Botnets DDoS: la menace pas si fantôme

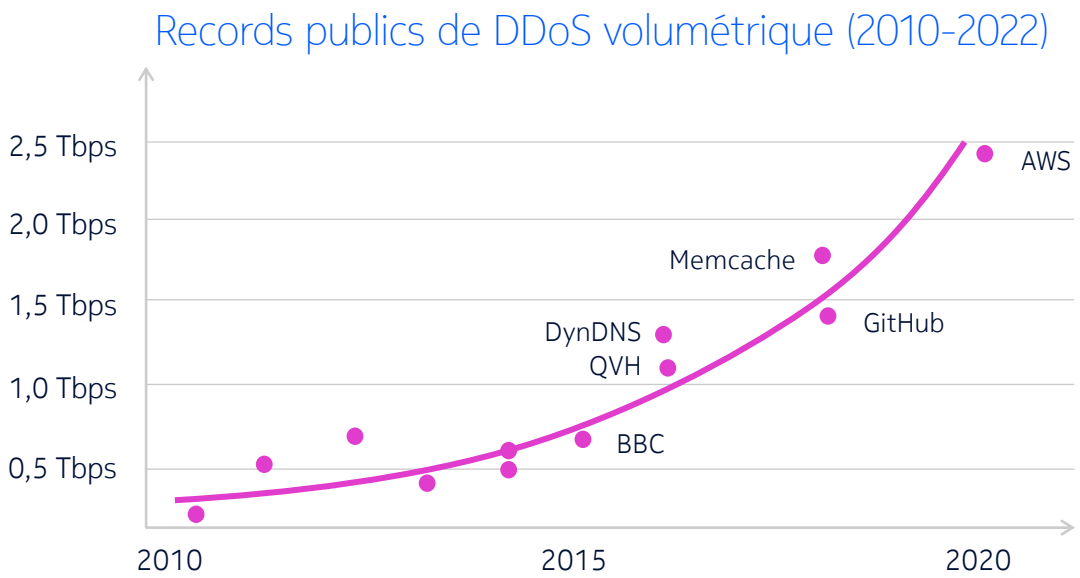
Jérôme Meyer — FRNOG 38

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.



Le DDoS aujourd'hui

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

CYBERSÉCURITÉ \ INFORMATIQUE \ JURIDIQUE

DDoS à la demande : une cinquantaine de sites fermés après une opération de police internationale

Gros coup de filet pour Europol, le FBI et les services de police britanniques qui ont annoncé jeudi 15 décembre avoir mis à l'arrêt une cinquantaine de sites vendant des attaques DDoS.

