Sécurité réseaux: Etude de cas pratique & simulation en laboratoire technique

APPY Guillaume

LANDRIEU Alexis

CSII2 – 12/2014

isitech
Institut Supérieur d'ingénierie Informatique

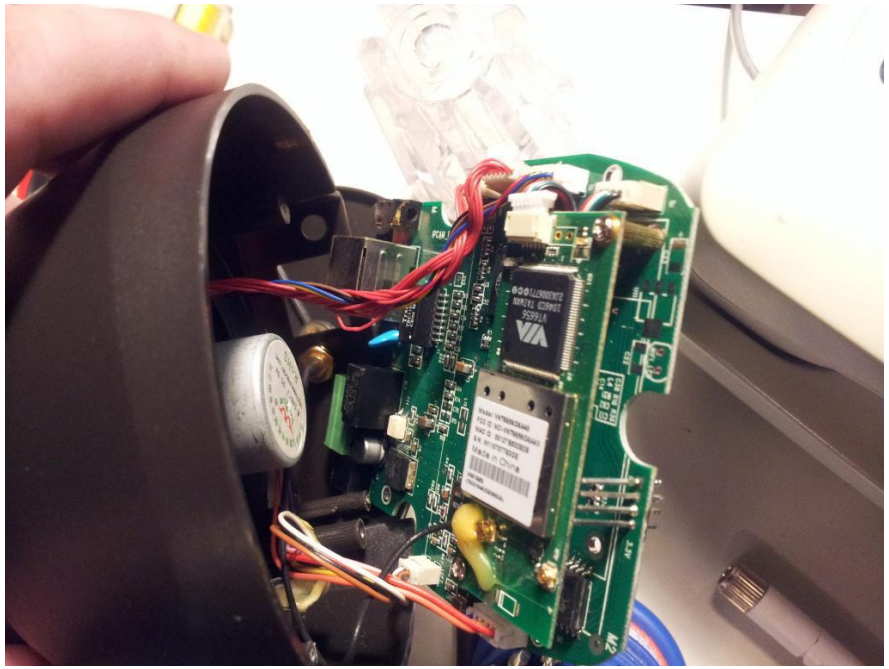
Sommaire

- Quelle victime ?
- Pourquoi ?
- Comment ?
- Démo
- Exploitations possibles
- Statistiques
- Se protéger
- Difficultés rencontrées
- Conclusion

La victime

- Webcam IP rotative
- Motorisation de 300° à l'horizontal, 120°à la verticale.
- Balayages programmables
- Vue nocture, Infrarouge 8m
- Détection mouvements jour/nuit avec envoi alertes en
- Snaphots, upload FTP, email
- Alarmes via MSN
- Wifi, DDNS, ethernet
- Gestion utilisateurs et droits
- Système audio bidirectionel, entrée micro
- Compatible IE et autres navigateurs
- Client Android, IOS

Sous le capot



- Modèle Fl8910W
- ARM Winbond W90N745 revision 1
- 8 MB RAM
- 4 MB Flash
- uCLinux version 2.4.20-uc0
- IPCAM SDK
- Serveur web monolitique spécifique
- Système de fichier: romfs (EPROM)
- Protocoles supportés: HTTP, TCP/IP, UDP, SMTP, PPPoE, Dynamic DNS, UPnP, DNS Client, SNTP, BOOTP, DHCP, FTP
- Serveur Web, RSTP, UPnP et Telnet.

Pourquoi ?

- We can do it !
- Matériel répandu
- Prendre conscience
  - Société de surveillance
  - Dégâts collatéraux possibles
- S’amuser

Comment ?

- Firmware d'origine
- Un OS d'audits: Kali
- Un requêtteur GET: lwp-request (Perl)
- Scripting: Bash
- Firmware du constructeur
- Getcamtool (https://github.com/artemharutyunyan/getmecamtool)
- Foscam_pkmgr(https://github.com/moldov/webui)
- Bruteforcer (http://www.thc.org/thchydra/)

Démonstration

1. Le Front
2. IP de la victime
3. Vérification version
4. Dump de la RAM du CGI via GET
5. Analyse du dump, extraction ID, PWD
6. PROFIT !

