industry sectors at a global scale, almost exclusively targeting C-Level employee logins. Due to the very low volume of around 2–3 login requests per week, the botnet is able to evade most security

176.96.34.210 (host34-210.toop.pl)

GART-AS (197956) Kujawsko-Pomorskie, Poland

network-administration remote-access

1 Matched Service

11288/SOCKS

1 Other Service

>_ 7777/TELNET

Among others, we identified HKVision software, Software related to TP-Link Routers, and Dahua digital video recorders. One of the most affected devices seems to be the TL-WR841N router which accounts for most of the infected devices in Bulgaria. We were able to identify that one of Bulgaria’s largest

Gitw0rm blogpost
Oct 2023

Intrinsec & Devices id.
Feb 2024

Hardware honeypot
Feb & March 2024

Intervention & Blogpost 1
June & July 2024

Blogpost 2
September 2024

...
February 2025

2023 | 2024 | 2025

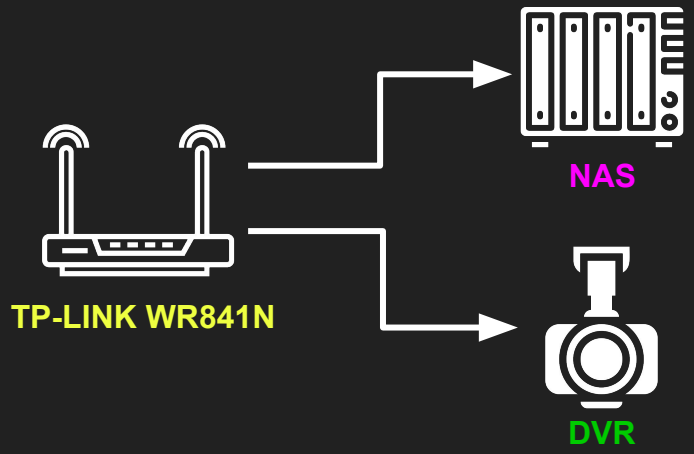
Liste de questions

> Quels appareils sont compromis ?
> Comment sont-ils compromis ?
> Quelles sont les finalités de “xlogin” et du proxy socks ?
> Comment ce botnet est administré ?
> D’autres campagnes sont-elles liées cet acteur ?

Identification des appareils compromis

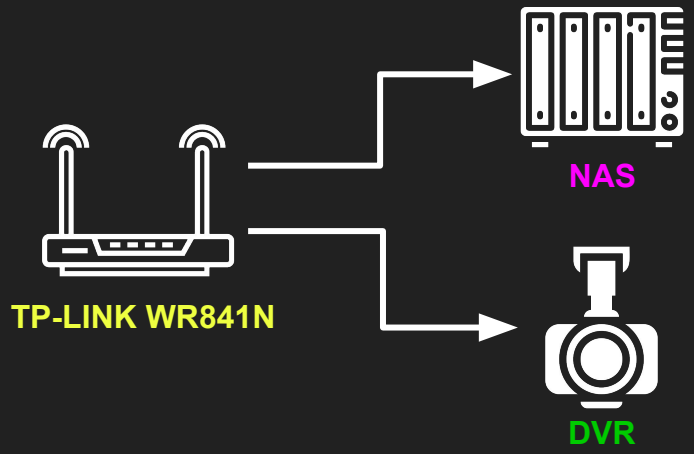
Identification des appareils

Ports
80 : TP-LINK
8443 : NAS
8080 : DVR



Identification des appareils

Ports
80 : TP-LINK
8443 : NAS
8080 : DVR
7777 : Xlogin
11288 : Socks

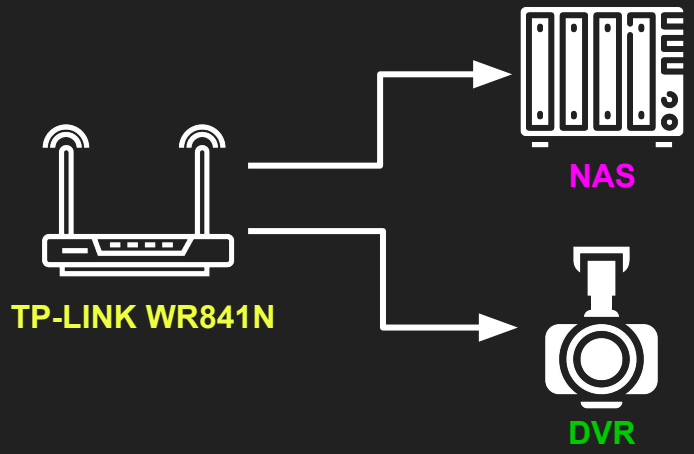


Identification des appareils

La question :

Sur quel appareil **xlogin** et **socks** s'exécutent-ils ?

Ports
80 : TP-LINK
8443 : NAS
8080 : DVR
7777 : Xlogin
11288 : Socks

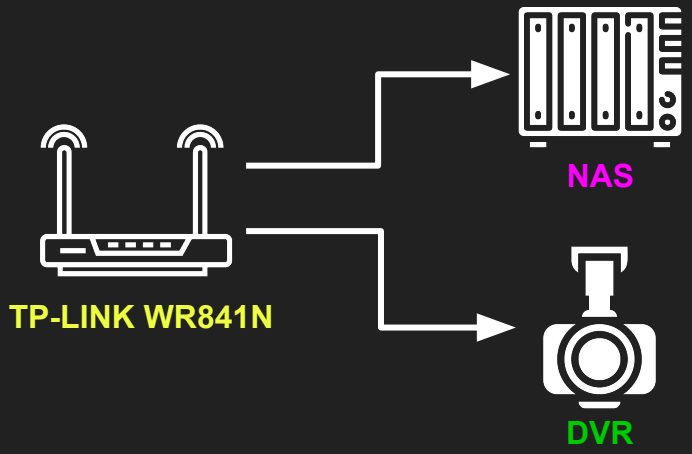


Identification des appareils

La réponse :

Les **tailles de fenêtre TCP des paquets** émis par l'adresse IP distante. Si les ports sont redirigés vers d'autres hôtes, la taille de la fenêtre TCP *peut* différer.