Mathieu Pollet

16 décembre 2022 | 13h40

2 min. de lecture

Réagir →

Le problème : les botnets

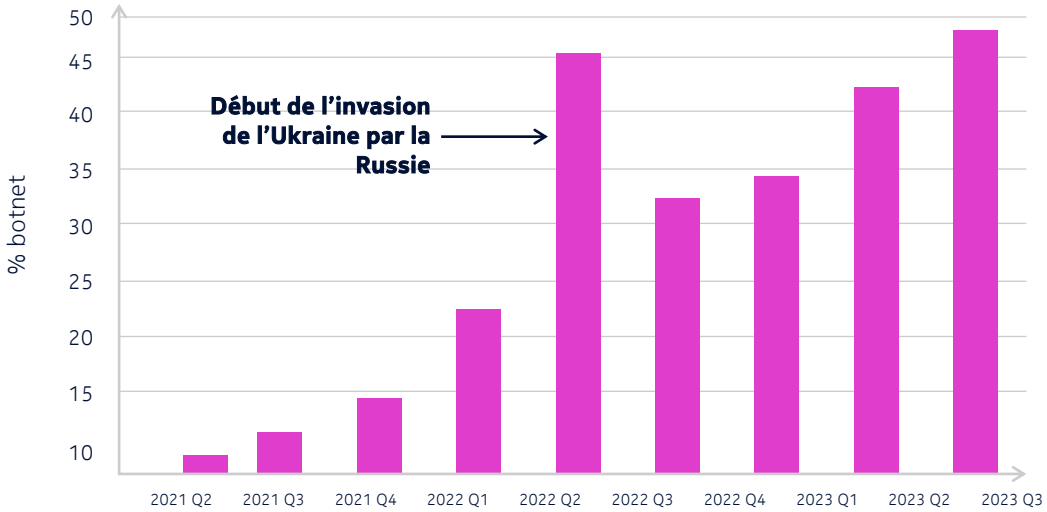
2002-2022

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

2023

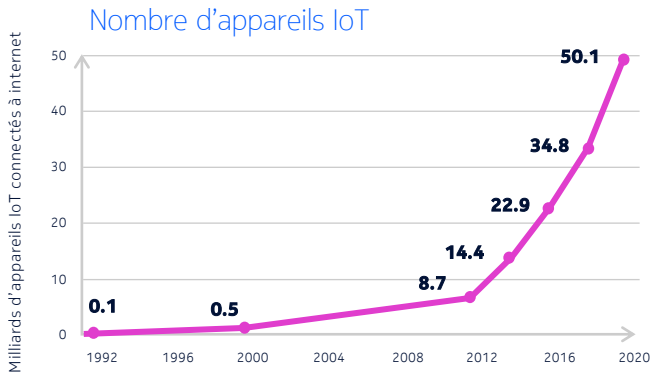
- Les botnets représentent la **majorité** du volume DDoS
- Et représentent plus de **90%** des attaques complexes

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

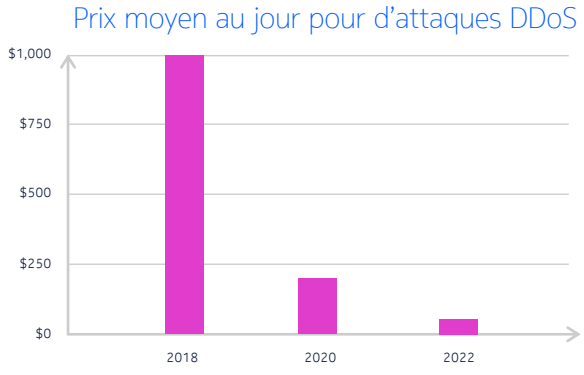


Le problème : l'IoT

- 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**



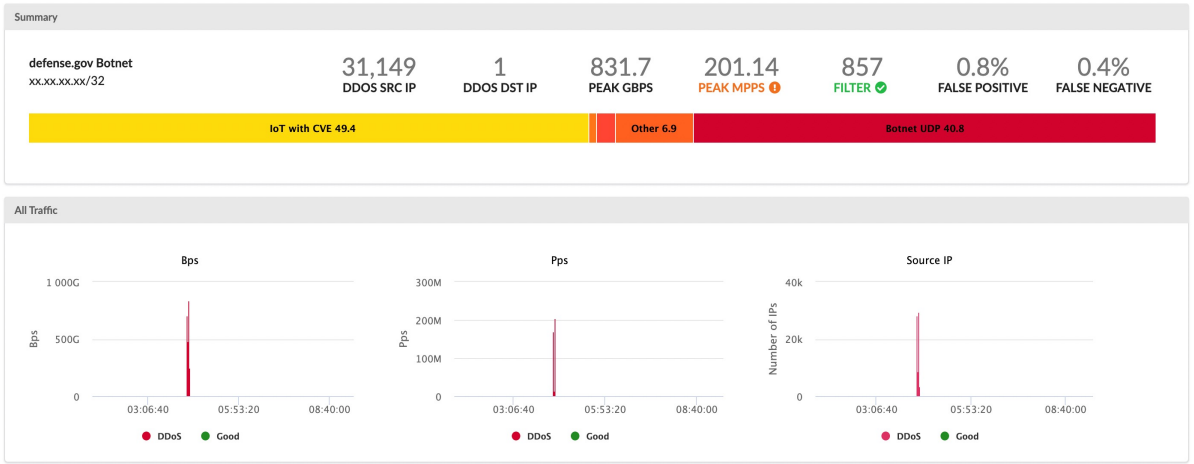
https://www.comptia.org/content/research/sizing-up-the-internet-of-things



