ANATOMIE D'UNE FORTISSION

TLP:GREEN PAP:GREEN

Origine


Why is it, when something happens, It is always you three?
Citrix Fortinet Ivanti
imgflip.com

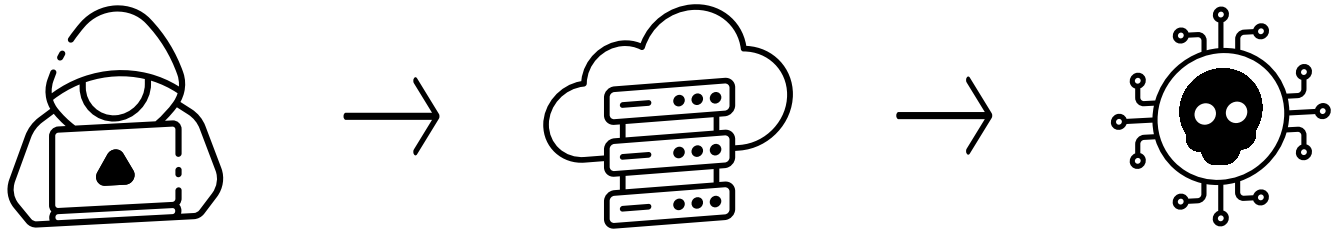
Fortission?

Fortission

nom féminin

(latin *fortis, -tionis*)

1. Fait de se faire compromettre son SI à partir d'une vulnérabilité d'un équipement Fortinet.

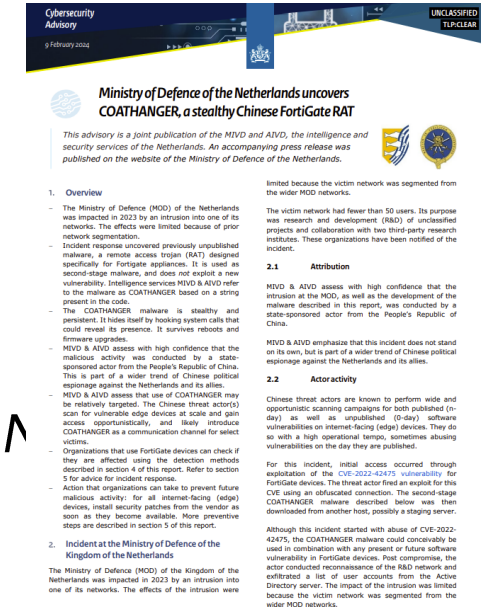


Forensic ?

- Peu de ressources disponibles
  - https://github.com/JSCU-NL/COATHANGER
  - PDF *"Ministry of Defence of the Netherlands uncovers COATHAN Chinese FortiGate RAT"*

- Pas d'outils

- Pas de génération de bundle de logs comme sur d'autres éditeurs


Cybersecurity Advisory

9 February 2024

UNCLASSIFIED TLP:CLEAR

Ministry of Defence of the Netherlands uncovers COATHANGER, a stealthy Chinese FortiGate RAT

This advisory is a joint publication of the MIVD and AIVD, the intelligence and security services of the Netherlands. An accompanying press release was published on the website of the Ministry of Defence of the Netherlands.

1. Overview

- The Ministry of Defence (MOD) of the Netherlands was impacted in 2023 by an intrusion into one of its networks. The effects were limited because of prior network segmentation.
- Incident response uncovered previously unpublished malware, a remote access trojan (RAT) designed specifically for Fortigate appliances. It is used as second-stage malware, and does not exploit a new vulnerability. Intelligence services MIVD & AIVD refer to the malware as COATHANGER based on a string present in the code.
- The COATHANGER malware is stealthy and persistent. It hides itself by hooking system calls that could reveal its presence. It survives reboots and firmware upgrades.
- MIVD & AIVD assess with high confidence that the malicious activity was conducted by a state-sponsored actor from the People's Republic of China. This is part of a wider trend of Chinese political espionage against the Netherlands and its allies.
- MIVD & AIVD assess that use of COATHANGER may be relatively targeted. The Chinese threat actor(s) scan for vulnerable edge devices at scale and gain access opportunistically, and likely introduce COATHANGER as a communication channel for select victims.
- Organizations that use FortiGate devices can check if they are affected using the detection methods described in section 4 of this report. Refer to section 5 for advice for incident response.
- Action that organizations can take to prevent future malicious activity: for all internet-facing (edge) devices, install security patches from the vendor as soon as they become available. More preventive steps are described in section 5 of this report.

