

Botnets DDoS: la menace pas si fantôme

Jérôme Meyer — FRNOG 38

NOKIA

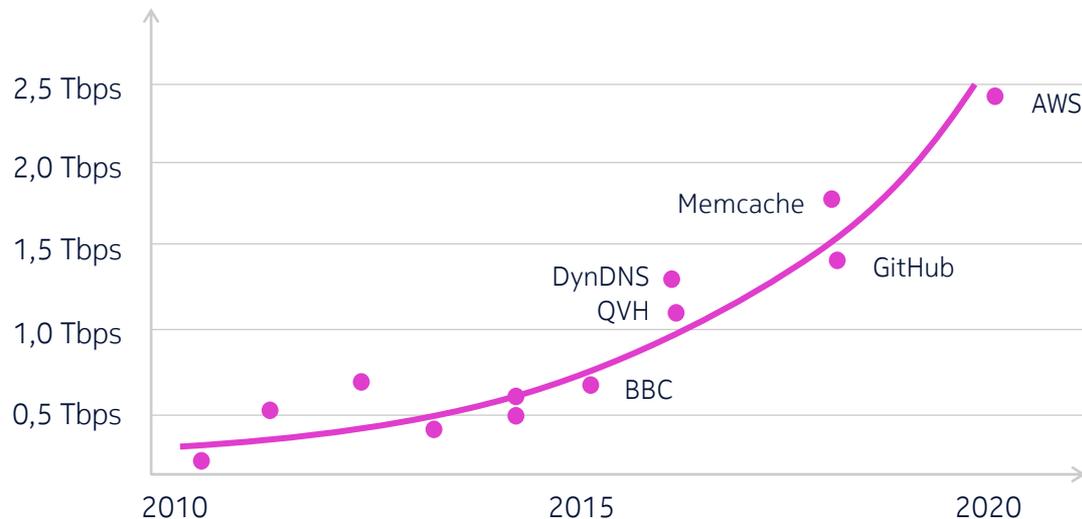
Disclaimer / introduction

- Je travaille pour un équipementier
- Récemment arrivé en France après 20 ans d'activités avec opérateurs en Asie
- Mon activité se concentre sur l'analyse d'attaques DDoS d'opérateurs fixes & mobiles pour Nokia Deepfield (outil spécialisé analyse de trafic et protection DDoS)

Le DDoS aujourd'hui

- Plusieurs milliards d'euros investis au niveau mondial pour la sécurité liée au DDoS...
- ... pour se retrouver à l'impasse avec les attaquants.

Records publics de DDoS volumétrique (2010-2022)



Le DDoS aujourd'hui

- Action agressive des forces de l'ordre avec coordination internationale...
- (et toujours l'impasse.)



Le problème : les botnets

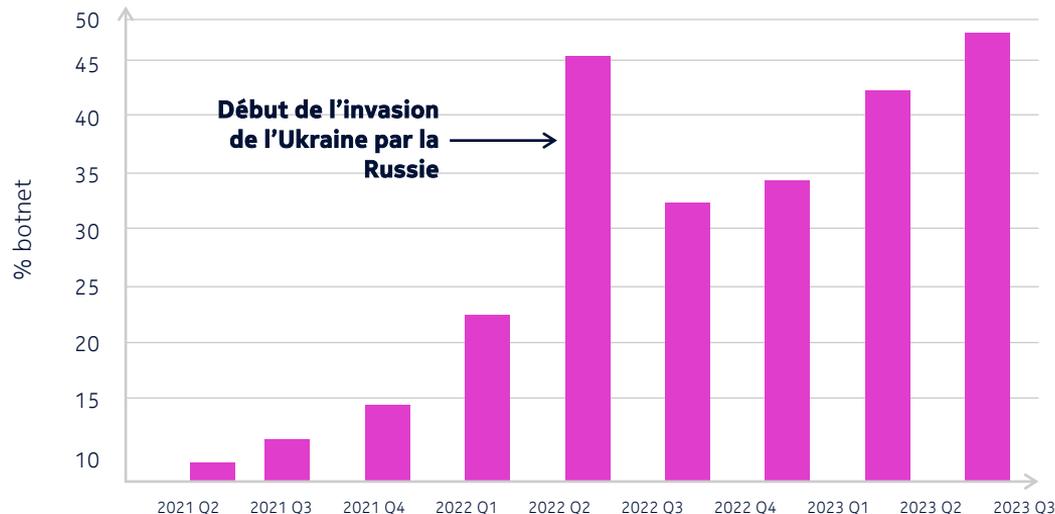
DDoS provenant de botnets comme % du tonnage d'attaque (octets)

