CUANDO EL 90% DE TU TRÁFICO NO ES "REAL"

es.NOG

DMNTR
NETWORK SOLUTIONS

by Felipe Cañizares Navarro
aka **Dement0r**

Sobre mi…

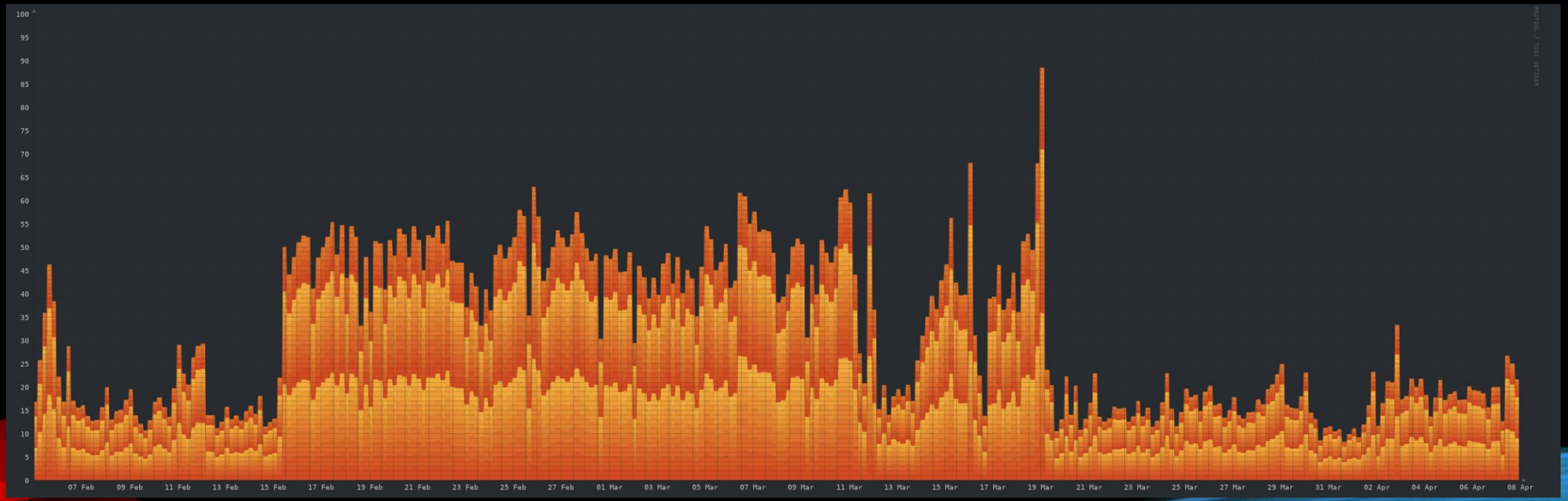
SOY DE GRANÁ

Trabajo en DMNTR Network Solutions – BIOS Technology
Me dedico a la Ciberseguridad y las Soluciones de Red
Escribo historias por Twitter
Envío una Newsletter semanal: *https://dmntr.news*
Algunos días cuento cosas en un "podcast"