2. Incident at the Ministry of Defence of the Kingdom of the Netherlands

The Ministry of Defence (MOD) of the Kingdom of the Netherlands was impacted in 2023 by an intrusion into one of its networks. The effects of the intrusion were limited because the victim network was segmented from the wider MOD networks.

The victim network had fewer than 50 users. Its purpose was research and development (R&D) of unclassified projects and collaboration with two third-party research institutes. These organizations have been notified of the incident.

2.1 Attribution

MIVD & AIVD assess with high confidence that the intrusion at the MOD, as well as the development of the malware described in this report, was conducted by a state-sponsored actor from the People's Republic of China.

MIVD & AIVD emphasize that this incident does not stand on its own, but is part of a wider trend of Chinese political espionage against the Netherlands and its allies.

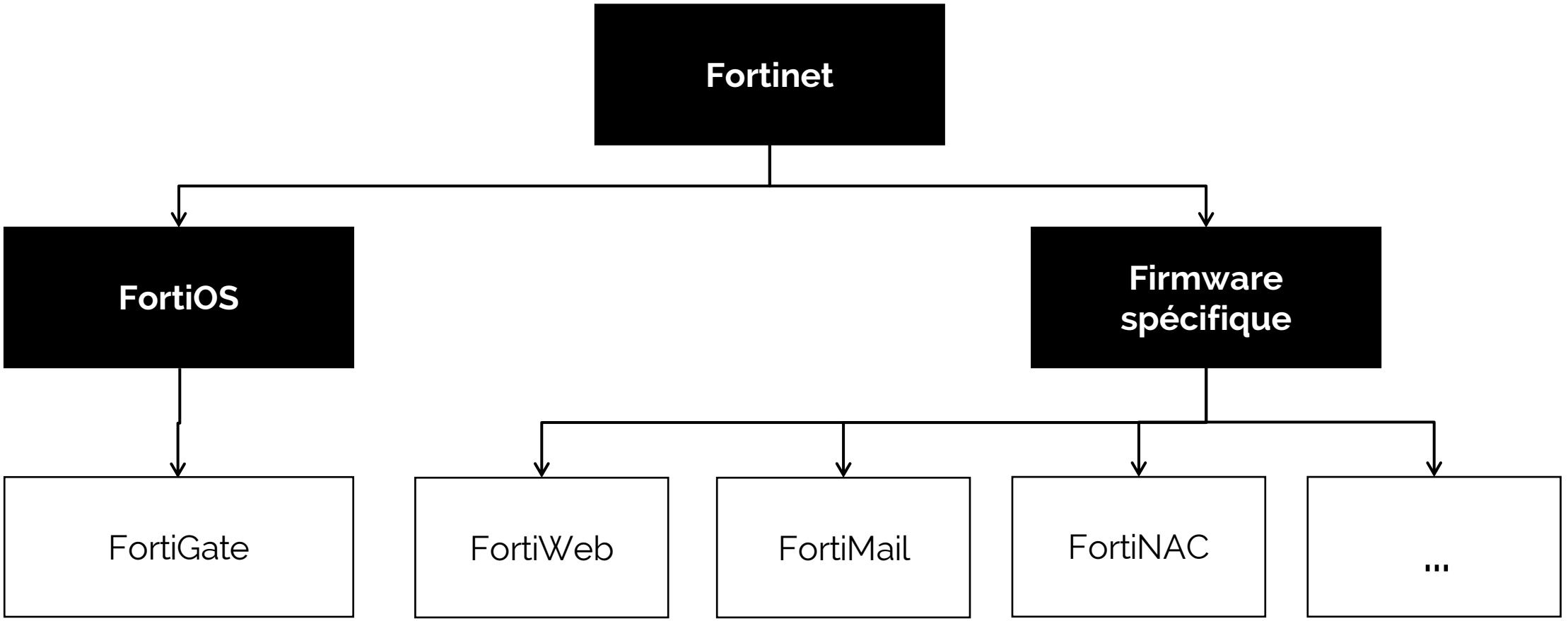
2.2 Actor activity

Chinese threat actors are known to perform wide and opportunistic scanning campaigns for both published (n-day) as well as unpublished (0-day) software vulnerabilities on internet-facing (edge) devices. They do so with a high operational tempo, sometimes abusing vulnerabilities on the day they are published.

For this incident, initial access occurred through exploitation of the CVE-2022-42475 vulnerability for FortiGate devices. The threat actor fired an exploit for this CVE using an obfuscated connection. The second-stage COATHANGER malware described below was then downloaded from another host, possibly a staging server.