Données du blog www.zero.bs

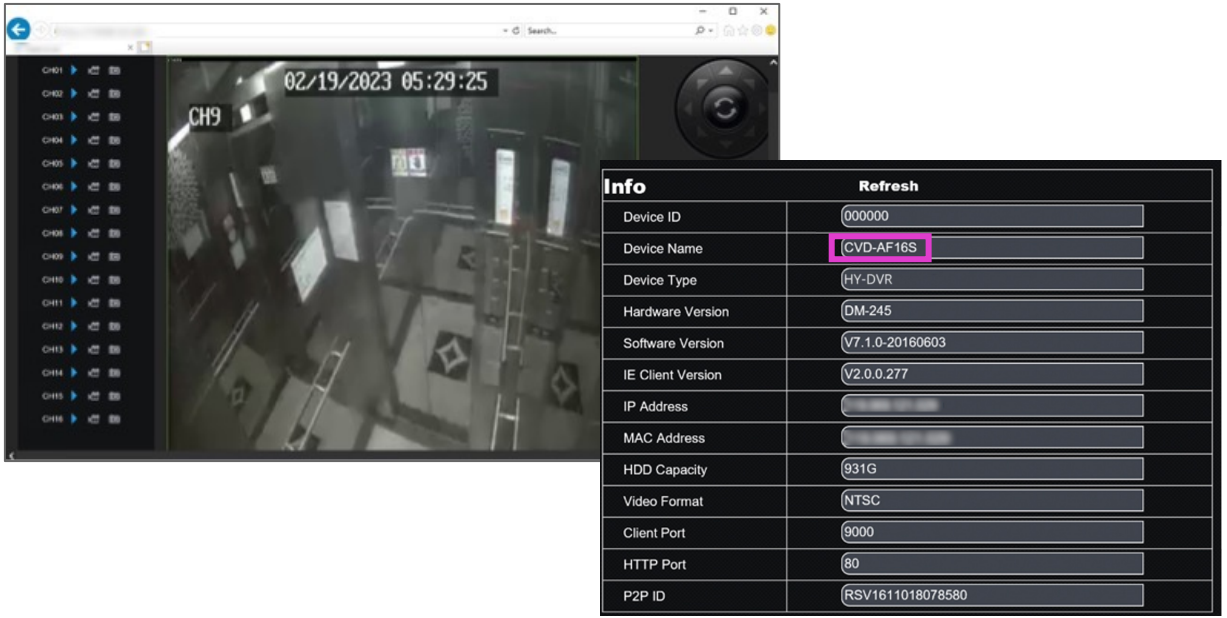
Exemple d’attaque IoT vers IP gouvernementale

- 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



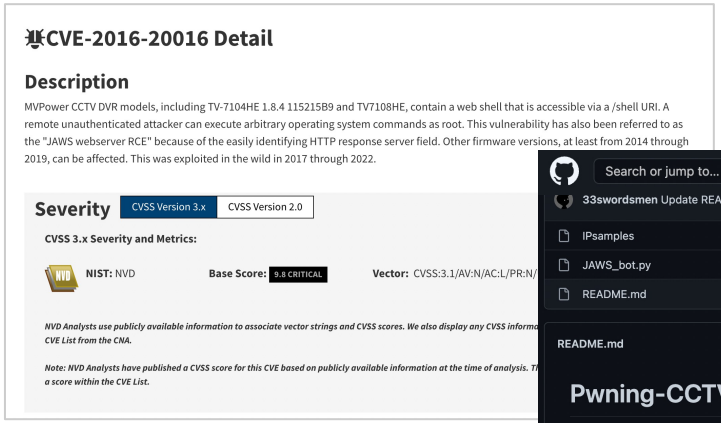
Exemple d’attaque IoT vers IP gouvernementale

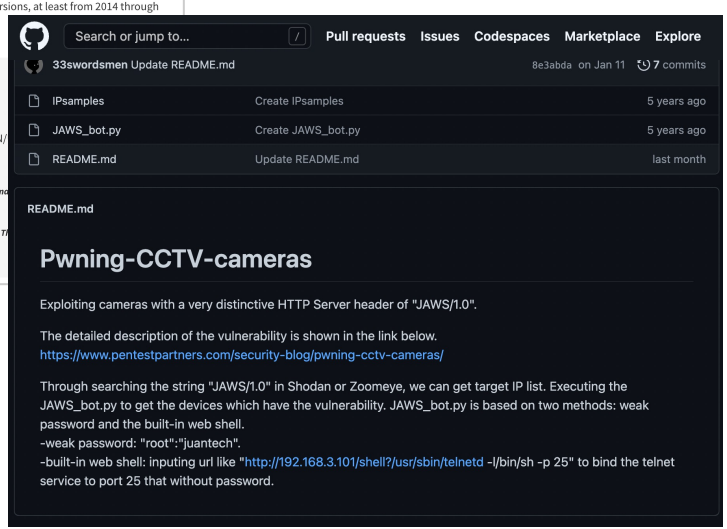
- Equipements DVRs non sécurisés et très facilement découvrables par « crawling »
- Utilise micrologiciel datant de 2016