@weareDMNTRs

https://t.me/gentedeIT

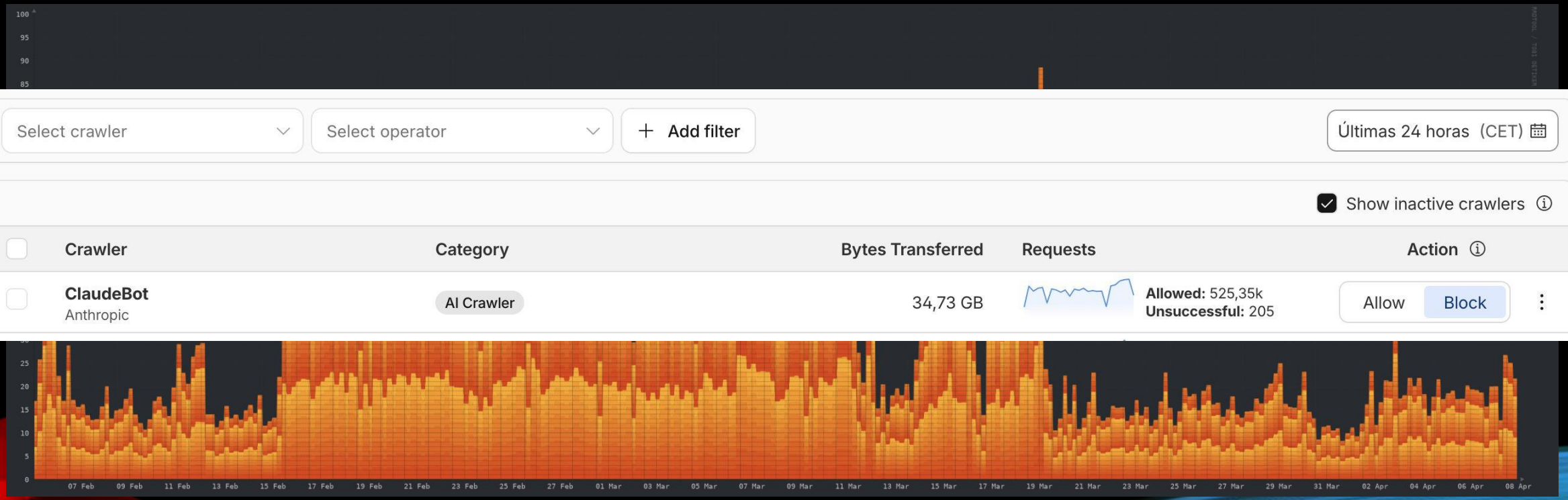
Porqué estamos aquí…



DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

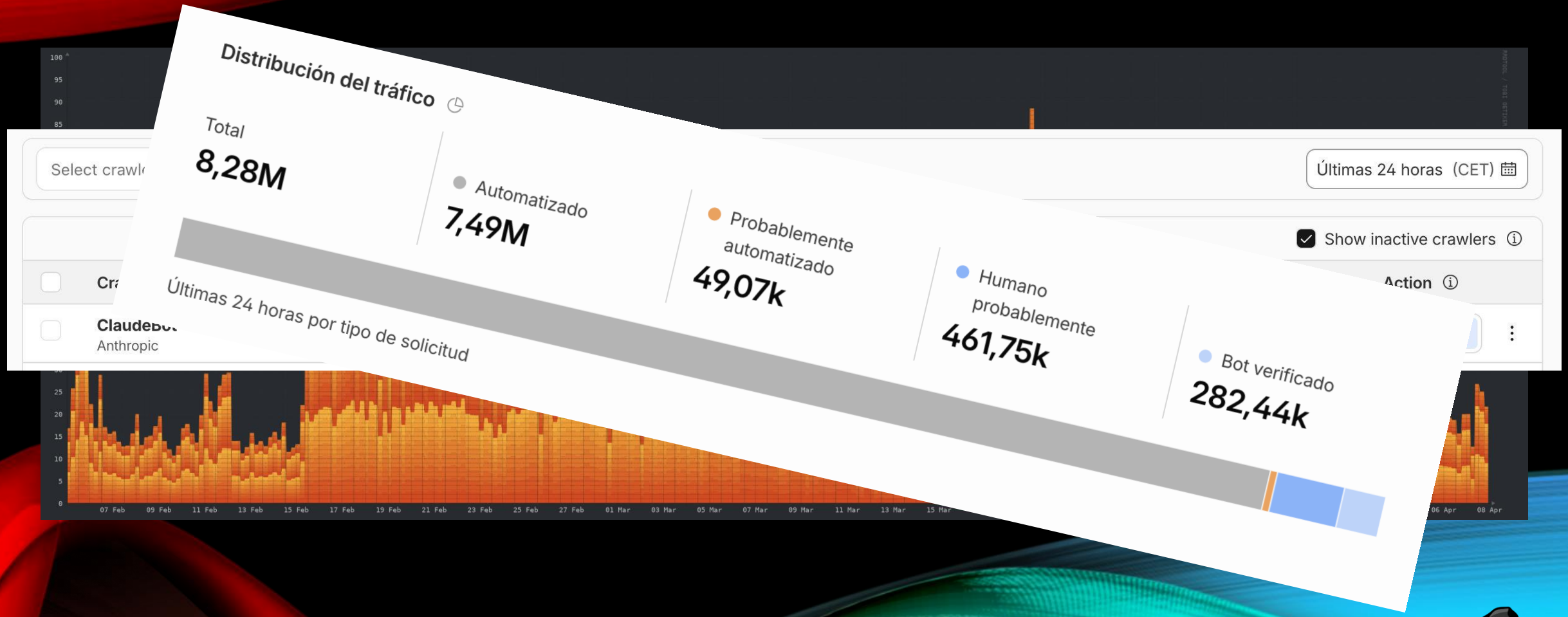
Porqué estamos aquí…



DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Porqué estamos aquí…



DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Porqué estamos aquí…

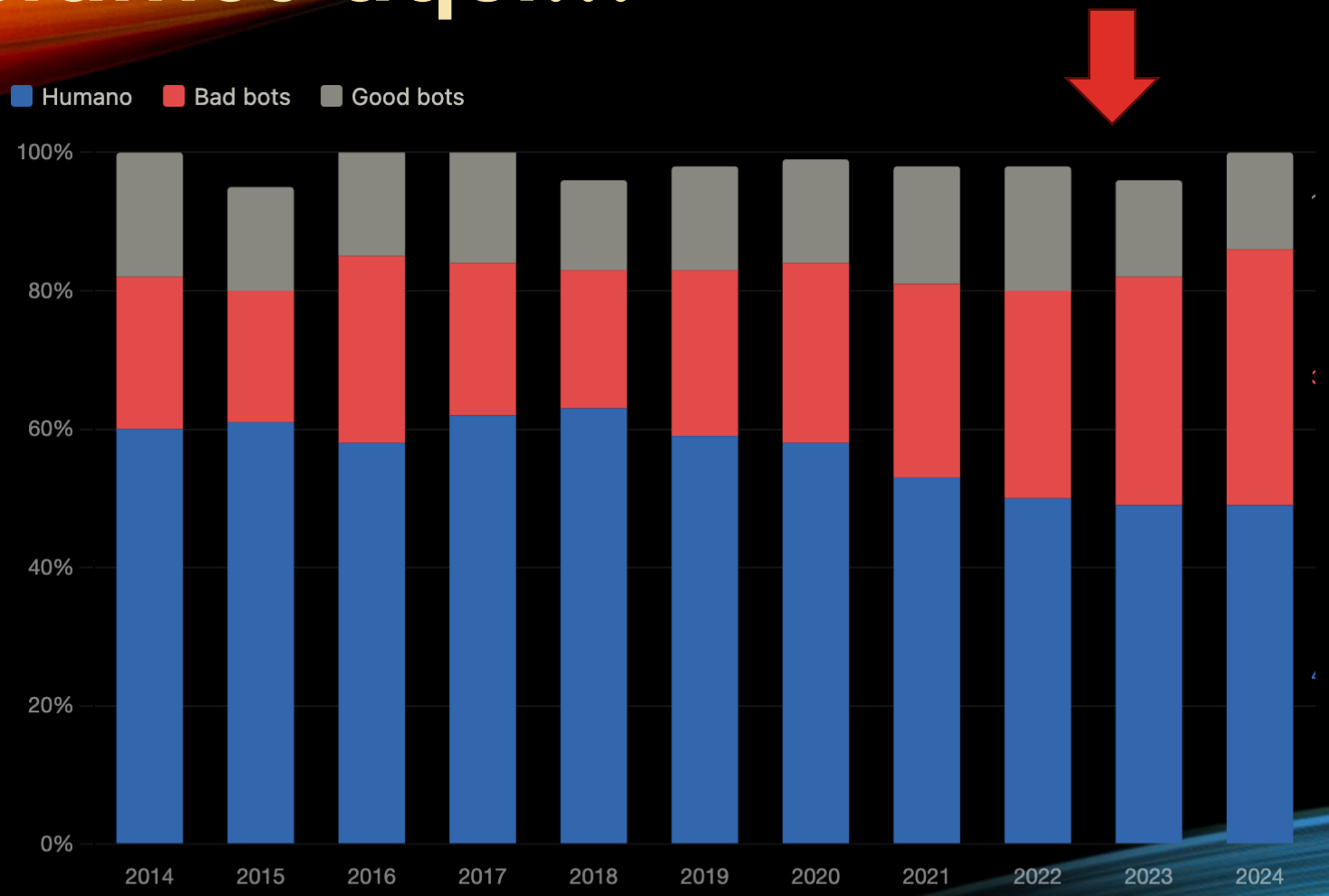
5%

“humanos”