Although this incident started with abuse of CVE-2022-42475, the COATHANGER malware could conceivably be used in combination with any present or future software vulnerability in FortiGate devices. Post compromise, the actor conducted reconnaissance of the R&D network and exfiltrated a list of user accounts from the Active Directory server. The impact of the intrusion was limited because the victim network was segmented from the wider MOD networks.

Système d'exploitation



Les commandes natives disponibles depuis la CLI sont différentes en fonction du système


COLLECTE

Collecte : 3 cas d'architecture

Appliance physique

Dump des disques impossibles ✗
Analyse « live » ✓

Appliance virtuelle interne

Dump des disques durs ✓
Analyse « live » ✓

Appliance virtuelle Cloud (licence)

Dump partielle des disques ✗
Analyse « live » ✓

Lab (Trial)

Collecte : cas virtuel interne

- VM interne sur Proxmox / ESXi / …

1. Créer un snapshot
2. Copier le disque dur virtuel
3. Exporter le disque pour analyse (.raw…)

Collecte : cas virtuel externe (licence)

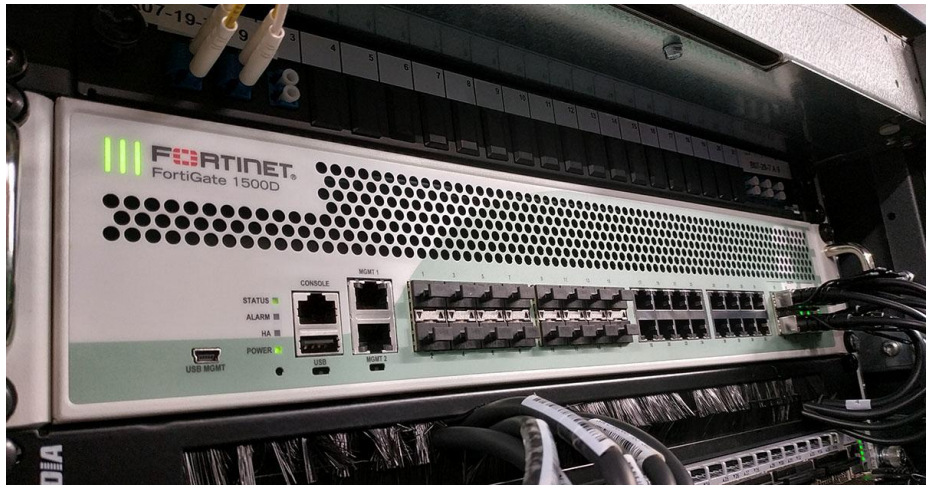
- VM type cloud public (AWS)

1. Créer un snapshot EBS
2. Créer un nouveau volume EBS à partir du snapshot
3. Attacher le volume à une VM d'investigation

Problème : la VM est basée sur un AMI officielle propriétaire. Le disque principal ne peut pas être rattachée à une autre VM.