2002-2022

- La majorité du trafic DDoS est spoofé depuis une cinquantaine de fournisseurs en Europe/Asie

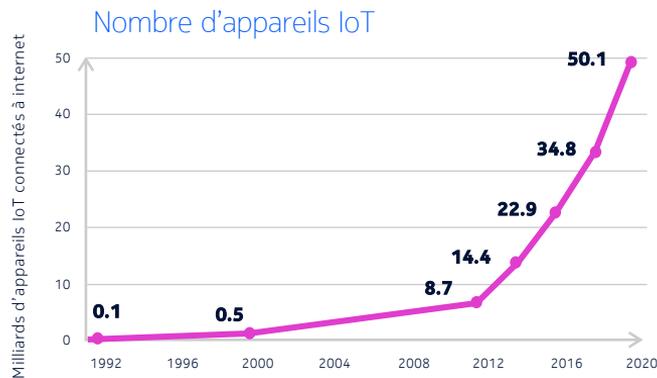
2023

- Les botnets représentent la **majorité** du volume DDoS
- Et représentent plus de **90%** des attaques complexes

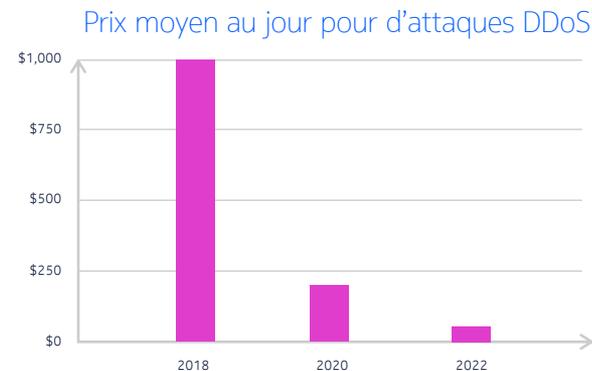


Le problème : l'IoT

- Croissance exponentielle du nombre d'appareils
- Très susceptibles au détournement (mot de passe par défaut et/ou vulnérabilité unauth RCE)
- Contribuant à **l'effondrement des prix de DDoS sur le marché noir**



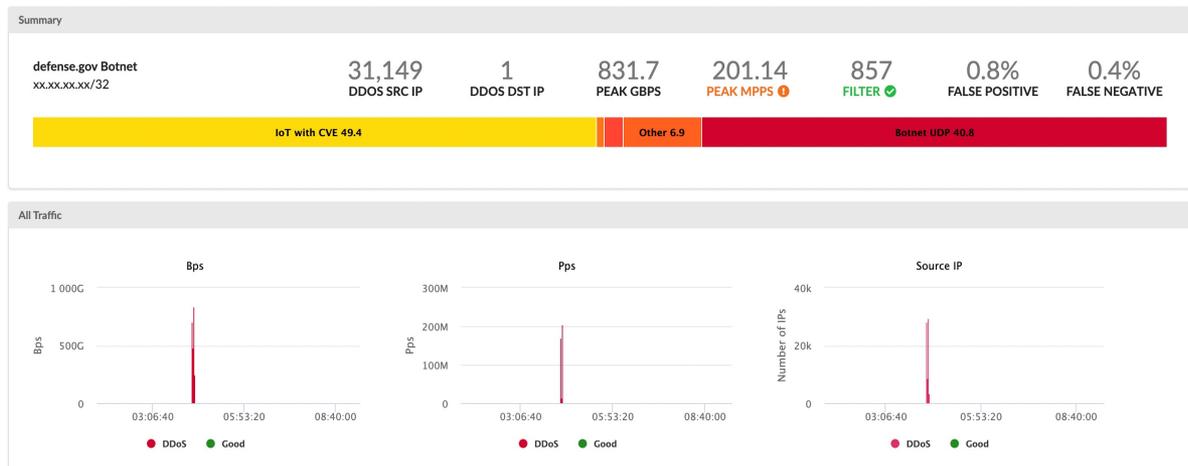
<https://www.comptia.org/content/research/sizing-up-the-internet-of-things>



