IA/ML en la mitigación de ataques DDoS

José Alberto Nistal Iglesias

19/05/2023

ES.NOG 29

Antes y ahora

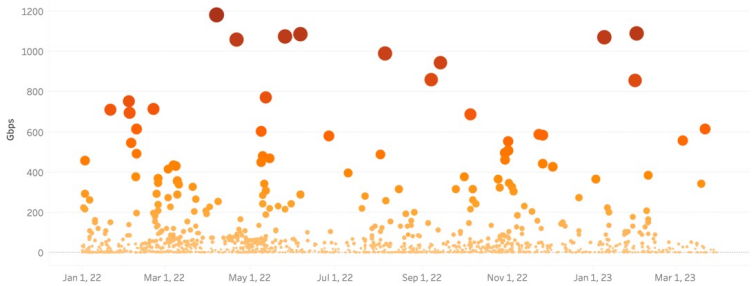
#1: Las botnets han conquistado el mundo (del DDoS)

2002 - 2022

- La mayoría del DDoS era spoofed (IP header modification, IPHM)
- Venía de ~50 proveedores de hosting en Europa / Asia
- Utilizaba servidores NTP / DNS mal configurados

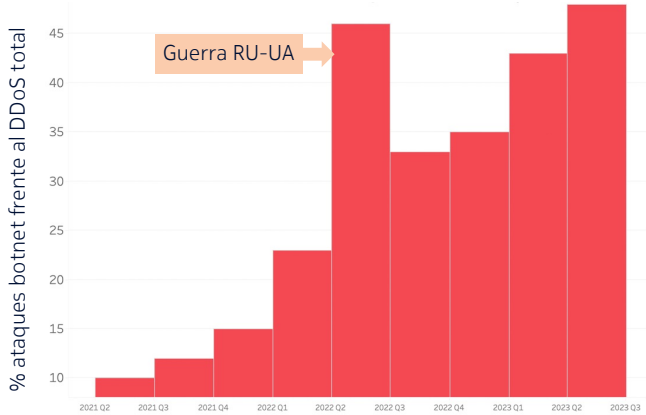
2023

- Los (miles de) ataques que hemos visto en 2022-2023



Hoy:

- Las botnets generan la mayoría del tráfico DDoS
- Las botnets suponen **el 90% de los ataques complejos**
- **Las botnets se saltan los sistemas anti-DDoS tradicionales**



Fuente: Nokia Deepfield

El gráfico muestra datos de Nokia sobre porcentaje de tráfico DDoS procedente de botnets sobre el tráfico DDoS total en el último año. Fuente de datos: proveedores de servicios y cloud participantes en la alianza Nokia Deepfield GDTA que utilizan la solución comercial anti-DDoS de Nokia.

Los bots: qué son y dónde viven

#2: Las amenazas están creciendo exponencialmente

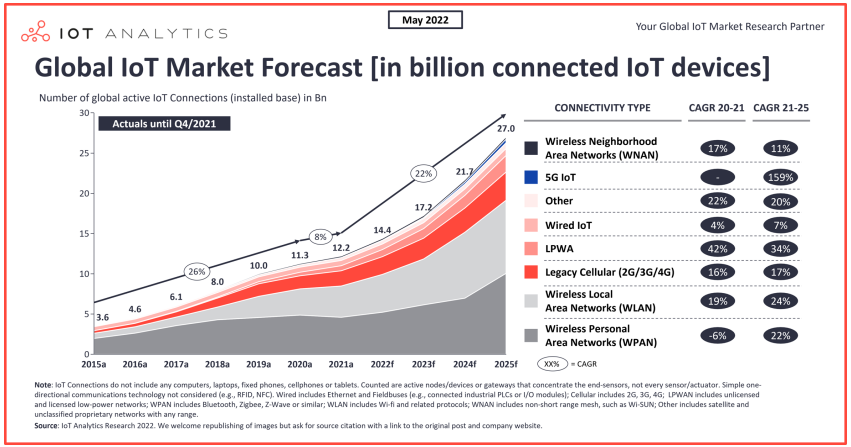
¿Dónde están los bots?

- Empresas: IoT y cloud se han generalizado
- Videovigilancia / Digital Video Recorders / Network Video Recorders
- TPVs, calefacción/ventilación/AC, control remoto y recolección de datos (contadores, parquímetros)
- Imagen médica

¿Qué son los bots?