Seul le disque secondaire (type `/data`) sera accessible

Collecte : cas physique



Source photo : ate[.]info

ANALYSE

Analyse : artefacts importants

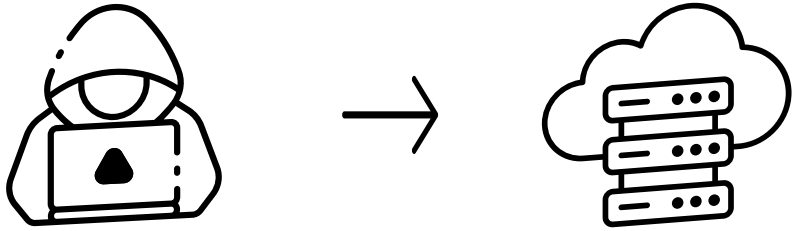
Accès au disque

« Analyse serveur Linux »

Hunt en live

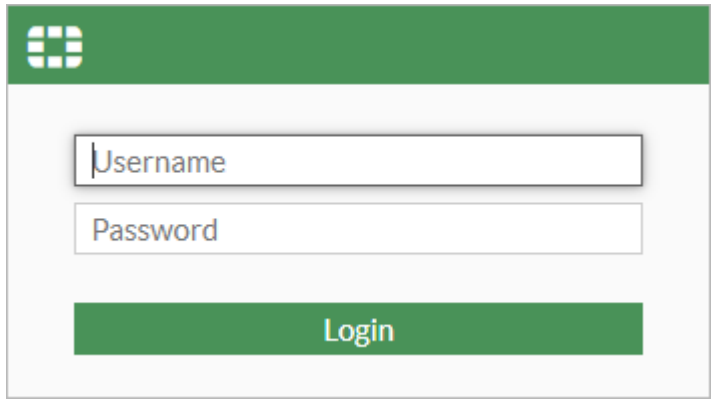
Récupération de données en live sur le système

Artefacts disque : serveur web



```
- [24/Jul/2025:02:11:46 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 19188us
- [24/Jul/2025:02:11:46 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 12352us
- [24/Jul/2025:02:11:46 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 2784us
- [24/Jul/2025:02:11:47 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 4354us
- [24/Jul/2025:02:11:47 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 5171us
- [24/Jul/2025:02:11:47 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 3222us
- [24/Jul/2025:02:11:47 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 2869us
- [24/Jul/2025:02:11:47 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 3968us
- [24/Jul/2025:02:11:47 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 5462us
- [24/Jul/2025:02:11:47 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 1889us
- [24/Jul/2025:02:11:47 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 8589us
- [24/Jul/2025:02:11:47 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 11379us
- [24/Jul/2025:02:11:47 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 2797us
- [24/Jul/2025:02:11:47 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 3595us
- [24/Jul/2025:02:11:47 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 4854us
- [24/Jul/2025:02:11:47 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 3143us
- [24/Jul/2025:02:11:47 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 2811us
- [24/Jul/2025:02:11:47 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 3699us
- [24/Jul/2025:02:11:47 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 3532us
- [24/Jul/2025:02:11:48 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 2852us
- [24/Jul/2025:02:11:48 -0700] "GET /api/fabric/device/status HTTP/1.1" 401 -B 2723us
- [24/Jul/2025:02:11:48 -0700] "GET /cgi-bin/ml-draw.py HTTP/1.1" 500 533B 278881us
- [24/Jul/2025:02:11:48 -0700] "GET /cgi-bin/x.cgi HTTP/1.1" 200 27B 4300us
- [24/Jul/2025:02:11:53 -0700] "GET /cgi-bin/x.cgi HTTP/1.1" 200 -B 3442us
```