Ports
80 : TP-LINK 5840
8443 : NAS 12600
8080 : DVR 14600
7777 : Xlogin
11288 : Socks

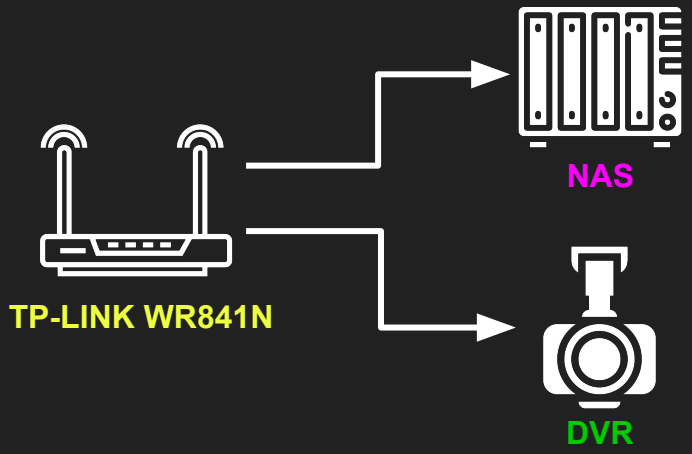


Identification des appareils

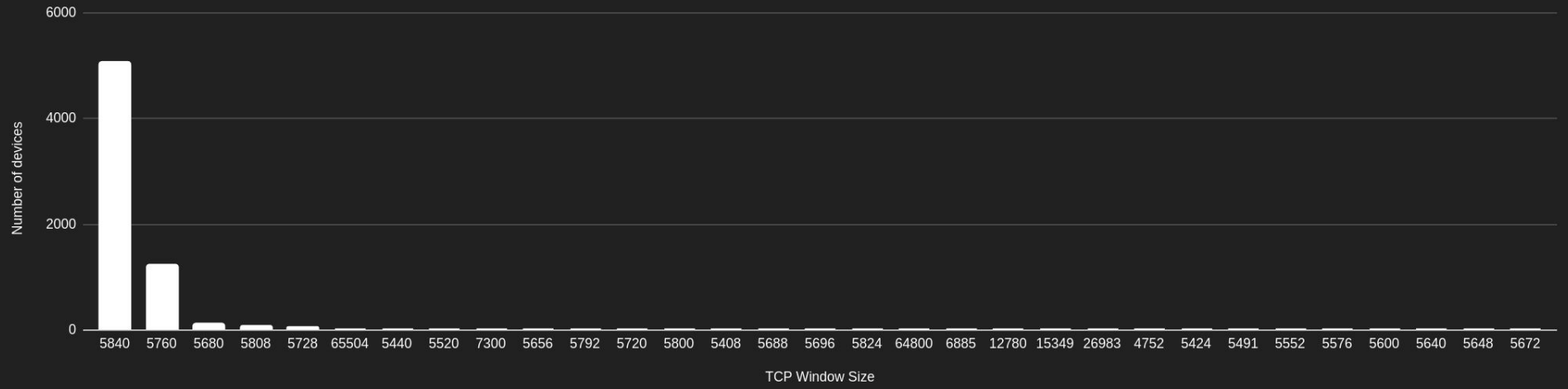
La réponse :

Les **tailles de fenêtre TCP des paquets** émis par l'adresse IP distante. Si les ports sont redirigés vers d'autres hôtes, la taille de la fenêtre TCP *peut* différer.

Ports
80 : TP-LINK 5840
8443 : NAS 12600
8080 : DVR 14600
7777 : Xlogin 5840
11288 : Socks 5840



Analyse des tailles de fenêtre de 6763 appareils compromis



Gitw0rm blogpost
Oct 2023

Intrinsec & Devices id.
Feb 2024

Hardware honeypot
Feb & March 2024

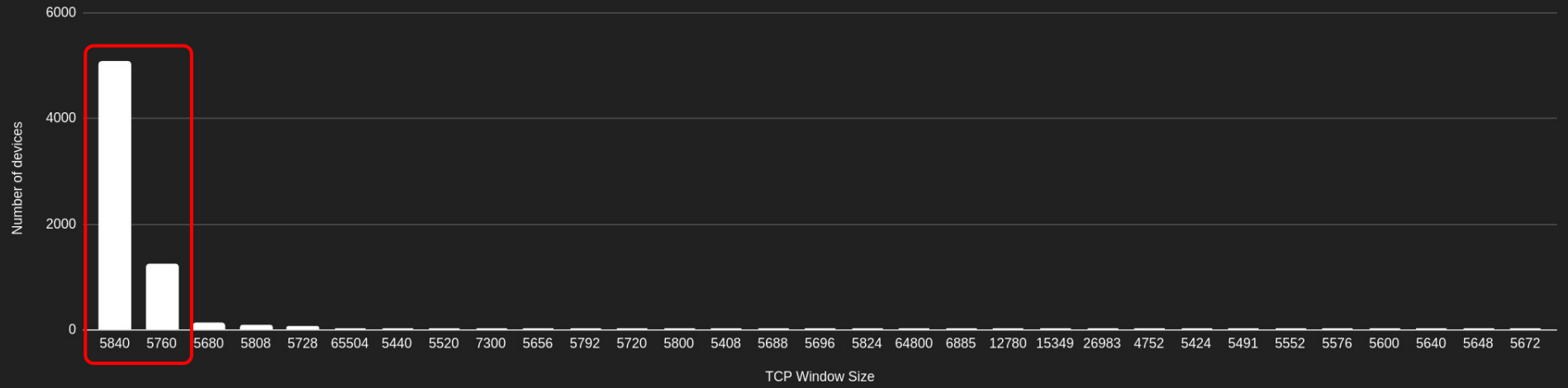
Intervention & Blogpost 1
June & July 2024

Blogpost 2
September 2024

...
February 2025

2023 | 2024 | 2025

Analyse des tailles de fenêtre de 6763 appareils compromis



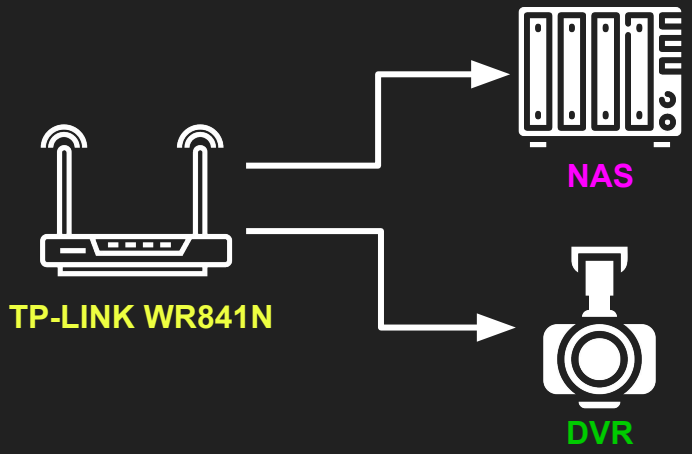
Nos suspects, des routeurs TP-LINK

Identification des appareils

La question :

Pourquoi certains ont parlé de NAS et de DVR ?

Ports
80 : TP-LINK 5840
8443 : NAS 12600
8080 : DVR 14600
7777 : Xlogin 5840
11288 : Socks 5840



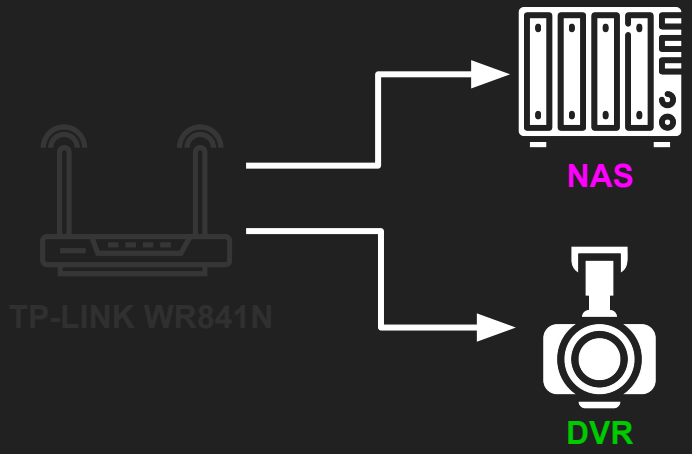
Identification des appareils

La réponse :

Les opérateurs éteignent l'interface d'administration après avoir compromis le routeur.

