Backbones sous attaque

Vulnérabilités logicielles au format 19”

orange™ Expert security

Pierre Emeriaud
27/01/2026

Bière SECU RENNES

about:

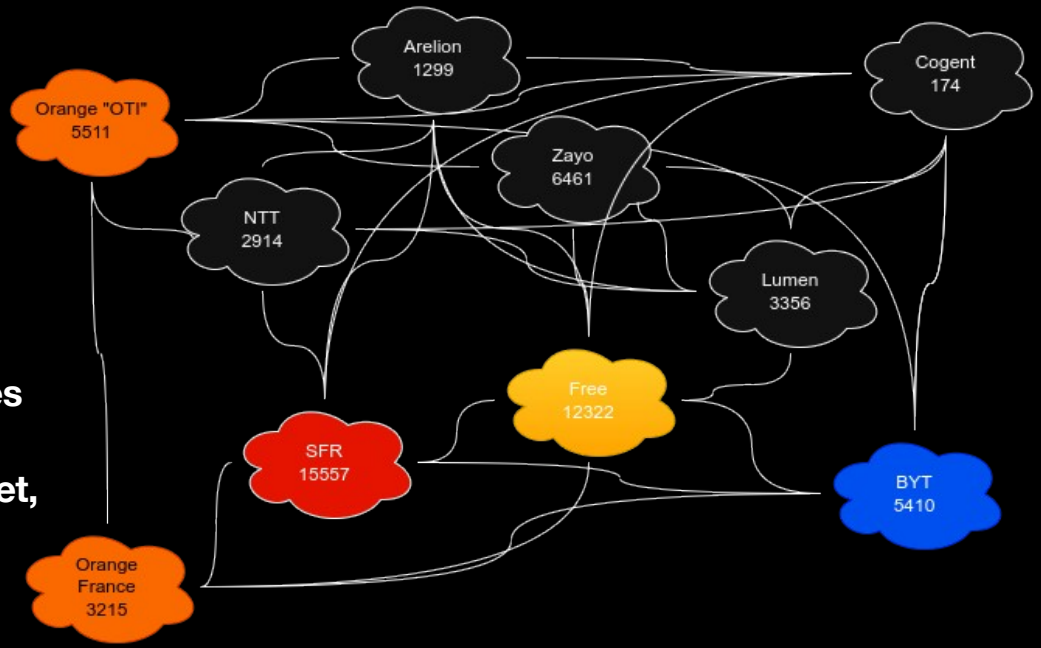
- Network security engineering chez Orange
  - OINIS = Orange International Networks, Infra & Services
    - IP/MPLS, WDM longue distance (terrestre & sous-marin), satellite...
  - Focus sur la sécurité des réseaux IP “wan”
    - leurs équipements
    - Les protocoles
    - Leur administration...

- Membre d’Orange Expert Security
  - 122 personnes parmis 650 au niveau groupe
  - Missions transverses, conseil au management

- Également radioamateur, plongeur tek passionné et mon propre ISP (as206155)

Intro & contexte
#define Backbone

- Infrastructure critique qui compose Internet
  - Coeur de réseau de chaque opérateur
- Pas uniquement Internet mais réseaux privés aussi
  - Réseau mobile (collecte antennes, internet, roaming,...)
  - Entreprise
  - Téléphone fixe
- Pas un réseau unique
  - Mais l'interconnexion de tous



Intro & contexte
Routeur de coeur

- Grosse machine bien différente d'une box
  - Modulaire
  - Très haut débit (100, 400+Gb/s / port)
  - 24x400G/slot, 9,6T/slot, 150T / chassis

- Cible de choix
  - Emplacement privilégié
  - Accès aux protocoles de routage de l'opérateur
  - De plus en plus de fonctionnalités

Evolution architecturale
L’ère monolithique

- Historiquement OS petits voire très petits (<100Mo)
- Architectures spécialisées (cpus MIPS, asic/fpga conçus spécifiquement)
- OS souvent temps réel
  - QNX, eCos, VxWorks…
- Pas exempts de vulnérabilités
  - Mais globalement compliqués à exploiter
  - Compétences nécessaires +++
  - Peu de recherches ou cas concrêts sur gros routeurs

Evolution architecturale
La transformation moderne

- Généralisation de l'utilisation d'architecture x86
  - Introduction d'OS unix-based (JunOS = FreeBSD custom, IOS-XE & XR basés linux)
  - Avec parfois du hardening sur ces Unixes (Verifed exec, SELinux)
  - Mais pas trop non plus (no privsep, shell+scripting, tcpdump...)

- Stack logicielle explosée
  - Apparition de conteneurisation (LXC sur XR, docker sur SONiC) & virtualisation (JunOS, XR, XE)
  - Pas pour la segmentation / sécurisation
  - Mais bien pour la facilité (abstraction hw, code reuse)

De nouvelles vulnérabilités
Surface d’attaque démultipliée

- 2+ OSes par carte
  - (XR = min 3 + LXCs)
  - Y compris les linecards

- LoC ↗️
  - Plus de code = plus de vulns

- Moins de hardening
  - Pas de veriexec ou selinux sur les hosts :(

De nouvelles vulnérabilités
Angles morts et persistance

- **Peu de possibilités de monitoring des OS “hôtes”**

- **Et des fonctionnalités supplémentaires !**

```
root@juniper-node:~# qemu-system-x86_64 -hda attacker.img -nographic -m 4G -k fr -device
virtio-net-pci,netdev=taproot -netdev tap,id=taproot,script=no,downscript=no -net
nic,model=virtio,macaddr=$(cat /sys/class/net/macvtap1/address) -net tap,fd=3 3<>/dev/tap$
(cat /sys/class/net/macvtap1/ifindex)
```

=> Persistance via une VM rogue sur l’une des cartes “CPU”

Accès complet au réseau de management de l’opérateur à travers les ports de management out-of-band

- **Relative invisibilité**

Défis opérationnels et mitigations
du simple au complexe

- **Sécuriser une telle usine est compliqué**
  - **Code de qualité douteuse**

```
[...]
USER_STARTUP='/var/tmp/gofigureitoutyourself.sh'
if [ -f $USER_STARTUP ]; then
echo "#!/bin/sh" > /var/tmp/.thesame.sh
echo "sh $USER_STARTUP &" >> /var/tmp/.thesame.sh
chmod 755 /var/tmp/.thesame.sh
chmod 755 $USER_STARTUP
debug_log "Executing User startup: $USER_STARTUP"
/var/tmp/.thesame.sh
(CVE-2025-30661 - 7.3 - CVSS:3.1/AV:L/AC:L/PR:L/UI:R/S:U/C:H/I:H/A:H)
```

  - **Pas besoin d'être un cador du reverse pour trouver des vulnérabilités :(**
- **Upgrader peut être difficile**
  - **Prend du temps, génère de l'impact**
  - **Durée du support constructeur limitée**
  - **Important de limiter l'exposition dès la conception**

Conclusion

- Gros routeur != effrayant
- Si tu connais unix tu devrais pouvoir te démerder
  - Modulo quelques détails d'archi

- Malheureusement également vrai pour les attaquants
  - Les malwares de routeurs étaient hautement spécialisésdésor
  - Désormais un shell script fonctionne tout aussi bien

- Monitorez vos équipements
- Upgradez aussi rapidement que possible
- Decomissionez le matos end-of-support
- Challengez les fournisseurs

Merci