7. Création firmware avec backdoor
8. Upload du firmware
9. PROFIT²

Mise en place d'une Backdoor

- Installation d'un Firmware modifié :
  - Outils :
    - Getcamtool (https://github.com/artemharutyunyan/getmecamtool)
    - Foscam_pkmgr(https://github.com/moldov/webui)
  - Firmware FOSCAN :
    - http://www.foscam.co.za/content/25-latest-firmware-updates

Mise en place d'une Backdoor

- Commande d'extraction du binaire :
  - root@debian:/tmp/getmecamtool/build/bin# ./sysextract -x ../../../Firmware/11.22.2.47/System\ firmware/lr_cmos_11_22_2_47.bin -o /tmp/TEMPBINSYS
    ```
    System firmware file has valid structure
    linux.bin size: 759609 bytes, romfs.img size: 1041408 bytes
    Extracting /tmp/TEMPBINSYS/linux.bin(759609 bytes)...
    Extracting /tmp/TEMPBINSYS/romfs.img(1041408 bytes)…
    ```
- Montage de l'image Système :
  - root@debian:/tmp/TEMPBINSYS# ls -lh
    ```
    total 1,8M
    -rw-r--r-- 1 root root  742K déc.   3 22:33 linux.bin
    -rw-r--r-- 1 root root 1017K déc.   3 22:33 romfs.img
    ```
  - root@debian:/tmp/TEMPBINSYS# mount romfs.img /media/romCustom/
  - root@debian:/media/romCustom# ls -lh
    ```
    total 0
    drwxr-xr-x 1 root root 32 janv.  1  1970 bin
    drwxr-xr-x 1 root root 32 janv.  1  1970 dev
    drwxr-xr-x 1 root root 32 janv.  1  1970 etc
    drwxr-xr-x 1 root root 32 janv.  1  1970 flash
    drwxr-xr-x 1 root root 32 janv.  1  1970 home
    drwxr-xr-x 1 root root 32 janv.  1  1970 proc
    drwxr-xr-x 1 root root 32 janv.  1  1970 swap
    drwxr-xr-x 1 root root 32 janv.  1  1970 tmp
    drwxr-xr-x 1 root root 32 janv.  1  1970 usr
    drwxr-xr-x 1 root root 32 janv.  1  1970 var
    ```