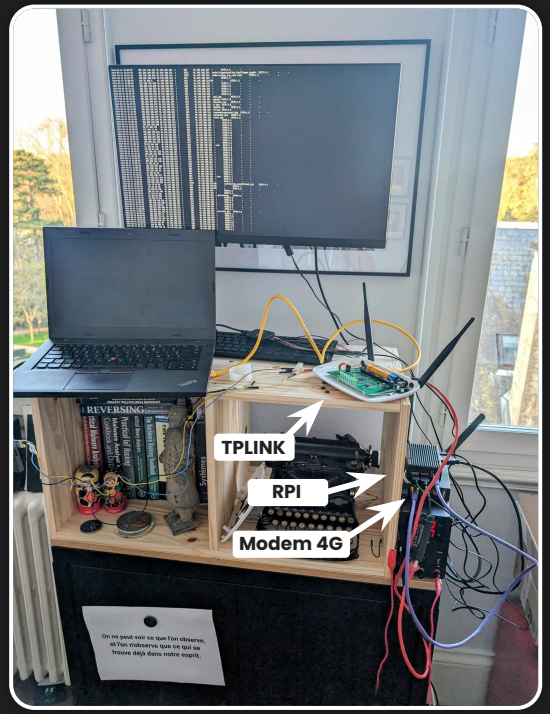
Ports

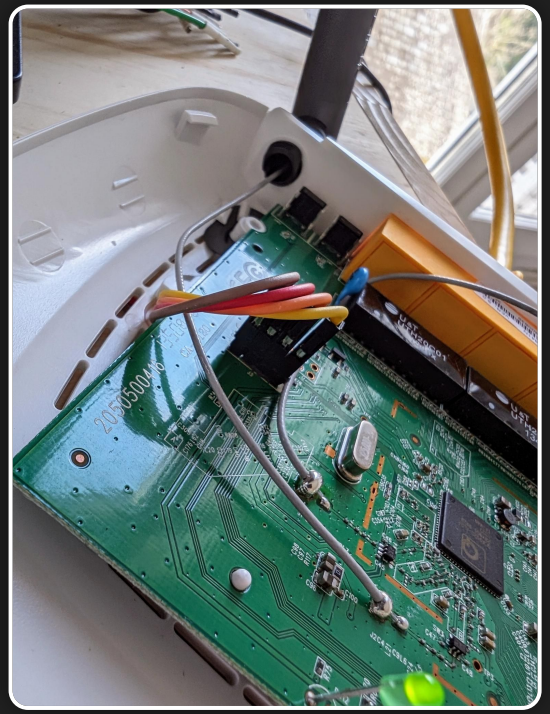
80 : TP-LINK 5840
8443 : NAS 12600
8080 : DVR 14600
7777 : Xlogin 5840
11288 : Socks 5840

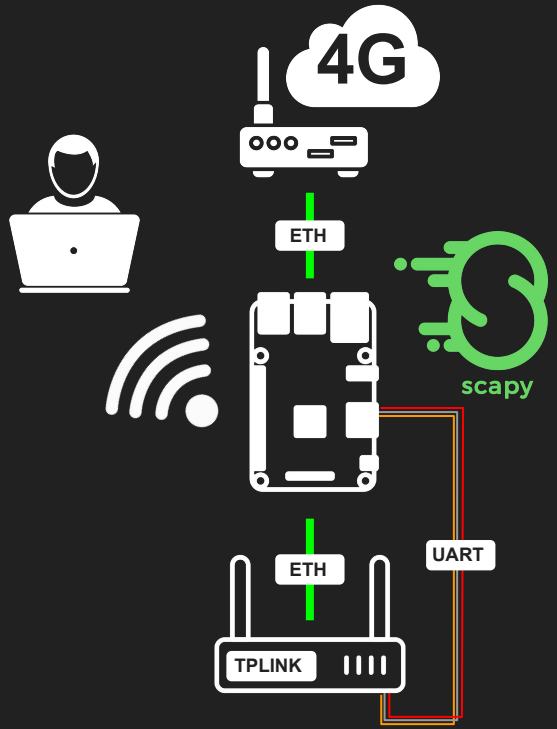


Comment sont-ils compromis?

Hacky-Hardware honeypot







Utilisation de scapy comme “NIDS”

Comme l’administration du routeur écoute sur HTTP, on a utilisé scapy sur notre sonde réseau pour:

- **Etre alerté** d’une tentative d’exploitation.
- **Aider l’attaquant** en changeant son mot de passe par le bon lors de ses tentatives de connexion.

```
        bytes_pkt = pkt[Raw].load

        if b"/      /" in bytes_pkt or b"/           " in bytes_pkt:

            message = "### Arbitrary file disclosure attempt\n"
            message = message + "IP source:" + pkt[IP].src + "\n"
            message = message + "Payload:\n"
            message = message + "```\n"
            message = message + bytes_pkt
            message = message + "```\n"

            headers = { 'Authorization': 'Bearer ;)' }
            to_post = { 'channel_id': "zcaz9jjdjbyqddkig6yw6zpc7e", 'message
            requests.post("https://                              /posts", headers

        if re.match(b"GET /([A-Z]{16}/userRpm/).*", bytes_pkt) and not b"/St

            message = "### Possible exploitation / reco attempt\n"
            message = message + "IP source: `" + pkt[IP].src + "`\n"
            message = message + "Payload:\n"
            message = message + "```\n"
            message = message + bytes_pkt
            message = message + "```\n"

            headers = { 'Authorization': 'Bearer ;)' }
            to_post = { 'channel_id': "zcaz9jjdjbyqddkig6yw6zpc7e", 'message
            requests.post("https://                              /posts", headers

        pkt[Raw].load = bytes_pkt

try:
    nfqueue = NetfilterQueue()
    nfqueue.bind(0, process_packet)
    nfqueue.run()
except KeyboardInterrupt:
    nfqueue.unbind()
```

Gitw0rm blogpost
Oct 2023

Intrinsec & Devices id.
Feb 2024

Hardware honeypot
Feb & March 2024

Intervention & Blogpost 1
June & July 2024

Blogpost 2
September 2024

...
February 2025

2023 | 2024 | 2025

Utilisation d'UART

Nous avons utilisé UART pour superviser des modifications sur le système :

- **L'ajout et la modification de fichiers** sous `/tmp/` à l'aide d'un simple `ls -al` récursif.
- **Supervision des processus exécutés** par un simple `ps`.