Exploitation de la CVE-2025-25257 en août (Fortiweb)



Dossier « /**migadmin** »
➔ *Panel exposé via HTTP(s)*

Artefacts disques : Fichiers de logs

- Commandes*
- Paquets installés*
  - Système
  - Packages Python

Artefacts disque : Fichiers

- Accès aux disques
  - Lister les fichiers
    - Générer la timeline du système de fichiers
      - Fichier / Chemin + Date de création
    - Identifier des créations de fichiers durant la période de compromission potentielle
  - Identifier des fichiers malveillants
    - Générer les hashs (SHA256) des fichiers
    - Comparer avec une base de données (réputation / baselining)

Artefacts live : pas d'accès disque / hunt

- Process

```
diagnose sys top
```

```
fnsysctl ps
```

```
01:36:24 PM up 2 days, 5 hours and 26 minutes
0U, 0N, 0S, 100I, 0WA, 0HI, 0SI, 0ST; 1994T, 892F
          newcli     9358      R <     0.1     0.8    1
       ipshelper     2183      S       0.0     4.5    0
            node     2173      S       0.0     3.5    0
             wad     2219      S       0.0     3.1    0
             wad     2216      S       0.0     2.8    1
         cmdbsvr     2086      S       0.0     2.7    0
             wad     2217      S       0.0     2.3    0
          cw_acd     2197      S       0.0     2.3    0
 initXXXXXXXXXXX        1      S       0.0     2.2    0
       forticron     2163      S       0.0     2.1    1
             wad     2209      S       0.0     2.0    0
             wad     2174      S       0.0     2.0    0
             wad     2212      S       0.0     1.9    1
            csfd     2201      S       0.0     1.9    0
         miglogd     2263      S       0.0     1.9    0
             wad     2210      S       0.0     1.9    0
           autod     2202      S       0.0     1.9    0
           fgfmd     2196      S       0.0     1.9    1
             wad     2214      S       0.0     1.9    1
         miglogd     2172      S       0.0     1.9    0
```

On peut même dumper un process pour voir les relations avec des fichiers, via `lsof`

```
FortiWeb # diagnose process lsof 31798
COMMAND   PID USER   FD   TYPE             DEVICE SIZE/OFF   NODE NAME
bash    31798 root  cwd    DIR               1,0     4096  15621 /migadmin/cgi-bin
bash    31798 root  rtd    DIR               1,0     4096      2 /
bash    31798 root  txt    REG               1,0  1367712  39204 /bin/bash
bash    31798 root  mem    REG               1,0  1590112  31150 /lib/libc.so.6
bash    31798 root  mem    REG               1,0   287480  33518 /lib/libtinfo.so.6
bash    31798 root  mem    REG               1,0   186224  33582 /lib/ld-linux-x86-64.so.2
bash    31798 root    0r  FIFO              0,9      0t0 260382 pipe
bash    31798 root    1u  unix 0x00000000df10d368      0t0 233045 /var/run/cgisock.3495 type=STREAM
bash    31798 root    2w  FIFO              0,9      0t0  23569 pipe
bash    31798 root    3u  unix 0x00000000ff0e9cd6      0t0  10907 /var/run/init.socket type=DGRAM
bash    31798 root    4u   REG              0,15        4      3 /tmp/cmdb_lock
bash    31798 root    5u   REG              0,15        1      4 /tmp/shm_lock
```

Plus d'informations sur les noms de process : https://community.fortinet.com/t5/FortiGate/Technical-Tip-How-to-list-processes-in-FortiOS/ta-p/195863