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

DMNTR
NETWORK SOLUTIONS

Porqué estamos aquí…

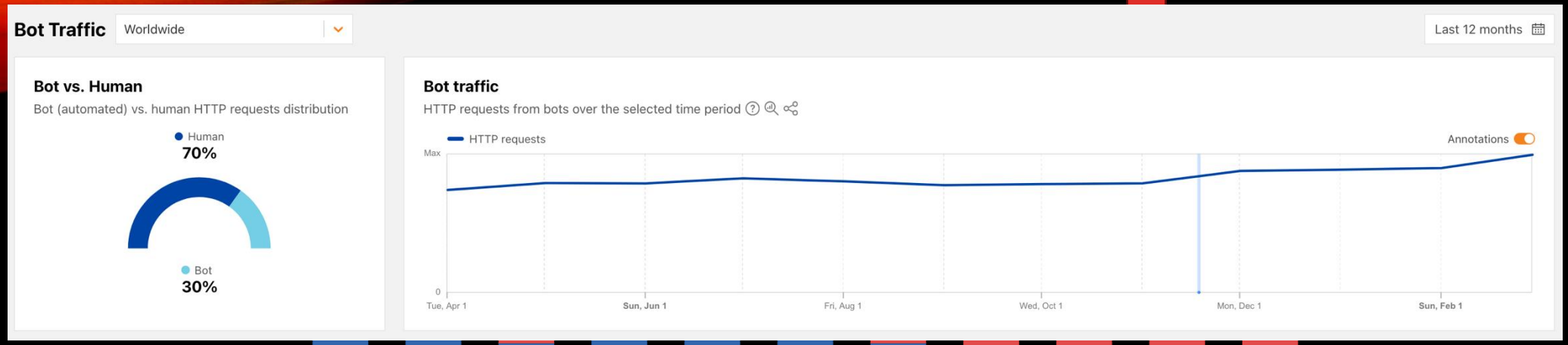


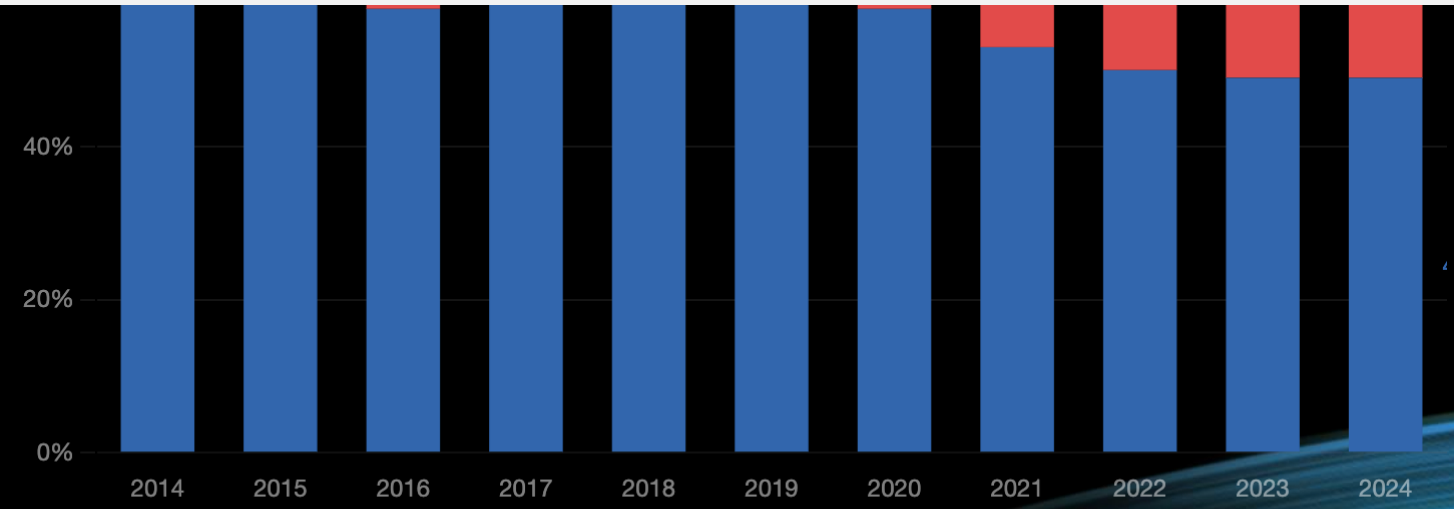
Fuente: Imperva Bad Bot Report (2015–2025) · Thales Group · imperva.com/resources/resource-library/reports/2025-bad-bot-report/
Los datos de cada informe anual corresponden al año anterior (ej: Bad Bot Report 2025 = datos de 2024). No existen datos publicados de 2025 a fecha de hoy.

DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Porqué estamos aquí…



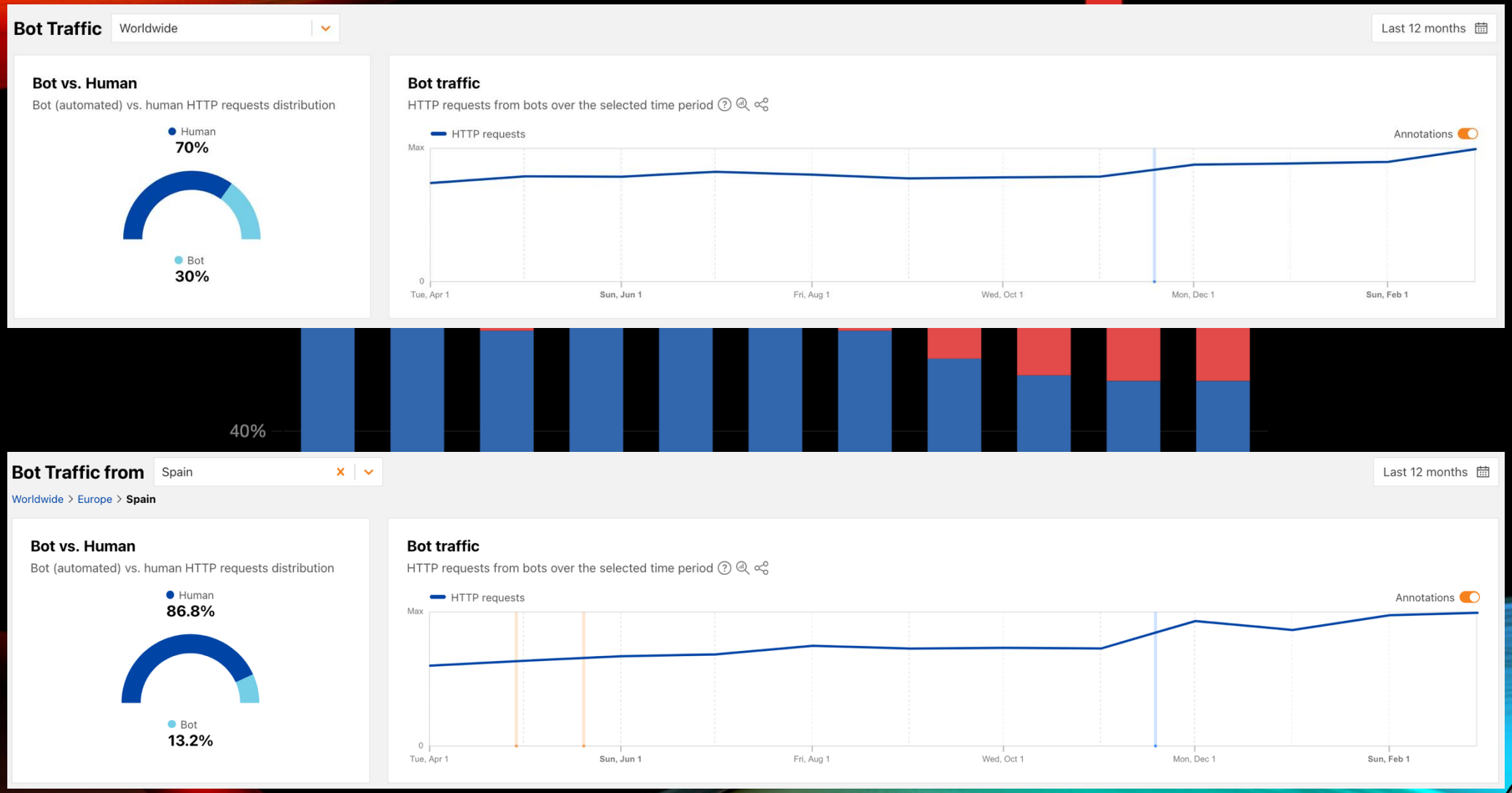


Fuente: Imperva Bad Bot Report (2015–2025) · Thales Group · imperva.com/resources/resource-library/reports/2025-bad-bot-report/
Los datos de cada informe anual corresponden al año anterior (ej: Bad Bot Report 2025 = datos de 2024). No existen datos publicados de 2025 a fecha de hoy.

DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

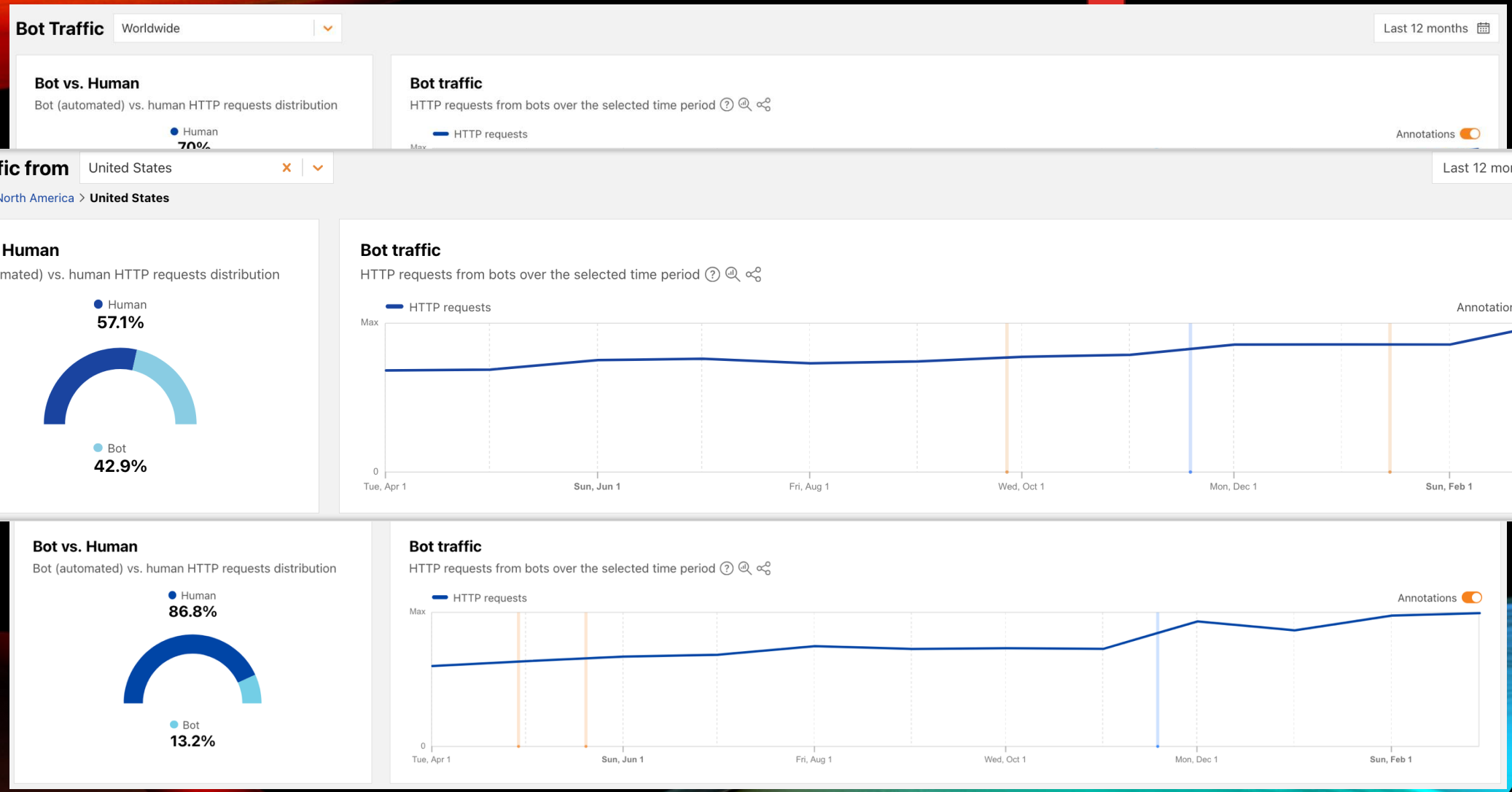
Porqué estamos aquí…



DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Porqué estamos aquí...



DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Porqué estamos aquí…

ERA DE LA IA

Un informe revela que la inteligencia artificial y los bots se han apoderado oficialmente de internet.

PUBLICADO EL JUEVES 26 DE MARZO DE 2026 • A LAS 9:00 A. M. EDT |
ACTUALIZADO EL JUEVES 26 DE MARZO DE 2026 • A LAS 11:42 A. M. EDT