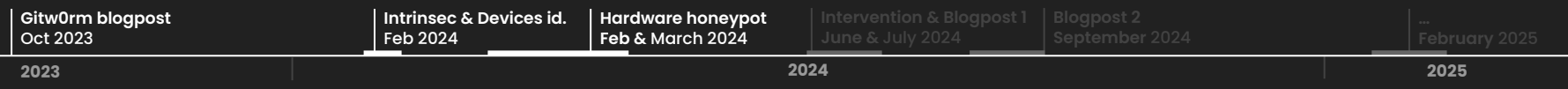
```python
ser = serial.Serial(
    port='/dev/ttyUSB0',
    baudrate=115200,
    timeout=1
)

if ser.isOpen():
    while True:
        command = f'ps -aux\n'.encode()
        ser.write(command)
        time.sleep(.3)
        response = ser.read_all()

        lines = response.decode("utf8").strip().split("\n")
        commands = []
        for line in lines:
            parts = line.split(maxsplit=4)
            if len(parts) == 5:
                command = parts[4]
                commands.append(command)

        commands = list(set(commands))
```


GET 46.149.108.124 /loginFs/passwd HTTP/1.1
GET 46.149.108.124 /loginFs/dropbear/dropbearpwd HTTP/1.1
GET 46.149.108.124 /userRpm/LoginRpm.htm?Save=Save HTTP/1.1
GET 46.149.108.124 /KOPMURFBCLSABMGB/userRpm/ParentCtrlRpm.htm?Del=0&Page=1 HTTP/1.1
GET 46.149.108.124 /loginFs/1 HTTP/1.1
GET 46.149.108.124 /loginFs/3 HTTP/1.1

Bonjour Enigmatic DropBear !

Unauth. Remote file disclosure + Auth. cmd. injection.
(Maintenant connue sous la CVE-2023-44447)

Lancement de dropbear.
Transfert de busybox, et… rien d'autre.



Après trois mois d'attente...

Pas de traces de Quad7.

Pourquoi ?

Les opérateurs ne semblent pas mettre à jour leur liste de cibles avec de nouvelles adresses IP.

Plan B: Aller chez une victime.

Gitw0rm blogpost
Oct 2023

Intrinsec & Devices id.
Feb 2024

Hardware honeypot
Feb & March 2024

Intervention & Blogpost 1
June & July 2024

Blogpost 2
September 2024

...
February 2025

2023 | 2024 | 2025

Plan B: Aller chez une victime.

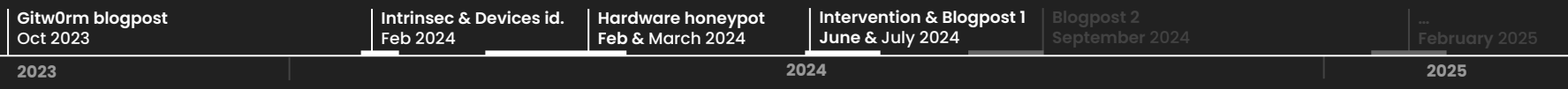
> Trouver et convaincre une victime en France ;

Plan B: Aller chez une victime.

> Trouver et convaincre une victime en France ;
> Mettre une sonde réseau devant son routeur ;

Plan B: Aller chez une victime.

> Trouver et convaincre une victime en France ;
> Mettre une sonde réseau devant son routeur ;
> Intervenir pour récupérer les codes malveillants.



Identification des victimes

Sur dix victimes en France trois ont été identifiées:

> **La première** identifiée à l'aide d'un site internet pointant vers son routeur. Aucune réponse.

> **La seconde** a transféré notre email à son client… qui ne nous a jamais répondu et a remplacé son routeur.

> **La troisième** était très intéressée par notre investigation et nous a permis d'intervenir chez un de ses clients, youpi.

Sonde réseau

Sonde réseau **plug and play** réalisé à l'aide d'un simple **Raspberry Pi** surveillant les ports:

- 7777 : Xlogin
- 11288 : Socks proxy
- 81 : Administration TP-LINK

```
@reboot /bin/bash -c 'sleep 60 && UUID=$(uuidgen) &&
/usr/bin/tcpdump -i br0 "port 81 or port 7777 or
port 11288" -w /home/tap/capture_${UUID}.pcap -C
1000 -W 10' >> /home/tap/tcpdump.log 2>&1
```

Gitw0rm blogpost
Oct 2023

Intrinsec & Devices id.
Feb 2024

Hardware honeypot
Feb & March 2024

Intervention & Blogpost 1
June & July 2024

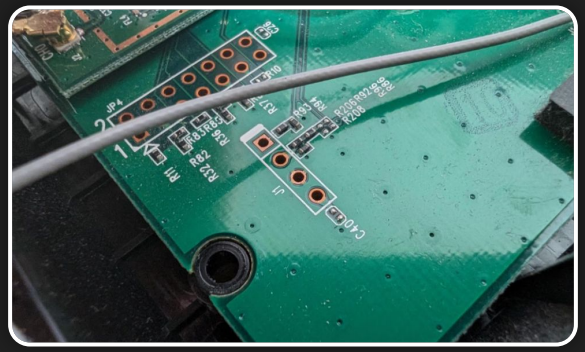
Blogpost 2
September 2024

...
February 2025

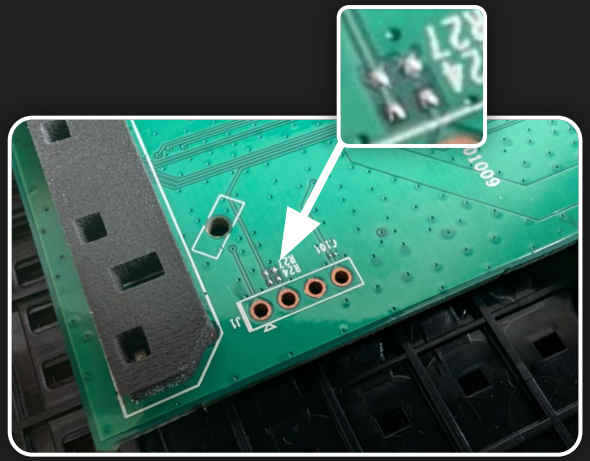
2023 | 2024 | 2025

Préparation

Nous savions que le routeur à investiguer était un **Archer C7**.
Nous avons donc acheté deux routeurs pour nos tests.



Archer C7(EU) version 2.0
(UART authentifié)



Archer C7(EU) version 5.0
(UART non authentifié + RCE via réseau local)

Préparation

Nous avons décidé quelques jours avant l'intervention de développer notre propre "**porte dérobée**".

Le but final était de pouvoir **pré-implanter** le routeur si ce dernier venait à être redémarré durant l'opération afin de récupérer les codes.

```python
import socket
import hashlib
import datetime
import os
import sys

def xor_encrypt_decrypt(data, key):
    return bytes([b ^ (key % 256) for b in data])

def main():

    if len(sys.argv) > 1 and "--rescue" in sys.argv[1]:
        SERVER_PORT = 34321
        BUFFER_SIZE = 1024
        SESSION_FILE = "listener_rescue.log"
    else:
        SERVER_PORT = 23412
        BUFFER_SIZE = 1024
        SESSION_FILE = "listener_default.log"

    server = socket.socket(socket.AF_INET, socket.SOCK_STREAM)
    server.bind(('', SERVER_PORT))
    server.setsockopt(socket.SOL_SOCKET, socket.SO_REUSEADDR, 1)
    server.listen(1)
    print(f"Welcome to the 7777 👻  buster.")

    conn, addr = server.accept()
    print(f"Connection from {addr[0]}")

    try:
        while True:
            # Prevent null command to be sent.
            while True:
```

Gitw0rm blogpost
Oct 2023

Intrinsec & Devices id.
Feb 2024

Hardware honeypot
Feb & March 2024

Intervention & Blogpost 1
June & July 2024

Blogpost 2
September 2024

...
February 2025

2023 | 2024 | 2025

Intervention

Intervention

Default states (ps, dirs...)