Artefacts live : pas d'accès disque / hunt

- Sockets

```
diagnose sys tcpsock
```

The specific version of COATHANGER that this report describes uses the process name `httpsd` to obfuscate itself. Therefore, any suspicious outgoing connections to external IP addresses from a process called `httpsd` is a **strong indicator** of the presence of COATHANGER:

```
<device_IP>:<device_port>-><c2_IP>:<c2_port>-
>state=established err=0 socktype=1 rma=0 wma=0
fma=0 tma=0 inode=<inode> process=<PID>/httpsd
```

```
FortiGate-VM64-KVM # diagnose sys tcpsock
0.0.0.0:10400->0.0.0.0:0->state=listen err=4294961664 socktype=23382400 rma=0 wma=0 fma=0 tma=0 inode=24439 process=2165/authd
0.0.0.0:7810->0.0.0.0:0->state=listen err=4294961664 socktype=23263232 rma=0 wma=0 fma=0 tma=0 inode=25278 process=2219/wad
0.0.0.0:10500->0.0.0.0:0->state=listen err=4294961664 socktype=22952960 rma=0 wma=0 fma=0 tma=0 inode=24445 process=2165/authd
0.0.0.0:135->0.0.0.0:0->state=listen err=22841920 socktype=4294961664 rma=0 wma=0 fma=0 tma=0 inode=25272 process=2219/wad
0.0.0.0:10600->0.0.0.0:0->state=listen err=4294961664 socktype=22682816 rma=0 wma=0 fma=0 tma=0 inode=25209 process=2219/wad
0.0.0.0:10601->0.0.0.0:0->state=listen err=4294961664 socktype=14889408 rma=0 wma=0 fma=0 tma=0 inode=25213 process=2219/wad
0.0.0.0:10602->0.0.0.0:0->state=listen err=0 socktype=0 rma=0 wma=0 fma=0 tma=0 inode=25217 process=2219/wad
0.0.0.0:10603->0.0.0.0:0->state=listen err=0 socktype=0 rma=0 wma=0 fma=0 tma=0 inode=25221 process=2219/wad
0.0.0.0:10604->0.0.0.0:0->state=listen err=0 socktype=0 rma=0 wma=0 fma=0 tma=0 inode=25225 process=2219/wad
0.0.0.0:10700->0.0.0.0:0->state=listen err=0 socktype=0 rma=0 wma=0 fma=0 tma=0 inode=25210 process=2219/wad
0.0.0.0:1004->0.0.0.0:0->state=listen err=0 socktype=0 rma=0 wma=0 fma=0 tma=0 inode=20031 process=2166/foauthd
0.0.0.0:1005->0.0.0.0:0->state=listen err=0 socktype=0 rma=0 wma=0 fma=0 tma=0 inode=25275 process=2219/wad
0.0.0.0:10605->0.0.0.0:0->state=listen err=0 socktype=0 rma=0 wma=0 fma=0 tma=0 inode=25229 process=2219/wad
0.0.0.0:10701->0.0.0.0:0->state=listen err=0 socktype=0 rma=0 wma=0 fma=0 tma=0 inode=25214 process=2219/wad
0.0.0.0:8013->0.0.0.0:0->state=listen err=0 socktype=0 rma=0 wma=0 fma=0 tma=0 inode=22901 process=2189/fsvrd
0.0.0.0:10606->0.0.0.0:0->state=listen err=0 socktype=0 rma=0 wma=0 fma=0 tma=0 inode=25233 process=2219/wad
0.0.0.0:10702->0.0.0.0:0->state=listen err=0 socktype=0 rma=0 wma=0 fma=0 tma=0 inode=25218 process=2219/wad
0.0.0.0:7822->0.0.0.0:0->state=listen err=0 socktype=0 rma=0 wma=0 fma=0 tma=0 inode=25205 process=2219/wad
0.0.0.0:10607->0.0.0.0:0->state=listen err=524293 socktype=0 rma=0 wma=0 fma=0 tma=0 inode=25237 process=2219/wad
0.0.0.0:10703->0.0.0.0:0->state=listen err=0 socktype=0 rma=0 wma=0 fma=0 tma=0 inode=25222 process=2219/wad
```