- La mayoría de los bots son CPEs comprometidos (por ejemplo, routers Mikrotik), seguidos por 30-40 marcas de DVR
- Las botnets tienden a atacar en “manadas” (dispositivos y topologías similares)
- La nube no es la mayor fuente (por número de dispositivos), pero sí una de las que más crece en capacidad de ancho de banda (bps) e intensidad de paquetes (pps)

Y va a empeorar:



Fuente: https://iot-analytics.com/number-connected-iot-devices/

El 99% del IoT empresarial está correctamente parcheado, protegido por cortafuegos y seguro, pero....

El 1% de muchos miles de millones de dispositivos es significativo.

¿Cuál es la magnitud del problema?

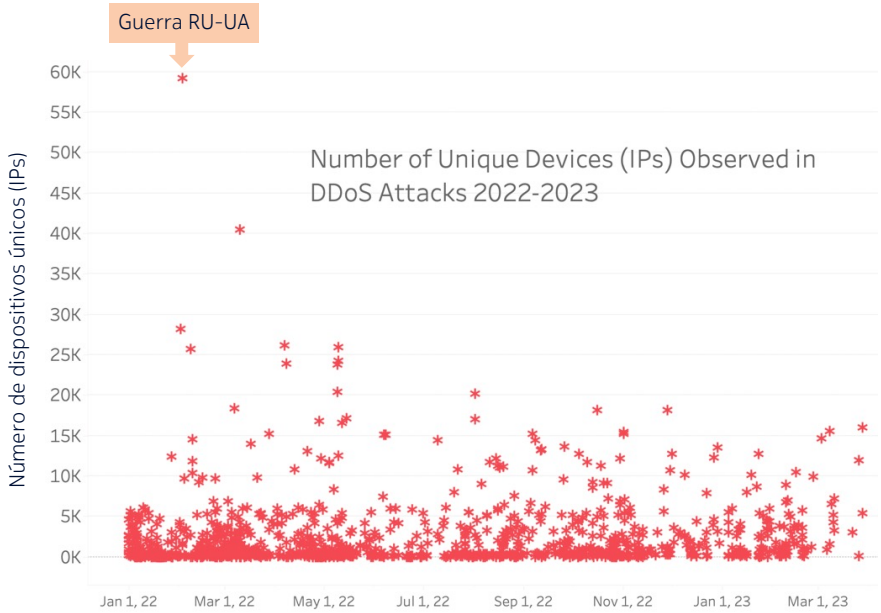
#3: Miles de botnets, cientos de miles de bots

A día de hoy, según datos de Nokia (y otros), las botnets suponen:

- **500k – 1M** dispositivos IoT activos
- **50 - 100 Tbps** de capacidad agregada
- **1-2 Tbps** de pico

¿Cuántos bots y cuántas botnets?

- **Mayoría de ataques < 5.000 dispositivos** y consiguen ataques efectivos a muchos servidores/aplicaciones
- Hay redes grandes con **> 60k dispositivos**
- Los ataques geopolíticos incluyeron dispositivos botnet desconocidos hasta entonces



Fuente: Nokia Deepfield

Algunas cifras

#4: Todavía estamos en las primeras etapas del impacto del DDoS desde botnets

Últimos 20 años de la historia de Internet

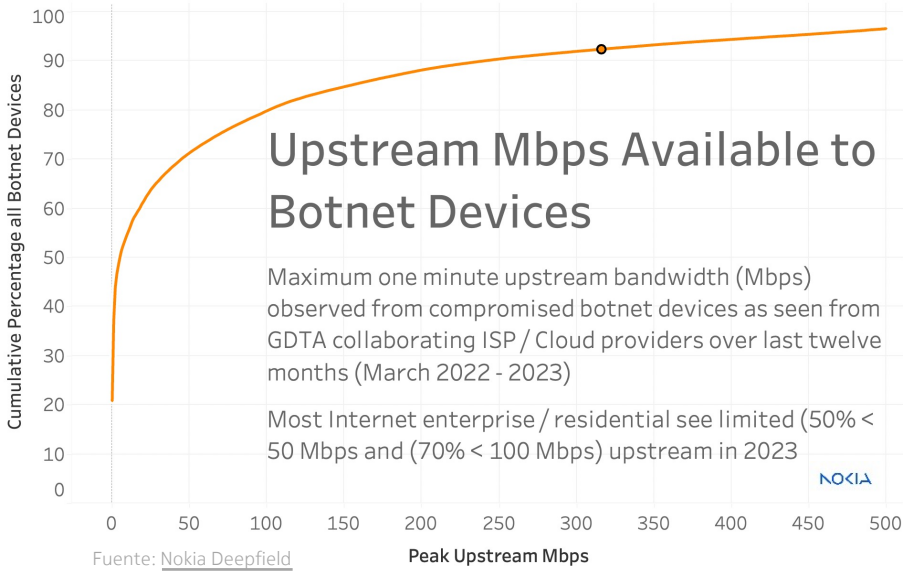
- Mayoría de accesos vía cable/ADSL
- Acceso asimétrico 90 Mbps/10 Mbps (bajada/subida)

La amenaza sigue siendo limitada

- El ancho de banda de los bots coincide con la media de la industria
- 70% bots < 50 Mbps a día de hoy

Sin embargo…

Hasta ahora, **las botnets están limitadas por el ancho de banda de subida actual** — pero la carrera hacia las velocidades gigabit y el ancho de banda simétrico ya está muy avanzada.