Le shell obtenu étant un shell restreint via BusyBox, il ne nous sera malheureusement pas possible de déterminer, via un `netstat` ou un `lsof`, quel processus écoute sur les ports 7777 et 11288. Il est possible de compiler un binaire lsof en MIPS et l'envoyer au routeur pour exécution. A voir si cette stratégie n'est pas trop gourmande en temps.

Si l'on se base uniquement sur les fichiers, nous devrons donc effectuer une comparaison (diff) entre les processus lancés par le routeur compromis et ceux lancés sur un routeur sain.

Voici des images de processus tournants sur un 2.0 et 5.0 et fichiers présents dans le répertoire /tmp/ avec les dates de dernière modification.

> Il est possible que cette simple comparaison ne suffise pas. Cependant, la plupart des menaces IOTs ne cherchent pas à se dissimuler une fois avoir compromis l'IOT.

Archer C7 2.0

```
ps w
  PID  Uid     VmSize Stat Command
    1 root        400 S    init
    2 root            SW<  [kthreadd]
    3 root            SW<  [ksoftirqd/0]
    4 root            SW<  [events/0]
    5 root            SW<  [khelper]
    6 root            SW<  [async/mgr]
    7 root            SW<  [kblockd/0]
    8 root            SW   [pdflush]
    9 root            SW   [pdflush]
   10 root            SW<  [kswapd0]
   11 root            SW<  [aio/0]
   18 root            SW<  [mtdblockd]
   19 root            SW<  [unlzma/0]
   73 root       2952 S    /usr/bin/httpd
   74 root       1808 S    /usr/bin/uclited
   82 root        208 S    ipcserver
   86 root       2952 S    /usr/bin/httpd
   87 root       2952 S    /usr/bin/httpd
  100 root        344 S    syslogd -C -l 7
  104 root        296 S    klogd
  127 root            SW<  [napt_ct_scan]
  278 root        352 S    /sbin/udhcpc -h Archer_C7 -i eth0.2 -p /tmp/wr841n/ud
  279 root        200 S    /sbin/udhcpc -h Archer_C7 -i eth0.2 -p /tmp/wr841n/ud
  283 root        324 S    /usr/sbin/udhcpd /tmp/wr841n/udhcpd.conf
  322 root       2952 S    /usr/bin/httpd
  335 root       2952 S    /usr/bin/httpd
  336 root       2952 S    /usr/bin/httpd
  417 root       2952 S    /usr/bin/httpd
  419 root       2952 S    /usr/bin/httpd
  421 root       2952 S    /usr/bin/httpd
  422 root       2952 S    /usr/bin/httpd
  472 root        548 S    hostapd -B /tmp/topology_ath0.conf
```