Artefacts live : pas d'accès disque / hunt

- Lister / Afficher des fichiers

```
fnsysctl ls -la /bin
```

```
fnsysctl cat FILE
```

Limitation suivant l'OS (Forti / Firmware)

- Peu d'arguments
- Pas de récursivité…

Utile pour créer un « mft » like de l'arborescence pour un fortiweb

```
FortiWeb # fnsysctl ls -al /migadmin/angular
drwxr-xr-x   10 0        0       Thu Jul 24 03:23:04 2025          4096 .
drwxr-xr-x   14 0        0       Thu Jul 24 01:10:33 2025          4096 ..
-rw-r--r--    1 0        0       Tue Nov 26 09:58:02 2024         10914 122.78d852b7405d1225.js
-rw-r--r--    1 0        0       Tue Nov 26 09:58:02 2024         13649 3.8688cf0748b125e6.js
-rw-r--r--    1 0        0       Tue Nov 26 09:58:02 2024         40956 3rdpartylicenses.txt
-rw-r--r--    1 0        0       Tue Nov 26 09:58:02 2024          4627 502.5b140694bc6768f4.js
-rw-r--r--    1 0        0       Tue Nov 26 09:58:02 2024           725 508.18221ea269a6f5fd.js
-rw-r--r--    1 0        0       Tue Nov 26 09:58:02 2024         25931 534.2b324030e3937ec4.js
-rw-r--r--    1 0        0       Tue Nov 26 09:58:02 2024         10859 667.3061a699760eed47.js
-rw-r--r--    1 0        0       Tue Nov 26 09:58:02 2024          1113 702.b580eb3b5f822c21.js
-rw-r--r--    1 0        0       Tue Nov 26 09:58:02 2024         14667 772.ec9802159f180811.js
-rw-r--r--    1 0        0       Tue Nov 26 09:58:02 2024        102920 783.eb85bcfea9aacbe7.js
-rw-r--r--    1 0        0       Tue Nov 26 09:58:02 2024          2084 812.835f76059cb15395.js
-rw-r--r--    1 0        0       Tue Nov 26 09:58:02 2024          5014 845.fc1684b24615766d.js
-rw-r--r--    1 0        0       Tue Nov 26 09:58:02 2024          1842 858.1afbb52bad0eae6f.js
-rw-r--r--    1 0        0       Tue Nov 26 09:58:02 2024          9835 933.b926b76e7805b838.js
-rw-r--r--    1 0        0       Tue Nov 26 09:58:02 2024           352 976.1c66a80434d2ea74.js
-rw-r--r--    1 0        0       Tue Nov 26 09:58:02 2024       4308713 app.min.js
-rw-r--r--    1 0        0       Thu Jul 24 03:23:04 2025            33 b.css
-rw-r--r--    1 0        0       Thu Jul 24 03:21:02 2025            33 bootstrap.css
-rw-r--r--    1 0        0       Tue Nov 26 09:58:02 2024          2486 common.e5c363828b6571cf.js
drwxr-xr-x    2 0        0       Tue Nov 26 09:58:02 2024          4096 css
drwxr-xr-x    2 0        0       Tue Nov 26 09:58:02 2024          4096 data
-rw-r--r--    1 0        0       Tue Nov 26 09:58:02 2024           318 favicon.ico
```

Exfiltration de données via le panel web!