Données du blog www.zero.bs

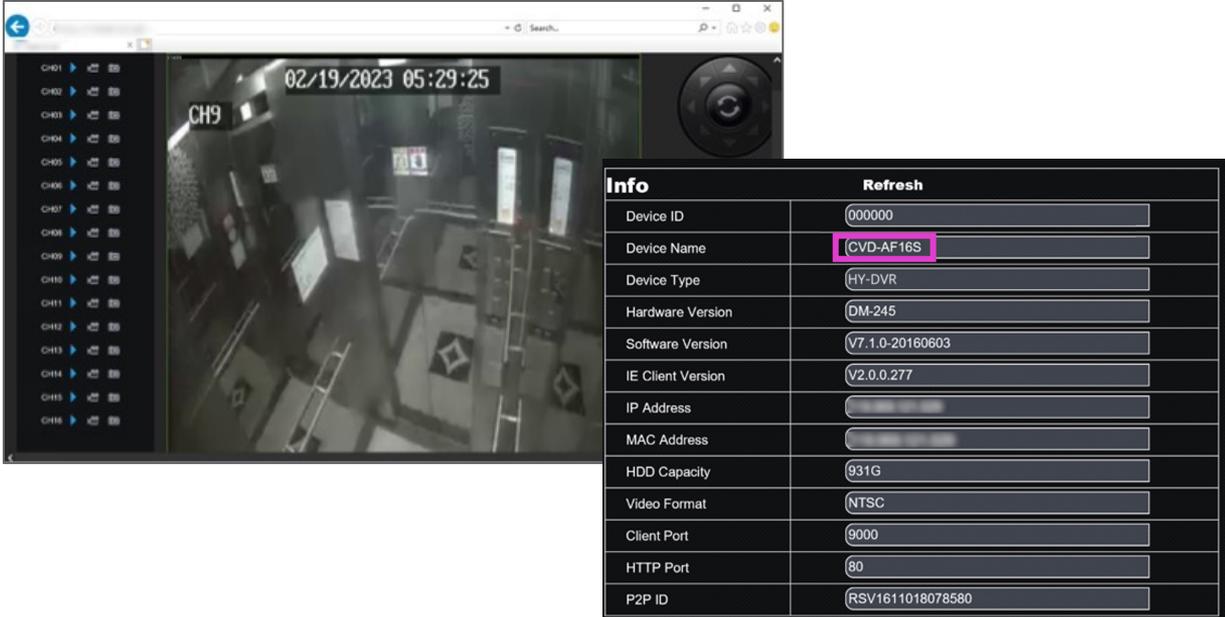
Exemple d'attaque IoT vers IP gouvernementale

- Attaque botnet de 830 Gb/s avec impact de service
- 31K appareils IoT compromis (webcams/DVRs)
- **> 60% provenant d'appareils IoT du même pays**
- Nombreux exemples similaires pour d'autres pays



Exemple d'attaque IoT vers IP gouvernementale

- Equipements DVRs non sécurisés et très facilement découvrables par « crawling »
- Utilise micrologiciel datant de 2016



The image shows a web browser interface for a security system. On the left, there is a list of channels from CH1 to CH16. The main area displays a camera feed for channel CH9, showing an interior view of a control room with a timestamp of 02/19/2023 05:29:25. On the right, there is an 'Info' panel with a 'Refresh' button and a table of device details.