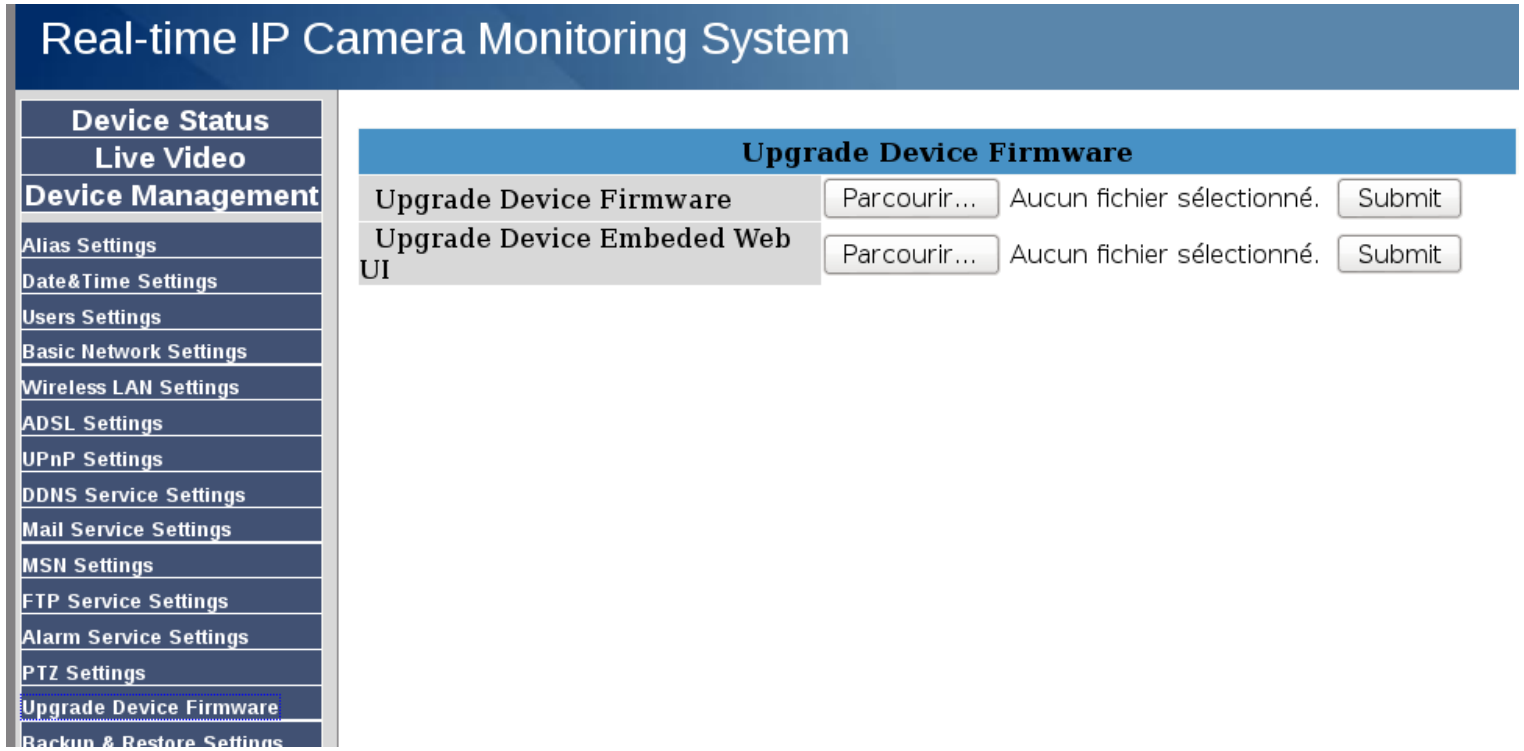
Mise en place d'une Backdoor

- Commande Installation :
  - root@debian::/tmp/NETWORK_TEST/getmecamtool/scripts# ./getmecamtool -h

```
A script for demonstrating the work of camtool utilities
Usage: ./getmecamtool -c <cmd> [OPTIONS]
OPTIONS:
    -c <cmd> command (availble commands are host_file inject_exec
inject_proxy poison_webui)
    -a <addr> address of the camera
    -u <username> username for accessing the camera
    -p <password> password for accessing the camera
    -e <exec> absolute path to executable file for injecting to the
camera
    -k <args> arguments with which the executable has to run
    -s <path> path to system firmware library folder
    -i <inject username> username to create on the camera
    -l <inject password> password for the new username
    -w <webui patch> absolute path to the Web UI patch file
    -f <file> absolute path to the file for hosting on the camera
    -o <new port> new port the camera firmware should listen on
    -h display this message
```

Mise en place d’une Backdoor

- Upload le nouveau Firmware sur la caméra :



Exploitations possibles

- Capture des flux vidéos, images, identifiants MSN, FTP, emails
- C’est un serveur Linux connecté à Internet
  - Logiciels arbitraires: botnet, proxies, scanners
  - Hebergement malwares, C&C, relai spam
- C’est aussi un serveur Linux connecté à l’intranet
- Attaques navigateurs clients

Et sur les zinternets ?

- Quelques chiffres
  - Caméras écoutants sur divers ports
    - Port 80 - 397,055
    - Port 8080 - 41,492
    - Port 7777 – 390
  - Palmarès pays
    - Allemagne 116,627
    - France 60,792
    - Etats-Unis 51,506
    - Italie 24,775

Source http://www.shodanhq.com – Octobre 2013

Safe Hex !

- Id originaux
- Limiter utilisateurs
- Mettre à jour firmware
- DNS alternatifs, dynamiques
- Restreindre au local (VPN)
- Poubelle !

Difficultés rencontrées

- Déchiffrement RAM, REGEX viable
- Hydra sensible à la casse
- Décompression et montage des binaires
- Réseau peu conciliant

Conclusion

- C’est une passoire
  - Mauvaise implémentation CGI
  - CSRF
  - Reset logs
- C’est une passoire :
  - Reliée à internet
  - A votre intranet
  - Qui a beaucoup de copines
- Limitations du Hack :
  - Serveur SSH
  - Matériel pas assez puissant pour miner du Bitcoin
  - Mots de passes plus élaborés (caractères spéciaux), encodage
- Mais peut s’avérer utile

Questions ?

- GitHub : https://github.com/Girakith/foscamTools

- Remerciements :
  - Core security
  - Shekyan
  - Shape security
  - Qualys Inc.
  - Artem Hartutyunyan