Fuente: Nokia Deepfield

¿Por qué son tan preocupantes los ataques de botnets?

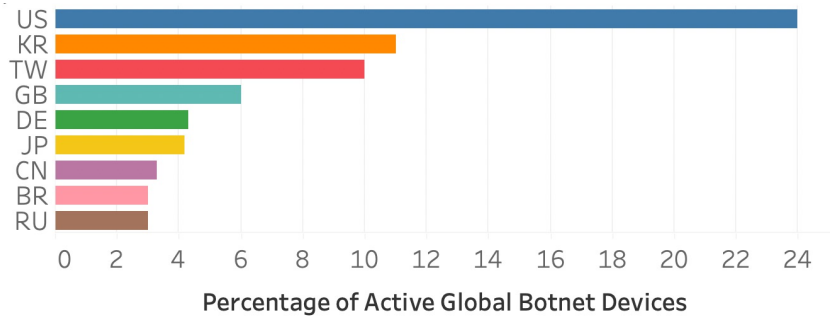
«Tenemos al enemigo en casa»

El modelo de seguridad tradicional de ISPs / CSPs:

- Proteger los bordes externos de la red frente a ataques entrantes
  - Especialmente problemático en Europa del Este / Asia
- Protección frente a spoofing o ataques de amplificación
  - Contramedidas activas (SYN cookie, HTTP redirect…)
  - Limitación/conformado de tráfico DNS, NTP, LDAP…

La realidad en 2023:

- La mayor parte del problema de las botnets afecta a Norteamérica y Europa
- **La mayor amenaza para muchos ISPs procede de sus propios clientes**



Fuente: Nokia Deepfield

¿Qué podemos hacer?

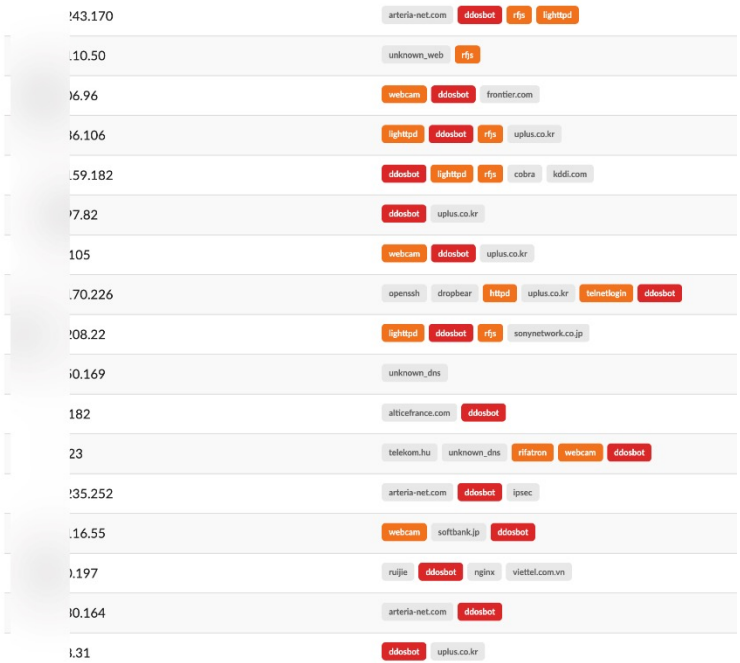
Baselines! Rate-limiting!

¿Qué podemos hacer (de verdad)?

#1 Detección de anomalías

En más del 95% del DDoS, ya no se trata de mirar lo que hay dentro del paquete, sino quién/qué lo está enviando.

- Los thresholds de bps/pps y los baselines son insuficientes e inadecuados para monitorizar la mayoría del tráfico actual (incluyendo eventos virales)
- Un **enfoque basado en big data** que correlacione el **tráfico de la red** en tiempo real con una **visión más amplia de internet** (por ejemplo, qué tipo de dispositivo hay detrás de una dirección IP de origen) es **mucho más eficaz** para reducir los falsos positivos



Datos de Nokia: Principales orígenes de tráfico en un ataque de amplificación DNS hacia una dirección IP residencial (víctima). Fuente de datos: proveedores de servicios y cloud participantes en la alianza Nokia Deepfield GDTA que utilizan la solución comercial anti-DDoS de Nokia.