Info	Refresh
Device ID	000000
Device Name	CVD-AF16S
Device Type	HY-DVR
Hardware Version	DM-245
Software Version	V7.1.0-20160603
IE Client Version	V2.0.0.277
IP Address	
MAC Address	
HDD Capacity	931G
Video Format	NTSC
Client Port	9000
HTTP Port	80
P2P ID	RSV1611018078580

Exemple d'attaque IoT vers IP gouvernementale

- À partir du numéro de modèle, il est trivial de trouver les exploits (liés au CVE)
- Avec le CVE, on trouve le code d'exploitation sur GitHub
- Avec le code d'exploitation, **vous avez un « bot »...**

🚩 CVE-2016-20016 Detail

Description

MVPower CCTV DVR models, including TV-7104HE 1.8.4 115215B9 and TV7108HE, contain a web shell that is accessible via a /shell URI. A remote unauthenticated attacker can execute arbitrary operating system commands as root. This vulnerability has also been referred to as the "JAWS webservice RCE" because of the easily identifying HTTP response server field. Other firmware versions, at least from 2014 through 2019, can be affected. This was exploited in the wild in 2017 through 2022.

Severity

CVSS Version 3.x CVSS Version 2.0

CVSS 3.x Severity and Metrics:

 NIST: NVD **Base Score: 9.8 CRITICAL** Vector: CVSS:3.1/(AV:N)/(AC:L)/(PR:N)

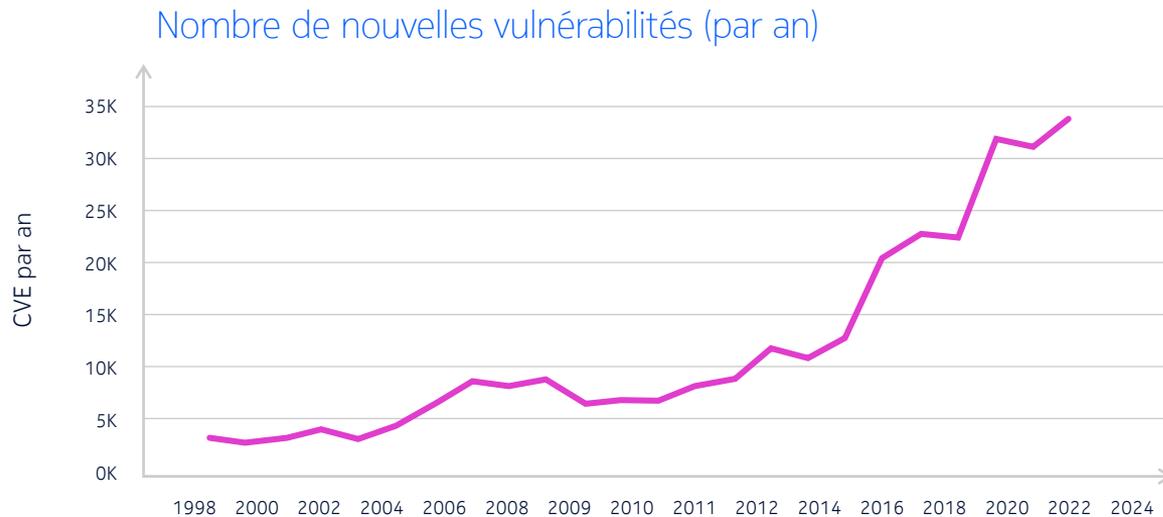
NVD Analysts use publicly available information to associate vector strings and CVSS scores. We also display any CVSS information from the CNA.

Note: NVD Analysts have published a CVSS score for this CVE based on publicly available information at the time of analysis. The score is within the CVE List.