Artefacts live : pas d'accès disque / hunt

- Hashs SHA256

Possible de spécifier un chemin spécifique

```
diagnose sys filesystem hash FOLDER
```

```
5395dd6b54581b117f112ad79811f8328ed0bac7c1bd3c4eca80650571b7d53c      /migadmin/service-worker.js.gz
f0cdec2d863b95950d7c601064e0f0f2566afc5a9da374865c7eede161a6507a      /migadmin/runtime.js.gz
3a64ada5dfadf4c3b409a76921bd4c3641fa30aace9bc9743cf12530893c7978      /migadmin/roboto-mono-regular.woff2
82c1ccab584700ea30220d81901b6fa74d6a9ebad5b0bc1862b9934ed6b20470      /migadmin/roboto-mono-light.woff2
6595cc51d2ae9f68114a6b91bcb818fd188f02c3f283b6d6ed004f8f2fa5eed7      /migadmin/rmt_index.html
2b15fd8de721be6949f93d247ddea8a38390caaba0927623da48c6db4fde7c1c      /migadmin/polyfills.js.gz
3d4684d0e06ec7f395b3e59c7eda0e3e60f64888ba7e0a18cba0c04302396633      /migadmin/main.js.gz
f52c7ffc424d50f187a110e60dac015b8f5b937b04019a823c3dfa453a42f559      /migadmin/logout.js.gz
c271b17ea9a4c0f792ad62cb148405ababe16f0dcec0919efbd138fd642f3add      /migadmin/login-redirect.js.gz
c3c0d3f472358aac78455515c4800771426770c22698e2486d39fdb5505634e1      /migadmin/lato-regular.woff2
9194059997d722ec01e41980dffbff03ebe00808b1cdd164a7fd18a561bc312a      /migadmin/lato-light.woff2
8d3ca80fa271e94b0c36cf3053b0f806b7a42bb3395b424c99dc0bd218f0ac20      /migadmin/lato-bold.woff2
d612f1212b452af07f1a5defb2b672e76a91f7139e7499fa48bb9b2b985c22d6      /migadmin/inter-regular.woff2
36b86832422c8b2f8eb7a0de635369c10fcebbeb8d3a0f80edeacf8252bfd6da      /migadmin/inter-light.woff2
c63158babcb7902203ed73476ccf901db34825ea524d4a36a52b5e5f97e1abf7      /migadmin/inter-bold.woff2
03a8dd5579f824642314ec760daf6163d828bfbb4685775257c0632ec77c704d      /migadmin/index.html.gz
de4858be052177a760d6464f2005ed1374ee3d21d542ab2e76cda0158309d345      /migadmin/flag_icons_16x11.png
```

Artefacts live : pas d'accès disque / hunt

- Automatiser les actions via un « wrapper » SSH :
  - Lister les fichiers à la racine
    - Si fichier : ajouté à la liste (chemin/timestamps)
    - Si dossier : lister les fichiers dedans
      - …

- Tips pour stocker la sortie STDOUT de la connexion SSH vers l'instance :

```
ssh user@host | tee output.txt
```

Baselining

- Quels fichiers ont pu être créé par l'attaquant?
  - Se concentrer sur les fichiers inconnus
- Contourner le timestomping
- Utiliser une liste de hashs de fichiers légitimes
  - Pas de référentiel public ☺ bientôt!

Annexes

- COATHANGER
  - Dutch Military Intelligence and Security Service (MIVD) & Dutch General Intelligence and Security Service (AIVD). (2024, February 6). Ministry of Defense of the Netherlands uncovers COATHANGER, a stealthy Chinese FortiGate RAT. Retrieved February 7, 2024.
    - https://attack.mitre.org/software/S1105/
- https://docs.fortinet.com/

PS :

Release	Released	End of Engineering Support	End of Support
7.4	9 months ago (11 May 2023)	Ends in 2 years (11 May 2026)	Ends in 3 years and 8 months (11 Nov 2027)
7.2	1 year and 10 months ago (31 Mar 2022)	Ends in 1 year (31 Mar 2025)	Ends in 2 years and 7 months (30 Sep 2026)
7.0	2 years and 11 months ago (30 Mar 2021)	Ends in 1 month and 6 days (30 Mar 2024)	Ends in 1 year and 7 months (30 Sep 2025)

OWN

PARIS _ RENNES _ TOULOUSE

+33 (0) 805 690 234

contact@**own.security**

WWW.**OWN.SECURITY**