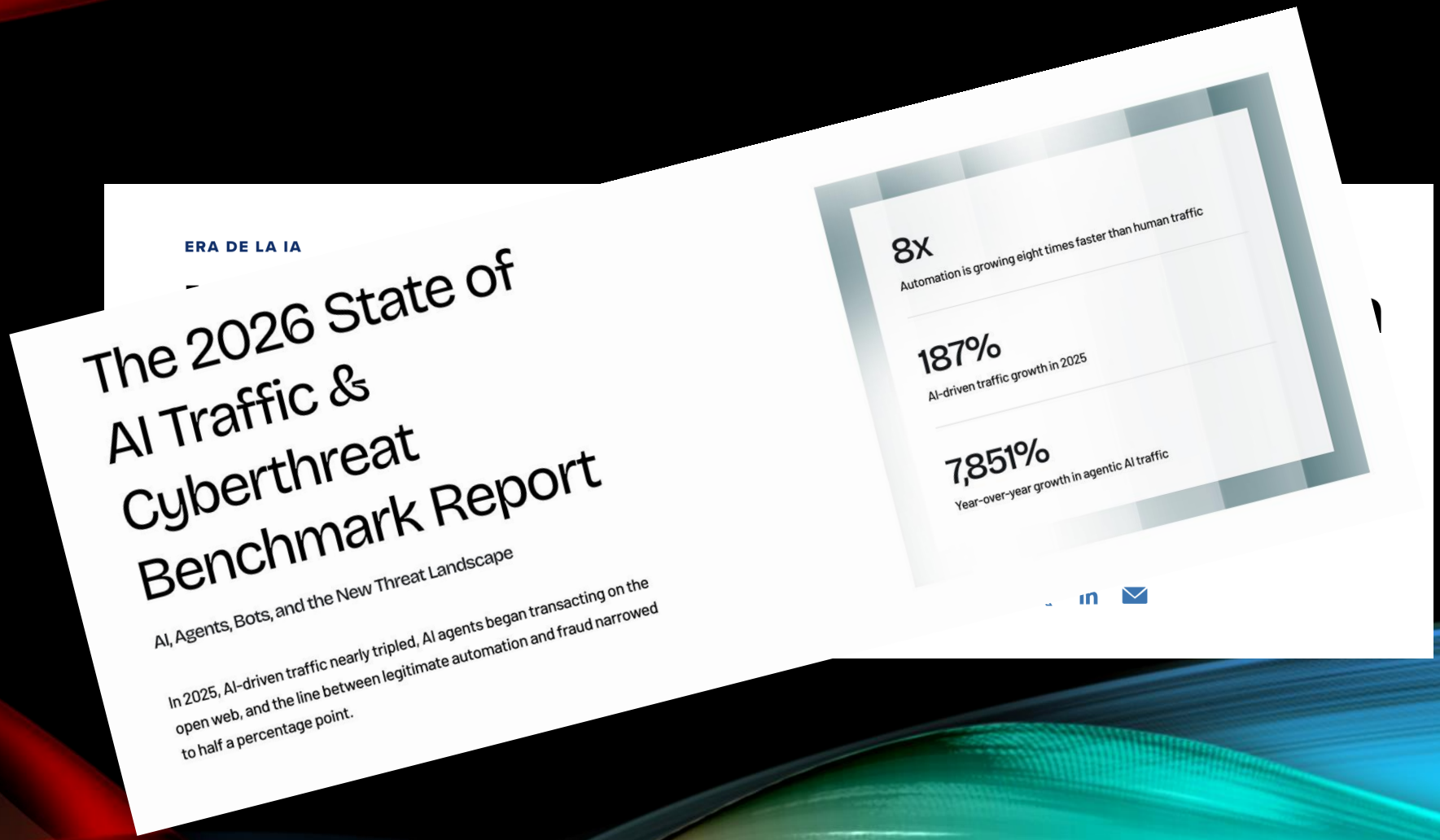
Lola Murti
@IN/LOLAMURTI/
@LOLAVKM

COMPARTIR

DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Porqué estamos aquí…

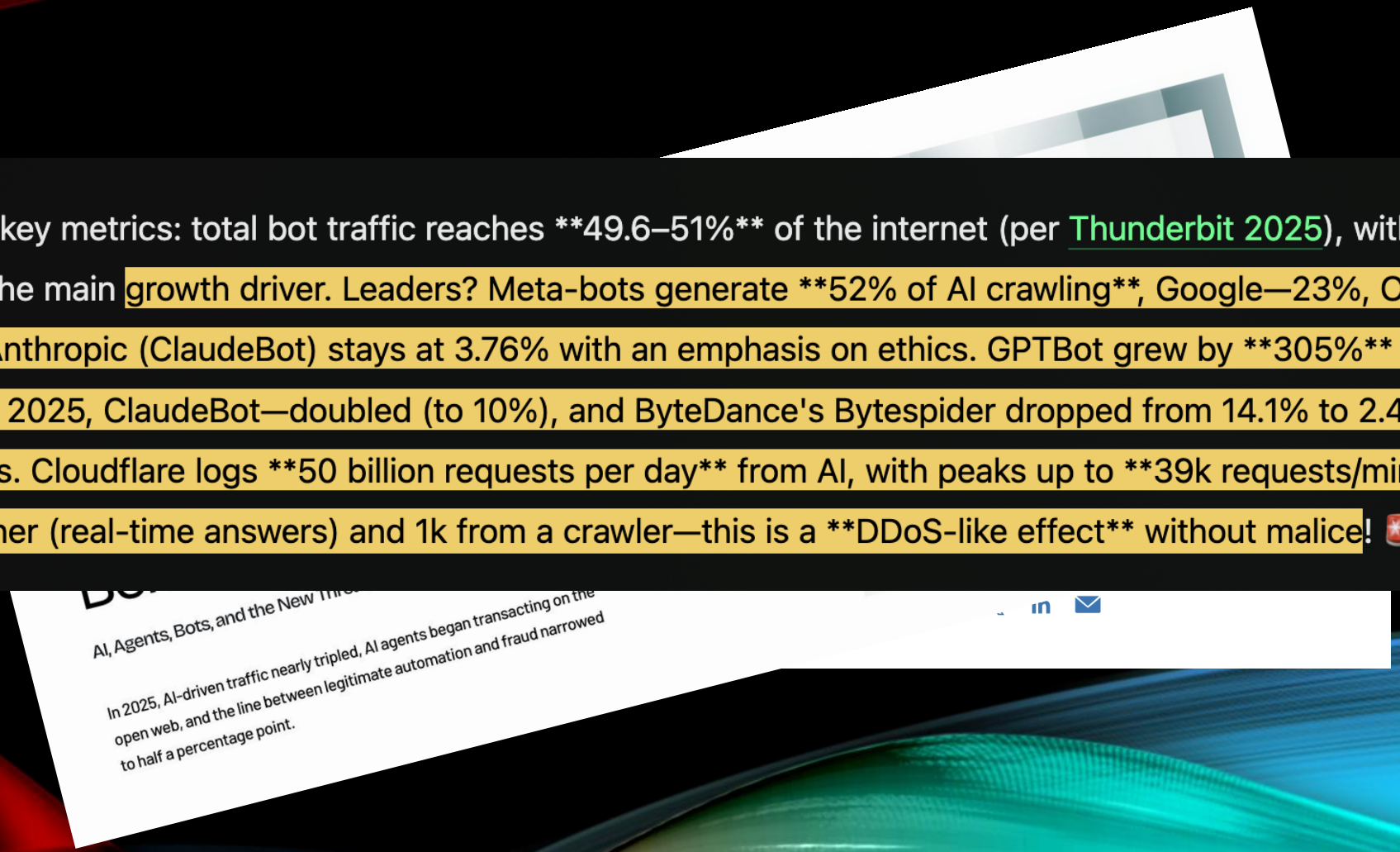


DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Porqué estamos aquí…

Let's look at key metrics: total bot traffic reaches **49.6–51%** of the internet (per Thunderbit 2025), with AI crawlers as the main growth driver. Leaders? Meta-bots generate **52% of AI crawling**, Google—23%, OpenAI—20%, while Anthropic (ClaudeBot) stays at 3.76% with an emphasis on ethics. GPTBot grew by **305%** from May 2024 to 2025, ClaudeBot—doubled (to 10%), and ByteDance's Bytespider dropped from 14.1% to 2.4% due to regulations. Cloudflare logs **50 billion requests per day** from AI, with peaks up to **39k requests/min** from a single fetcher (real-time answers) and 1k from a crawler—this is a **DDoS-like effect** without malice! 🚨



DMNTR
NETWORK SOLUTIONS

Porqué estamos aquí…

Aumento del rastreo mediante IA. Los rastreadores de IA fueron los agentes de usuario que con mayor frecuencia fueron bloqueados por completo en los archivos robots.txt.

- Anthropic mostró la mayor proporción de rastreo a referencia entre las principales plataformas de IA y búsqueda, lo que significa que rastreó mucho más contenido del que envió como tráfico. La proporción alcanzó un máximo cercano a ~500 000:1 a principios de año, y luego se estabilizó entre ~25 000:1 y ~100 000:1 después de mayo. Para comparar:
  - La relación OpenAI se disparó a aproximadamente 3700:1 en marzo.
  - La perplejidad fue la más baja entre las principales plataformas de IA. Comenzó por debajo de 100:1, subió brevemente por encima de 700:1 a finales de marzo durante un pico de actividad de PerplexityBot, y luego se mantuvo mayormente por debajo de 400:1 y por debajo de 200:1 desde septiembre en adelante.

Qué vemos nosotros como ISP…

- **User-Agents falseados:** bots que se disfrazan de Chrome, Safari, móviles...
- **Ignoran robots.txt:** da igual lo que pongas, pasan igualmente…
- **Rotan IPs constantemente:** residenciales, proxies, cloud providers…
- **Crawlers sin identificar:** no declaran quiénes son ni qué quieren…
- **Mismo bot, múltiples identidades**: un solo crawler usa 10+ user-agents distintos…
- **Scraping agresivo en horarios de alta actividad**: NO buenas prácticas…
- **Aumento progresivo del tráfico**: mismos clientes + tráfico…

DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Qué vemos nosotros como ISP…

#	HITS	VISITANTES	TX. AMOUNT	PROM. T.S.	CUM. T.S.	MAX. T.S.	DATOS
MIN.	1 (00,04%)	1 (00,18%)	98 B (00,00%)	–	804.00 us	804.00 us	–
MAX.	522 (21,07%)	189 (33,22%)	33.6 MiB (35,03%)	–	21.90 s	4.91 s	–
AVG.	20 (00,81%)	4 (00,70%)	811.71 KiB (00,83%)	25.82 ms	528.49 ms	528.49 ms	–
1	1240 (50.06%)	206 (36.14%)	43.5 MiB (45.32%)	27.42 ms	34.01 s	3.69 s	Chrome
2	522 (21.07%)	189 (33.16%)	33.6 MiB (35.03%)	8.74 ms	4.56 s	302.14 ms	Unknown
3	162 (06.54%)	16 (02.81%)	4.8 MiB (05.03%)	51.66 ms	8.37 s	1.93 s	Firefox
4	122 (04.93%)	18 (03.16%)	2.9 MiB (03.01%)	79.71 ms	9.72 s	1.83 s	Edge
5	122 (04.93%)	34 (05.96%)	2.7 MiB (02.85%)	3.23 ms	393.80 ms	9.35 ms	Others
6	107 (04.32%)	39 (06.84%)	686.2 KiB (00.70%)	3.49 ms	373.67 ms	13.16 ms	Crawlers
7	83 (03.35%)	34 (05.96%)	2.8 MiB (02.94%)	5.43 ms	451.11 ms	33.31 ms	Safari
TOT.	2477	569	95.91 MiB	–	1.07 m	1.07 m	121

Estimaciones:

Optimista (Chrome = 100% humano):

1. Humano = ~1.620 hits → 65%
2. Bot = ~860 hits → 35%

Realista (Chrome = 60% humano, 30% bot, 10% dudoso):

- Humano= ~1.125 hits → 45%
- Bot = ~1.230 hits → 50%
- Dudoso= ~125 hits → 5%

DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Qué vemos nosotros como ISP...