The screenshot shows a GitHub repository page for 'Pwning-CCTV-cameras' by user '33swordsmen'. The repository has 7 commits and was last updated on Jan 11. The file list includes 'IPsamples', 'JAWS_bot.py', and 'README.md'. The 'README.md' file is open, displaying the title 'Pwning-CCTV-cameras' and a description: 'Exploiting cameras with a very distinctive HTTP Server header of "/>

Le problème : l'abandon logiciel (et les bugs)

Croissance soutenue pour le nombre de vulnérabilités IoT divulguées publiquement chaque année



Source: CVE® Program <https://cve.mitre.org/>

Le problème : la course au Gigabit symétrique

Ces 20 dernières années

- La plupart des accès HFC/DSL sont fortement asymétriques et des botnets sont limités à 10-20 Mb/s en débit montant
- La menace des botnets est relativement gérable dans la mesure où **la bande passante montante n'augmente pas**

Pourquoi Free offre la fibre la plus rapide ?

Free est le premier fournisseur d'accès à internet en France à proposer l'offre fibre la plus rapide au monde avec la **technologie Fibre 10G EPON**. Cette technologie vous assure une navigation internet sans ralentissement même lorsque plusieurs appareils sont connectés en même temps grâce à un débit jusqu'à 400 fois plus rapide que l'ADSL (débit descendant théorique de 8 Gbits/s et débit montant théorique de 700 Mbits/s.)

Et selon le baromètre nPerf, Free propose l'offre fibre numéro 1 sur les débits en 2022*.

Nouvelle SFR BOX 8X, une expérience plus intense

NOUVEAU !

Avec la Fibre, bénéficiez d'un débit jusqu'à 8 Gb/s !*

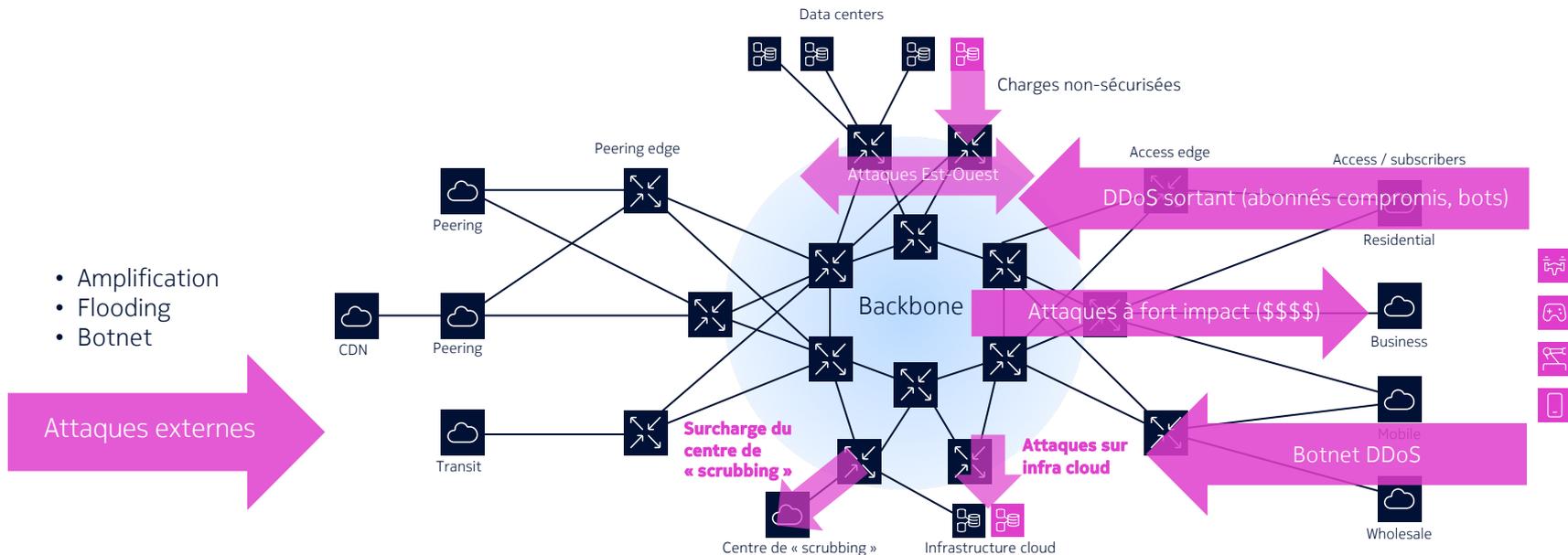
Un Wifi 3 fois plus performant avec le WIFI 6, une image et un son cinéma avec la 4K HDR, le Dolby Vision et le Dolby Atmos et un assistant vocal. Installez-vous confortablement et préparez-vous à vivre une expérience inédite !