Exemple d’attaque IoT vers IP gouvernementale

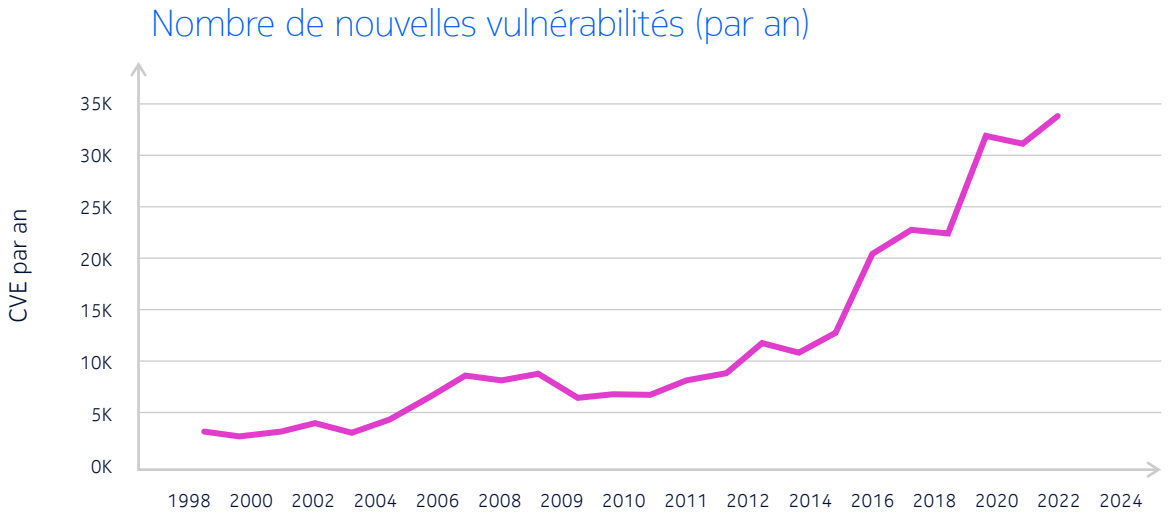
- À partir du numéro de modèle, il est trivial de trouver les exploits (liés au CVE)
- Avec le CVE, on trouve le code d’exploitation sur GitHub
- Avec le code d’exploitation, **vous avez un « bot »…**





Le problème : l’abandogiciel (et les bugs)