Spamhaus ✓
@spamhaus

Mostrar traducción

An individual, Zhenyun Sun (...te.company-information.service.gov.uk/officers/svz68...), is registering UK "fibre ISPs" at Companies House at an unusual rate. On the surface, they could pass for legitimate broadband providers. But look closer, and the picture soon changes 🕵️ ...

Some of these companies are assigned an ASN, sharing the same abuse contact: onesproxy[.]com. ⤵️

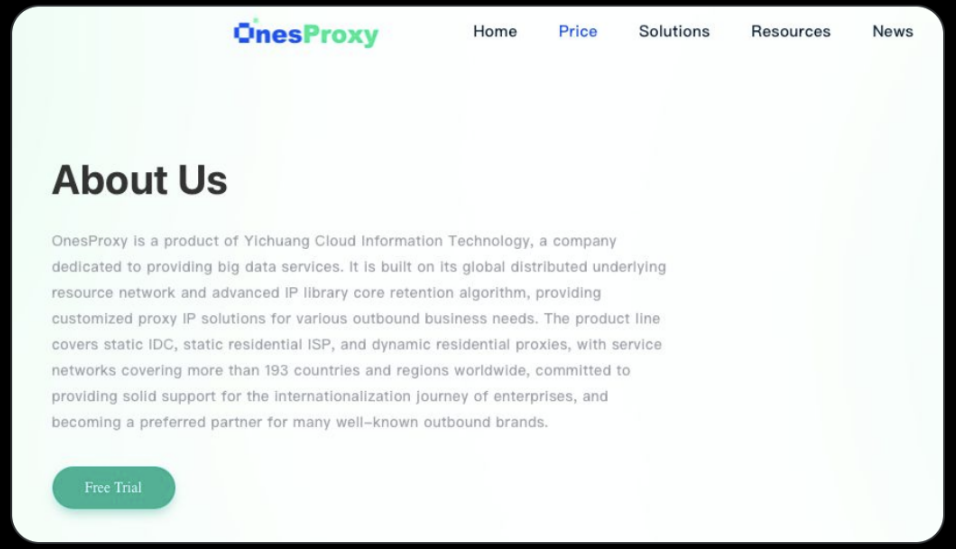
```
Abuse contact for 'AS203048' is 'xh@onesproxy.com'
Abuse contact for 'AS203054' is 'xh@onesproxy.com'
Abuse contact for 'AS203057' is 'xh@onesproxy.com'
Abuse contact for 'AS203075' is 'xh@onesproxy.com'
Abuse contact for 'AS203076' is 'xh@onesproxy.com'
Abuse contact for 'AS203094' is 'xh@onesproxy.com'
Abuse contact for 'AS203106' is 'xh@onesproxy.com'
Abuse contact for 'AS203109' is 'xh@onesproxy.com'
Abuse contact for 'AS203113' is 'xh@onesproxy.com'
Abuse contact for 'AS203146' is 'xh@onesproxy.com'
Abuse contact for 'AS203149' is 'xh@onesproxy.com'
```

3:35 p. m. · 19 mar. 2026 · **5.845** Visualizaciones

Spamhaus ✓ @spamhaus · 19 mar.

This same company openly markets itself as a Chinese provider of "residential proxies." These ASNs are registered at @ripencc as assigned to ISPs delivering fibre to UK homes.

One possible explanation is that this setup makes proxy traffic appear to originate from genuine residential broadband customers. But it may not necessarily be for malicious purposes. Instead, it could be targeting SEO and those who want to "cheat the system" by simulating traffic from a large pool of users for marketing or analytics purposes. ⤵️



2 5 14 2 mil

DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Qué vemos nosotros como ISP

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Qué vemos nosotros como ISP…

Spamhaus
@spamhaus

Mostrar traducción

An individual, Zhenyun
officers/svz68...), is reg
unusual rate. On the su
providers. But look clo

Some of these compa
contact: onesproxy[.

```
Abuse contact for 'AS203054' is 'xh@onesproxy.com'
Abuse contact for 'AS203057' is 'xh@onesproxy.com'
Abuse contact for 'AS203075' is 'xh@onesproxy.com'
Abuse contact for 'AS203076' is 'xh@onesproxy.com'
Abuse contact for 'AS203094' is 'xh@onesproxy.com'
Abuse contact for 'AS203106' is 'xh@onesproxy.com'
Abuse contact for 'AS203109' is 'xh@onesproxy.com'
Abuse contact for 'AS203113' is 'xh@onesproxy.com'
Abuse contact for 'AS203146' is 'xh@onesproxy.com'
Abuse contact for 'AS203149' is 'xh@onesproxy.com'
```

3:35 p. m. · 19 mar. 2026 · **5.845** Visualizaciones

Europol and international partners disrupt ‘SocksEscort’ proxy service

Joint operation targeted malicious proxy service exploiting residential routers worldwide

Spamhaus @spamhaus · 19 mar.

This same company openly markets itself as a Chinese provider of "residential proxies." These ASNs are registered at @ripencc as assigned to ISPs delivering fibre to UK homes.

…ssible explanation is that this setup makes proxy traffic appear to …sidential broadband customers. But it may not …tead, it could be targeting SEO …ffic from a large

…ources News

OnesProxy is a product of …
dedicated to providing big data services. It is built …
resource network and advanced IP library core retention algorithm, providing …
customized proxy IP solutions for various outbound business needs. The product line covers static IDC, static residential ISP, and dynamic residential proxies, with service networks covering more than 193 countries and regions worldwide, committed to providing solid support for the internationalization journey of enterprises, and becoming a preferred partner for many well-known outbound brands.