Hunting for malicious files and processes

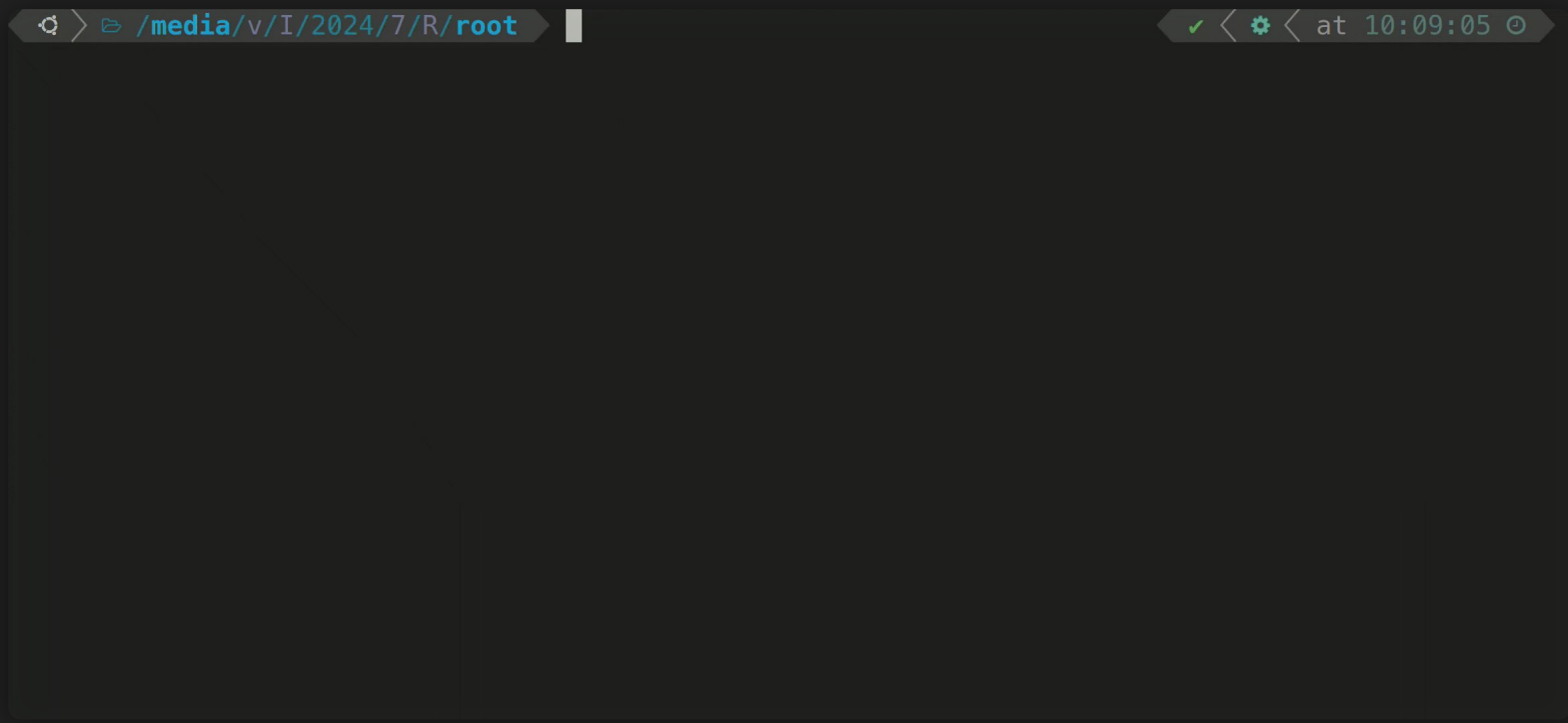
```
ls -al /tmp/
drwxr-xr-x   10 0        0             0 Jul 14 14:21 .
drwxr-xr-x   15 0        0           212 Mar  5  2018 ..
drwxr-xr-x    2 0        0             0 Jan  1  2018 3G
srwxr-xr-x    1 0        0             0 Jan  1  2018 client_dhcp6c
srwxr-xr-x    1 0        0             0 Jan  1  1970 client_dhcpc
srwxr-xr-x    1 0        0             0 Jan  1  1970 client_httpd
-rw-------    1 0        0        106496 Jul 10 18:19 core
----------    1 0        0          1872 Jan  1  1970 dec-model.conf
drwxr-xr-x    2 0        0             0 Jan  1  2018 dev
-rw-r--r--    1 0        0           161 Jan  1  2018 dhcp6c.conf
-rw-r--r--    1 0        0             4 Jan  1  2018 dhcp6c.pid
-rw-r--r--    1 0        0            12 Jan  1  2018 dhcp6c_duid
drwxr-xr-x    2 0        0             0 Jan  1  2018 dropbear
-rw-r--r--    1 0        0            85 Jan  1  2018 hostapd.eap_user
-rw-r--r--    1 0        0            85 Jan  1  2018 hostapd_5G.eap_user
-rw-r--r--    1 0        0             2 Jan  1  2018 httpd_ready
srwxr-xr-x    1 0        0             0 Jan  1  1970 ipc
-rw-r--r--    1 0        0             0 Jan  1  2018 logger.text
srwxr-xr-x    1 0        0             0 Jan  1  2018 manual_handle_card
drwxr-xr-x    2 0        0             0 Jan  1  2018 mediaserver
-rw-r--r--    1 0        0           511 Jan  1  2018 passwd
prw-r--r--    1 0        0             0 Jan  1  2018 pipe_mud89
-rw-r--r--    1 0        0            52 Jan  1  2018 resolv.conf
-rw-r--r--    1 0        0            30 Jan  1  2018 resolv.ipv6.conf
drwxr-xr-x    4 0        0             0 Jan  1  2018 samba
-rwxrwxrwx    1 0        0        114964 Jul 14 14:22 socks5
-rwxrwxrwx    1 0        0        118052 Jul  1 10:23 telnetd
-rw-r--r--    1 0        0          1437 Jan  1  2018 topology_5G_ath1.conf
-rw-r--r--    1 0        0          1437 Jan  1  2018 topology_ath0.conf
drwxr-xr-x    2 0        0             0 Jan  1  2018 usbdisk
drwxr-xr-x    7 0        0             0 Jan  1  2018 vsftp
-rw-r--r--    1 0        0            80 Jan  1  2018 wlanstaticcfg
srwxr-xr-x    1 0        0             0 Jan  1  2018 wpa_ctrl_73-1
srwxr-xr-x    1 0        0             0 Jan  1  2018 wpa_ctrl_73-2
srwxr-xr-x    1 0        0             0 Jan  1  2018 wpa_ctrl_73-3
srwxr-xr-x    1 0        0             0 Jan  1  2018 wpa_ctrl_73-4
drwxr-xr-x    2 0        0             0 Jan  1  2018 wr841n
-rwxrwxrwx    1 0        0         64160 Jul  1 10:24 xlogin
```

```
ps w
  PID  Uid     VmSize Stat Command
    1 root        400 S    init
    2 root            SW<  [kthreadd]
    3 root            SW<  [ksoftirqd/0]
    4 root            SW<  [events/0]
  [...]
   10 root            SW<  [kswapd0]
   11 root            SW<  [aio/0]
   18 root            SW<  [mtdblockd]
   19 root            SW<  [unlzma/0]
   74 root       1808 S    /usr/bin/uclited
   82 root        208 S    ipcserver
  100 root        456 S    syslogd -C -l 7
  104 root        296 S    klogd
  131 root            SW<  [napt_ct_scan]
  291 root        356 S    /sbin/udhcpc -h Archer_C7 -i eth0.2 -p /tmp/wr841n/ud
  292 root        280 S    /sbin/udhcpc -h Archer_C7 -i eth0.2 -p /tmp/wr841n/ud
  296 root        356 S    /usr/sbin/udhcpd /tmp/wr841n/udhcpd.conf
  483 root        840 S    hostapd -B /tmp/topology_ath0.conf
  577 root        836 S    hostapd -B /tmp/topology_5G_ath1.conf
  679 root        348 S    tphotplug -u 2
  691 root        348 S    tphotplug -u 2
  692 root        348 S    tphotplug -u 2
  703 root            SW<  [khubd]
  724 root            SW   [ telnetDBGD ]
  725 root            SW   [ acktelnetDBGD ]
  727 root            SW   [NU TCP]
  728 root            SW   [NU UDP]
  787 root        332 S    /usr/sbin/dnsproxy
  824 root        412 S    /usr/sbin/dhcp6c -c /tmp/dhcp6c.conf -p /tmp/dhcp6c.p
  825 root        208 S    /usr/sbin/dhcp6c -c /tmp/dhcp6c.conf -p /tmp/dhcp6c.p
  827 root        300 S    /usr/bin/lld2d br0 ath0
  847 root        348 S    /usr/bin/dropbear -p 22 -r /tmp/dropbear/dropbear_rsa
 1117 root        124 S    ./telnetd -p 7777 -l /tmp/xlogin
 1131 root        136 S    socks5 -a 0.0.0.0 -u [redacted] -k [redacted] -p 11288
 2181 root        456 R    -sh
 2190 root         64 S    tphotplug -u 2
 2191 root        408 R    ps w
```