¿Qué podemos hacer (de verdad)?

#2 Mitigación automática basada en IA

Una vez detectado un ataque, un sistema puede generar una respuesta automatizada basada en múltiples parámetros, que creará un modelo optimizado para **ese ataque**, en **ese momento**, en **esa red**.

Por ejemplo:

- ¿Cuál es el mix de vectores de ataque?
- ¿Qué dispositivos de mitigación están disponibles en la red, a qué escala y coste por bit?
- ¿Cómo se programan esos dispositivos?
- ¿Qué botnet está lanzando el ataque?

>95% de los ataques pueden mitigarse en los routers (modernos) gracias a los avances en rendimiento del hardware y la programabilidad (en particular NETCONF).

```
entry 8 create
    description ";#DFA;acl_90"
    match protocol 17
        dst-ip ip-prefix-list "VLAB_7_1"
        packet-length lt 40
        fragment false
    exit
    action
        drop
    exit
exit
entry 9 create
    description ";#DFA;acl_571"
    match protocol 6
        dst-ip ip-prefix-list "VLAB_7_1"
        tcp-fin true
        tcp-syn true
    exit
    action
        drop
    exit
exit
entry 10 create
    description ";#DFA;acl_579"
    match protocol 6
        src-ip ip-prefix-list "VLAB_9_518"
    exit
    action
        drop
    exit
exit
entry 4 create
    description ";#DFA;acl_13498"
    match
        dst-ip ip-prefix-list "VLAB_9_495"
        ttl range 1 37
    exit
    action
        drop
    exit
```

Salida del modelo de estrategia de mitigación hacia un router vía NETCONF.

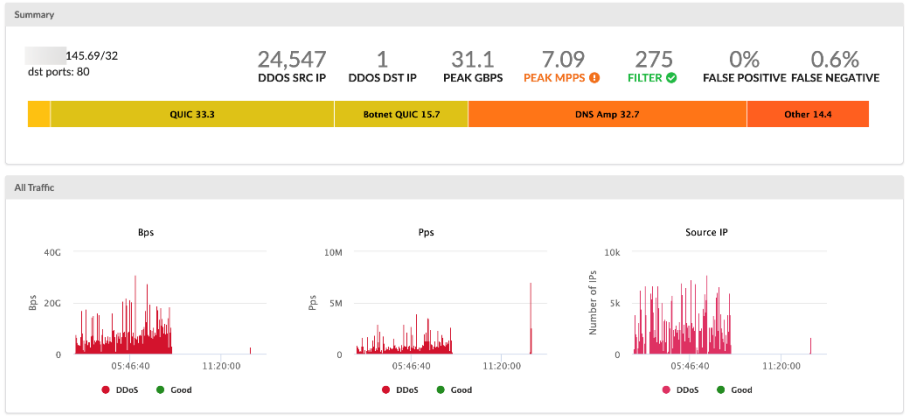
¿Qué podemos hacer (de verdad)?

#3 Mitigación adaptativa y aprendizaje colaborativo

En lugar de dejarse llevar por la incertidumbre:

- La eficacia de una mitigación puede **medirse** frente a ataques reales
- El modelo puede ser **entrenado** con nuevos ataques para optimizar las contramedidas
- Se pueden conocer y optimizar las tasas de falsos negativos/falsos positivos

Esto requiere una **colaboración activa entre proveedores de servicios** para compartir datos (anonimizados) de inteligencia sobre amenazas DDoS en tiempo real.



Informe de un ataque DDoS en abril de 2023 a un host de un gobierno de la UE. Fuente de datos: proveedores de servicios y cloud participantes en la alianza Nokia Deepfield GDTA que utilizan la solución comercial anti-DDoS de Nokia.

En resumen

Estamos en los albores de las botnets, pero ya generan la mayoría del tráfico DDoS actual

- Crecimiento exponencial del IoT empresarial
- Apuesta por la conectividad simétrica gigabit, lo que impulsa aún más la "carrera armamentística"

Las botnets IoT son un problema de todos

- ISPs, empresas y suministradores deben tomar medidas proactivas para mitigar las amenazas del IoT

La IA/ML nos da herramientas para atajar esta amenaza

- Los modelos pueden (y deben) ser entrenados con datos del mundo real
- Es esencial una mayor colaboración para compartir datos actuales de ataques DDoS


NOKIA