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

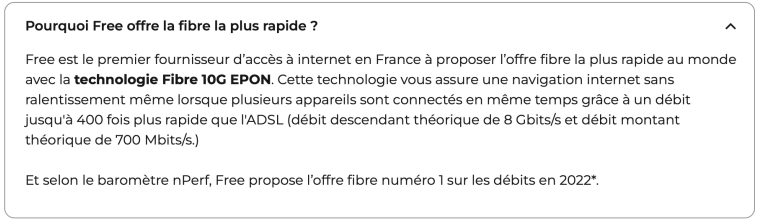


Source: CVE® Program https://cve.mitre.org/

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**

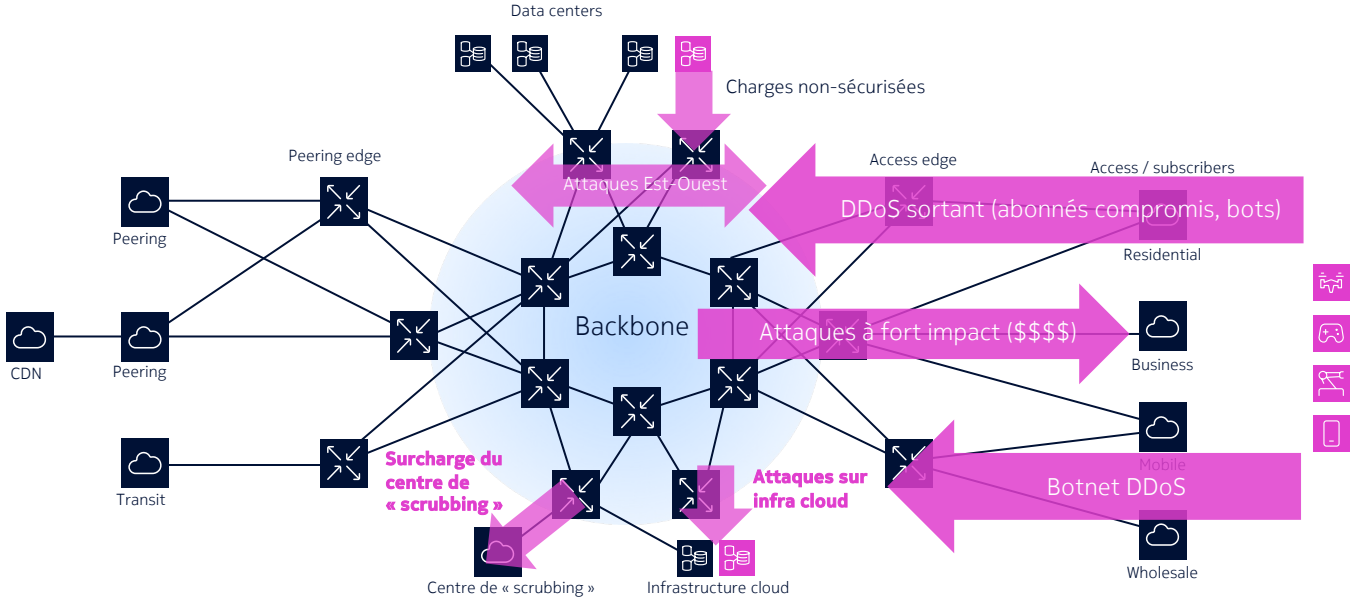


Le haut débit symétrique (multi-)Gigabit nourrit le feu des botnets

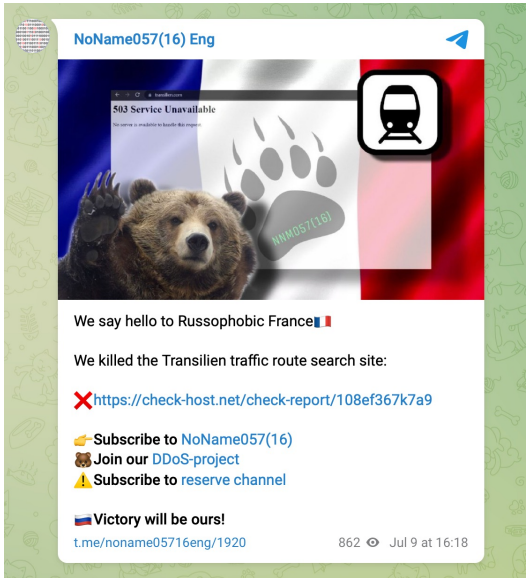
Le problème : votre réseau

- Amplification
- Flooding
- Botnet

Attaques externes

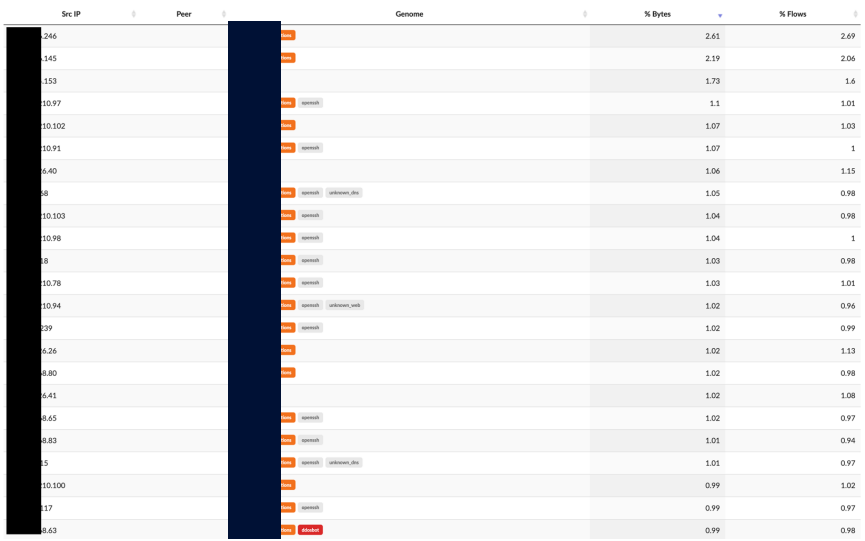


(mais ce n’est pas que IoT)



- 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
.246			2.61	2.69
.145			2.19	2.06
.153			1.73	1.6
10.97		openssh	1.1	1.01
10.102			1.07	1.03
10.91		openssh	1.07	1
6.40			1.06	1.15
58		openssh unknown_dns	1.05	0.98
10.103		openssh	1.04	0.98
10.98		openssh	1.04	1
18		openssh	1.03	0.98
10.78		openssh	1.03	1.01
10.94		openssh unknown_web	1.02	0.96
239		openssh	1.02	0.99
6.26			1.02	1.13
8.80			1.02	0.98
6.41			1.02	1.08
8.65		openssh	1.02	0.97
8.83		openssh	1.01	0.94
15		openssh unknown_dns	1.01	0.97
10.100			0.99	1.02
17		openssh	0.99	0.97
8.63		Abobot	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