Intervention

Rev3rsing

sekoia



Gitw0rm blogpost
Oct 2023

Intrinsec & Devices id.
Feb 2024

Hardware honeypot
Feb & March 2024

Intervention & Blogpost 1
June & July 2024

Blogpost 2
September 2024

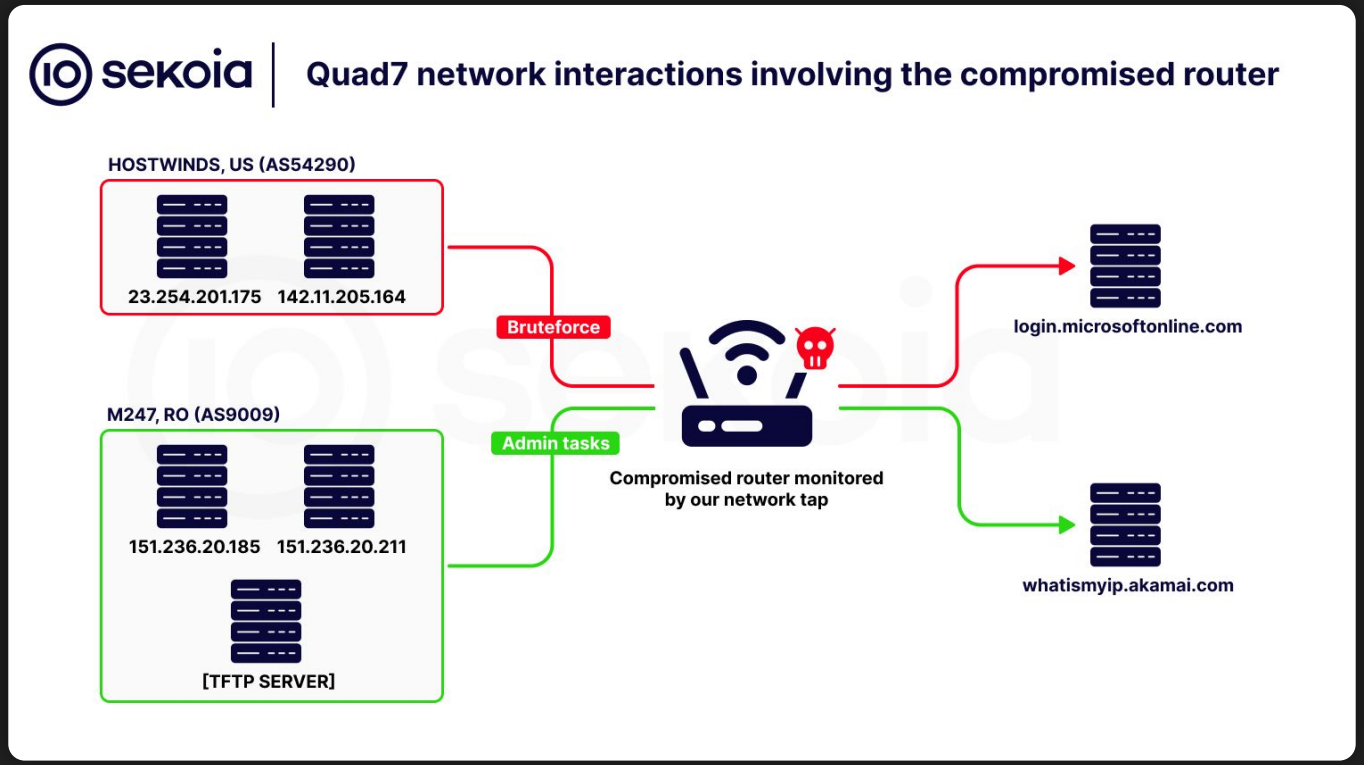
...
February 2025

2023 | 2024 | 2025

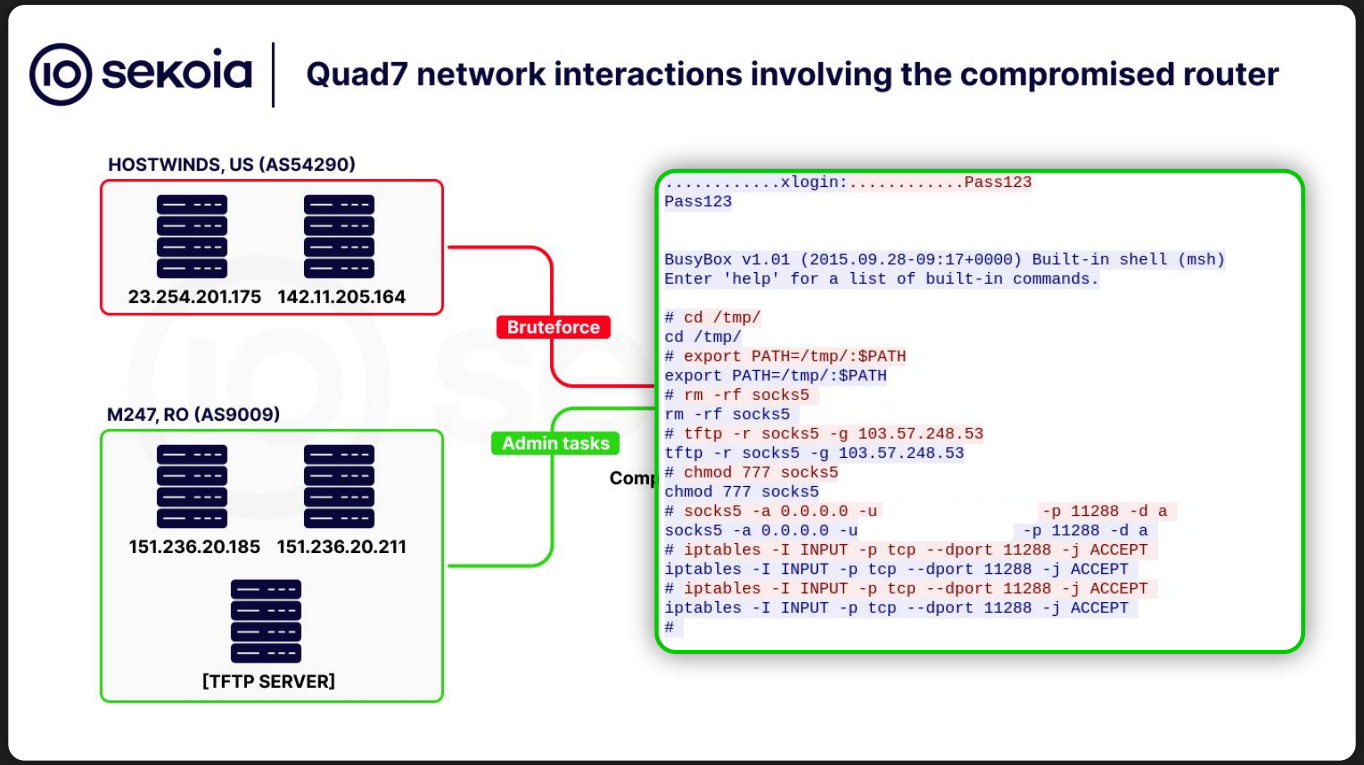
Rev3rsing

```
 %0e
/@%J
0%(D
0$0B
G@#)
@%P@
xlogin:
/bin/sh
/tmp/login
Pass123
(nil)
(null)
hlLjztqZ
npxXoudifFeEgGaACScs
 +0-#'I
Unknown error
 !"-N.Y]Z
#$%&'()*+,234567
;<=>?@ABCDEFGJIMOPQRSTUVWX[\^_`abcxyz{|}~
Success
:
```

Analyse de la capture réseau



Analyse de la capture réseau



La galaxie Quad7

Après une première publication...

[Redacted]

alogin :
ff17e9bc[...]8a35b2c

Hébergé sur

Host	Archi	Sample
http://103.57.248.237	/mipsel/	alogin
http://45.77.44.119	/mipsel/	alogin
http://158.247.194.125	/mipsel/	alogin
http://103.140.239.63	/mipsel/	alogin

Quelques pivots...

```
http://[IP]/mips/microso
http://[IP]/arm/microso
http://[IP]/mipsel/microso
http://[IP]/mips/rlogin
http://[IP]/mips/alogin
http://[IP]/arm/alogin
http://[IP]/mipsel/alogin
http://[IP]/Ruckus/fsy.bin
http://[IP]/asus/netd
http://[IP]/ASUS/arm/netd
http://[IP]/ASUS/mipsel/netd
http://[IP]/ASUS/netd
```

Quelques pivots...

```
http://[IP]/mips/microso
http://[IP]/arm/microso
http://[IP]/mipsel/microso
http://[IP]/mips/rlogin
http://[IP]/mips/alogin
http://[IP]/arm/alogin
http://[IP]/mipsel/alogin
http://[IP]/Ruckus/fsy.bin
http://[IP]/asus/netd
http://[IP]/ASUS/arm/netd
http://[IP]/ASUS/mipsel/netd
http://[IP]/ASUS/netd
```

+ Scan d'AS + Brute Force d'URL

Quelques pivots...

```
http://[IP]/mips/microso
http://[IP]/arm/microso
http://[IP]/mipsel/microso
http://[IP]/mips/rlogin
http://[IP]/mips/alogin
http://[IP]/arm/alogin
http://[IP]/mipsel/alogin
http://[IP]/Ruckus/fsy.bin
http://[IP]/asus/netd
http://[IP]/ASUS/arm/netd
http://[IP]/ASUS/mipsel/netd
http://[IP]/ASUS/netd
```

```
103.57.248.237
 45.77.44.119
158.247.194.125
103.140.239.63
```