*Sous réserve d'éligibilité avec la SFR Box 8X et l'offre SFR Fibre Premium, débit théorique descendant maximum de 8Gb/s depuis un équipement compatible branché en filaire grâce au module SFR Box 8X fourni sur demande, ou partagé entre plusieurs équipements branchés en filaire (jusqu'à 1Gb/s par équipement, hors module SFR BOX 8X) et en Wifi. Débit théorique montant maximum de 1 Gb/s. Dans la limite des stocks disponibles.

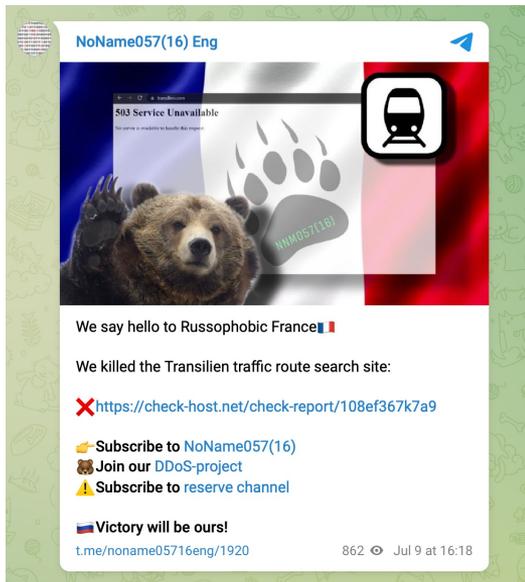
[VOIR LES OFFRES BOX](#)

Le haut débit symétrique (multi-)Gigabit
nourrit le feu des botnets

Le problème : votre réseau



(mais ce n'est pas que IoT)



- Attaques « efficaces » contre divers sites de pays après annonces pro-Ukraine
 - Nombre de sources et trafic relativement faibles...
 - ...mais agent utilisateur valide, « handshakes » TCP & TLS valides, et requêtes dans formulaires avec paramètres valides
- La réponse fréquente: blocage de pays source, faute de mieux

(mais ce n'est pas que IoT)

Src IP	Peer	Genome	% Bytes	% Flows
346			2.61	2.69
345			2.19	2.06
153			1.73	1.6
10.97			1.1	1.01
10.102			1.07	1.03
10.91			1.07	1
6.40			1.06	1.15
8			1.05	0.98
10.103			1.04	0.98
10.98			1.04	1
8			1.03	0.98
10.78			1.03	1.01
10.94			1.02	0.96
239			1.02	0.99
6.26			1.02	1.13
8.80			1.02	0.98
6.41			1.02	1.08
8.65			1.02	0.97
8.83			1.01	0.94
5			1.01	0.97
10.100			0.99	1.02
17			0.99	0.97
6.63			0.99	0.98

Mais lorsque qu'on regarde de plus près, on peut facilement voir des éléments communs qui peuvent permettre de remédier plus efficacement à l'attaque

En résumé

- Le DDoS est toujours là, mais avec des caractéristiques très différentes
 - l'adoption IoT va continuer (et déjà 600k à 1 million de « bots » IoT actifs)
 - Capacité agrégée de 50 à 100 Tb/s estimée aujourd'hui
 - Puissance de frappe en passe d'augmenter « grâce » au Gbps montant
- Protéger le peering est **toujours nécessaire — mais plus suffisant**
- Il devient essentiel de maintenir une bonne **visibilité sur l'ensemble du réseau** (et à terme: utiliser le réseau pour se défendre)

NOKIA