4 Serveurs sur VT

```
158.247.194.125
 45.77.44.119
151.236.20.30
103.140.239.63
103.57.248.202
151.236.20.171
103.57.248.237
103.57.248.63
```

8 Servers après notre scan

http://[IP]/arm/xargs
http://[IP]/arm/tcpdump
http://[IP]/arm/nohup
http://[IP]/arm/load
http://[IP]/arm/curl

Utilitaires

http://[IP]/mips/rlogin
http://[IP]/mips/alogin
http://[IP]/arm/rlogin
http://[IP]/mipsel/alogin
http://[IP]/mipsel/rlogin
http://[IP]/arm/alogin

***login bind shells**

http://[IP]/test
http://[IP]/mips/m
http://[IP]/main

Reverse shell

http://[IP]/arm/kill.sh
http://[IP]/arm/tcpdump.sh
http://[IP]/archive.tgz
http://[IP]/r.sh
http://[IP]/c.php
http://[IP]/f.php
http://[IP]/exec.sh

Fichiers attaquant

http://[IP]/ASUS/arm/netd
http://[IP]/ASUS/mipsel/netd
http://[IP]/ASUS/netd

Netd implant

http://[IP]/Ruckus/fsy.bin
http://[IP]/fsy.bin

Fsy implant

sekoia

Gitw0rm blogpost
Oct 2023

Intrinsec & Devices id.
Feb 2024

Hardware honeypot
Feb & March 2024

Intervention & Blogpost 1
June & July 2024

Blogpost 2
September 2024

...
February 2025

2023 | 2024 | 2025

Netd

Permet de rejoindre un réseau de confiance basé sur **cjdns**

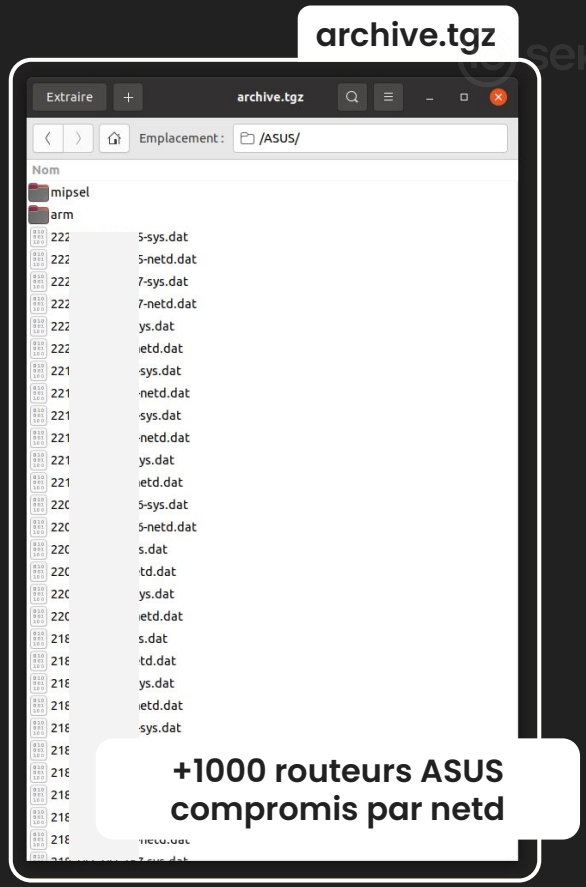
cjdns:
- Projet open source
- réseau IPv6, UDP
- chiffré et décentralisé

Rôle de netd :
- générer le matériel cryptographique
- envoi des informations au C2 pour rejoindre le réseau de confiance

Netd

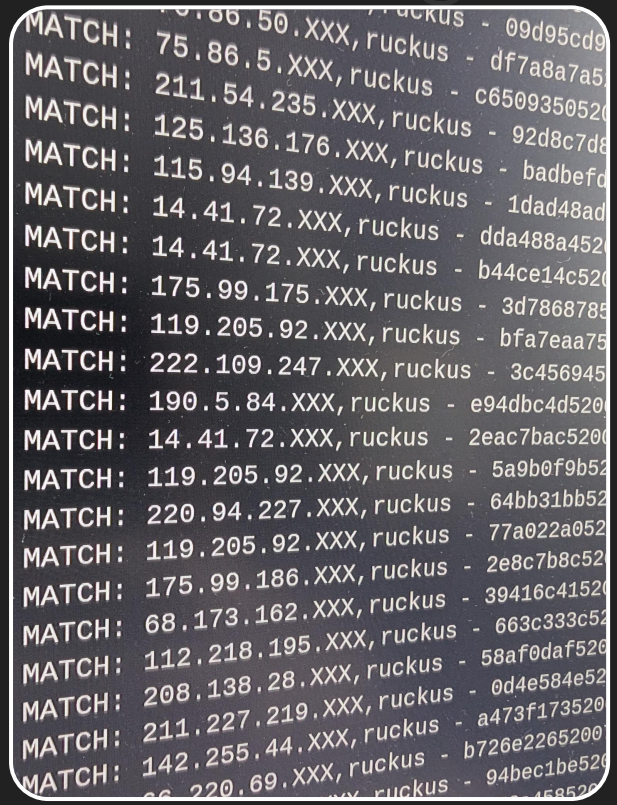
> Récupération d'une archive avec toutes les configurations chiffrées

> +1000 routeurs Asus



Deuxième implant : FSY

- Gestion d'un réseau d'anonymisation
- Création d'un scanner
- Déployé sur des appareils Ruckus



Gitw0rm blogpost
Oct 2023

Intrinsec & Devices id.
Feb 2024

Hardware honeypot
Feb & March 2024

Intervention & Blogpost 1
June & July 2024

Blogpost 2
September 2024

...
February 2025

2023 | 2024 | 2025

Une menace à multiples s/facettes/botnets/g

sekoia

xlogin	alogin	zylogin	rlogin	axlogin	?	?
						
6,003	4,486	8	294	?	?	?
Proxy bindshell	Proxy bindshell netd	Bindshell	Bindshell FsyNet	Not seen ITW	Not seen ITW	Not seen ITW
Bruteforce against M365 VIPs accounts and more broader since June.	Telnet & SSH bruteforce attempts (possibly from another actor)	Unknown	Unknown	Unknown	Unknown	Unknown

Conclusion

Toujours pas d'exploitation observée sur les TP-LINK, mais on a notre petite idée.

Au final, c'était "marrant".

Quad7 un acteur parmi d'autres suivi par Sekoia faisant des réseaux d'ORBs.

Questions ?

Félix Aimé

Charles Meslay

sekoia

Ils sont toujours là ;]

Gitw0rm blogpost
Oct 2023

Intrinsec & Devices id.
Feb 2024

Hardware honeypot
Feb & March 2024

Intervention & Blogpost 1
June & July 2024

Blogpost 2
September 2024

...
February 2025

2023 | 2024 | 2025

Questions ?

Félix Aimé

Charles Meslay

sekoia