Free Trial

2 5 14 2 mil

DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Qué vemos nosotros como ISP

DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

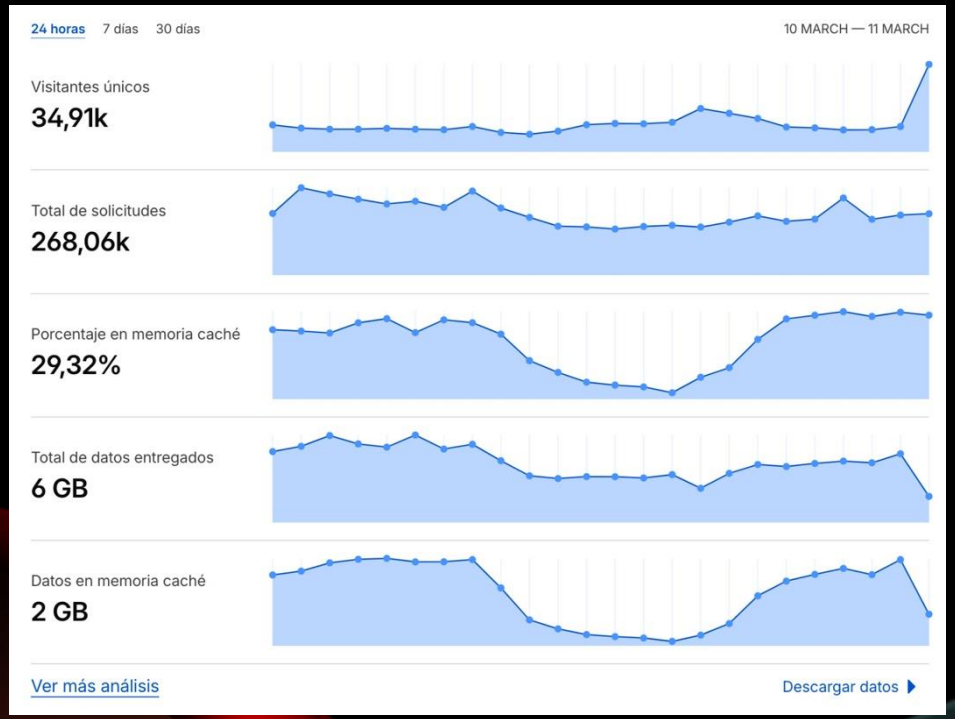
Qué vemos nosotros como ISP

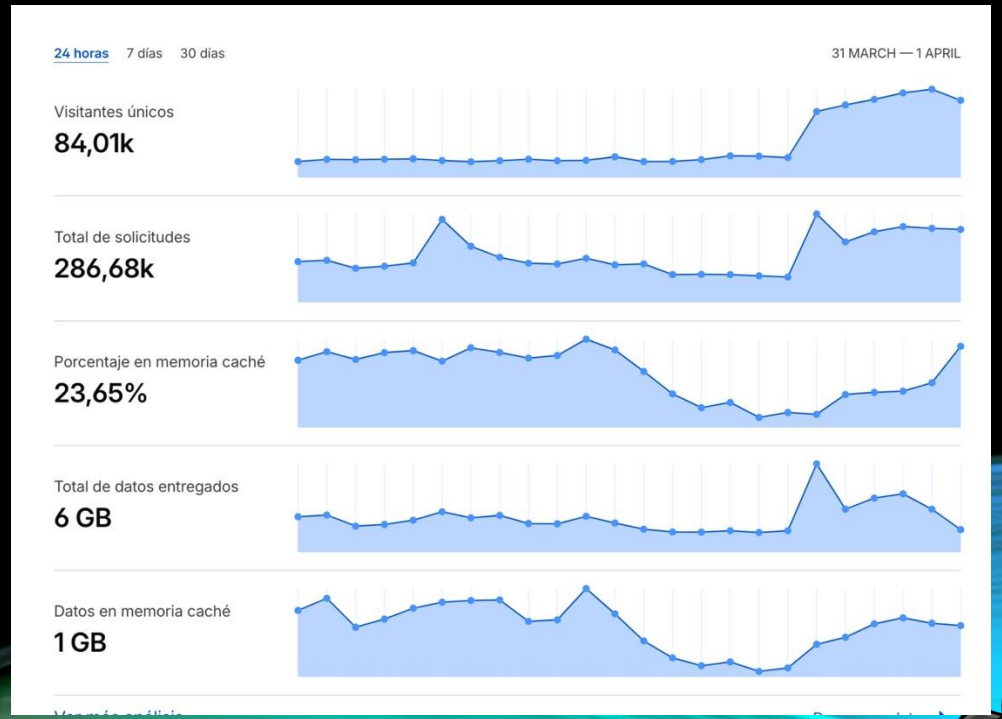
DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Qué ven nuestros clientes…

Agencias de Marketing
Departamentos de E-Commerce
Empresas digitales





DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Qué ven nuestros clientes…

Problemas de rendimiento: **Prestashop**

Si tienes una tienda online en PrestaShop, es muy probable que en los últimos meses hayas notado caídas del servidor, lentitud inesperada o picos de consumo de recursos sin una causa aparente. No eres el único. Estamos viendo este problema cada vez más en tiendas de todos los tamaños, y tiene un culpable claro: los rastreadores automáticos de inteligencia artificial y los bots de scraping.

¿Qué está pasando exactamente?

Los motores de IA, los rastreadores de precios y otros bots recorren Internet de forma continua para recopilar información de las tiendas online. No es nada nuevo, pero la intensidad ha crecido enormemente en los últimos tiempos, y algunos de estos bots están aprovechando **el parámetro `resultsPerPage`**.

Este parámetro es el que controla cuántos productos muestra una página de categoría o de resultados de búsqueda. El problema es que PrestaShop no pone ningún límite a este valor por defecto. Eso significa que un bot puede hacer una petición como esta:

```
https://tutienda.com/categoria?resultsPerPage=99999
```

¿Y qué ocurre? Que PrestaShop obedientemente intenta recuperar de la base de datos los 99.999 productos solicitados. Si tu categoría tiene miles de referencias, la consulta es tan pesada que puede saturar el servidor y dejarte la tienda caída durante minutos… o más.

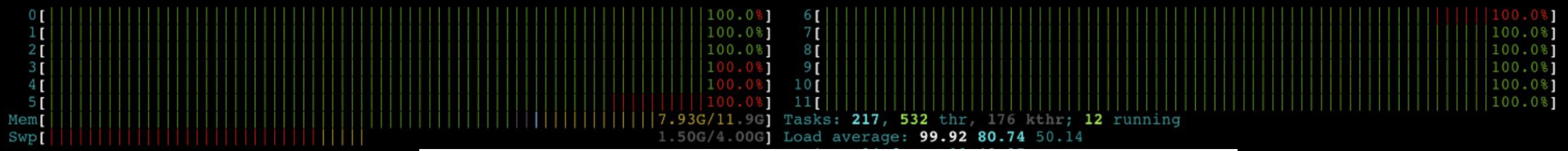
No es un ataque sofisticado. No hace falta ningún conocimiento especial. Cualquier bot —o persona con malas intenciones— puede hacerlo con una simple URL manipulada. Y lo estamos viendo en tiendas reales, con consecuencias reales.

DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Qué ven nuestros clientes…

Problemas de rendimiento: **Prestashop**



¿Qué está pasando exactamente?

Los motores de IA, los rastreadores de precios y otros bots recorren Internet de forma continua para recopilar información de las tiendas online. No es nada nuevo, pero la intensidad ha crecido enormemente en los últimos tiempos, y algunos de estos bots están aprovechando **el parámetro `resultsPerPage`**.

Este parámetro es el que controla cuántos productos muestra una página de categoría o de resultados de búsqueda. El problema es que PrestaShop no pone ningún límite a este valor por defecto. Eso significa que un bot puede hacer una petición como esta:

```
https://tutienda.com/categoria?resultsPerPage=99999
```

¿Y qué ocurre? Que PrestaShop obedientemente intenta recuperar de la base de datos los 99.999 productos solicitados. Si tu categoría tiene miles de referencias, la consulta es tan pesada que puede saturar el servidor y dejarte la tienda caída durante minutos… o más.

No es un ataque sofisticado. No hace falta ningún conocimiento especial. Cualquier bot —o persona con malas intenciones— puede hacerlo con una simple URL manipulada. Y lo estamos viendo en tiendas reales, con consecuencias reales.

DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Qué ven nuestros clientes…

Problemas de rendimiento: **Prestashop**

DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Qué ven nuestros clientes…

Problemas de rendimiento: **Prestashop**

+35%

tickets

DMNTR
NETWORK SOLUTIONS

Qué ven nuestros clientes…

Aumento de costes: **Caso Connectif**

Plataforma de “marketing automation” para ecommerce

Trackea cada visitante de tu tienda online (anónimos incluidos), monta perfiles, lanza emails, push, pop-ups personalizados... y **cobra por "actividades"**, es decir, por cada interacción que registra.

Concepto	Periodo	Unidades	Precio Unitario	Total
E20k-A250k	08/04/2026-07/05/2026	1	133,00 €	133,00 €
Excesos Actividades	08/03/2026-07/04/2026	228.028	0,0002 €	45,61 €

DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Qué ven los clientes de nuestros clientes…

Vaya... no se puede obtener acceso a

www.dominio.com tardó demasiado tiempo en responder

Prueba a:

- Comprobando la conexión
- Comprobando el proxy y el firewall
- Ejecutar el Diagnóstico de red de Windows.

ERR_CONNECTION_TIMED_OUT

Detalles

DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Qué hacer: ¡A los problemas soluciones!

A nivel de red…

- Bloqueo de ASNs con proxies residenciales detectados
- Geoblocking por país de origen
- Bloqueo de rangos IP de providers conocidos por hospedar bots
- Listas negras de IPs compartidas / feeds de threat intelligence

Qué hacer: ¡A los problemas soluciones!

A nivel de red…

- ~~Bloqueo de ASNs con proxies residenciales detectados~~
- Geoblocking por país de origen
- Bloqueo de rangos IP de providers conocidos por hospedar bots
- Listas negras de IPs compartidas / feeds de threat intelligence

MALWARE Y AMENAZAS

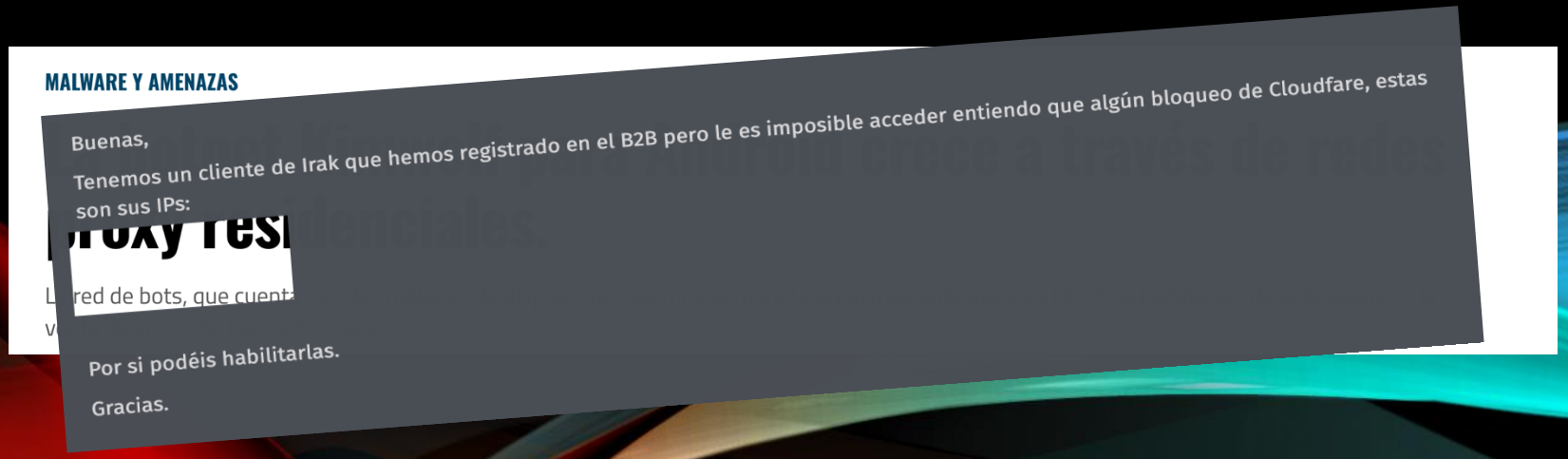
La botnet Kimwolf para Android crece a través de redes proxy residenciales.

La red de bots, que cuenta con dos millones de dispositivos, permite la monetización mediante ataques DDoS, la instalación de aplicaciones y la venta de ancho de banda de proxy.

Qué hacer: ¡A los problemas soluciones!

A nivel de red…

- ~~Bloqueo de ASNs con proxies residenciales detectados~~
- ~~Geoblocking por país de origen~~
- Bloqueo de rangos IP de providers conocidos por hospedar bots
- Listas negras de IPs compartidas / feeds de threat intelligence

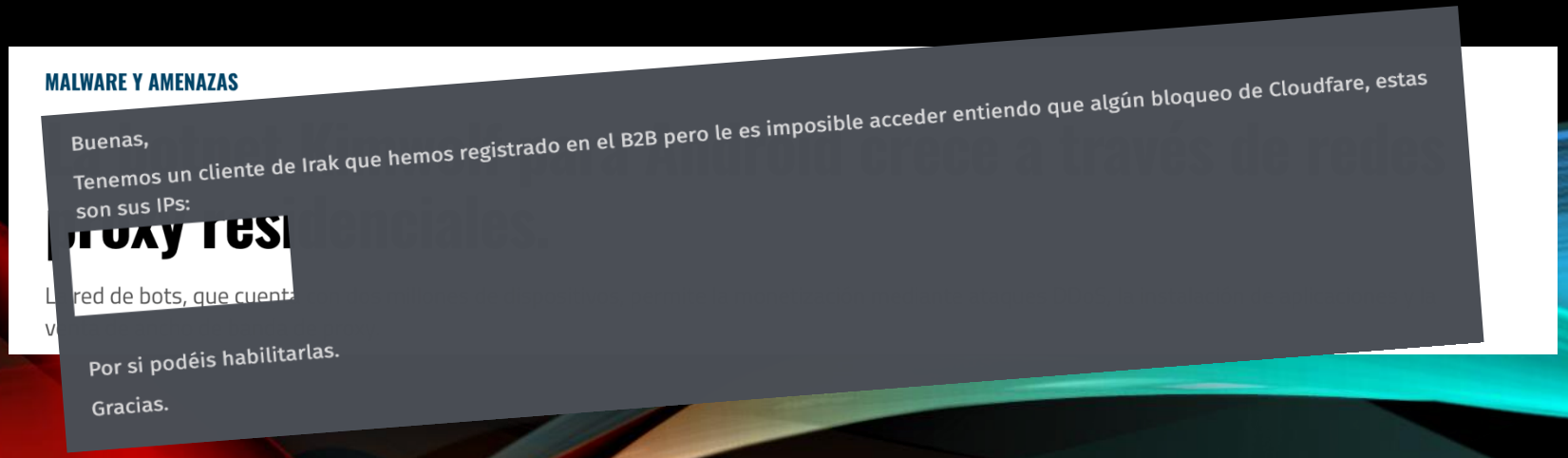


DMNTR
NETWORK SOLUTIONS

Qué hacer: ¡A los problemas soluciones!

A nivel de red…

- ~~Bloqueo de ASNs con proxies residenciales detectados~~
- ~~Geoblocking por país de origen~~
- ~~Bloqueo de rangos IP de providers conocidos por hospedar bots~~
- Listas negras de IPs compartidas / feeds de threat intelligence

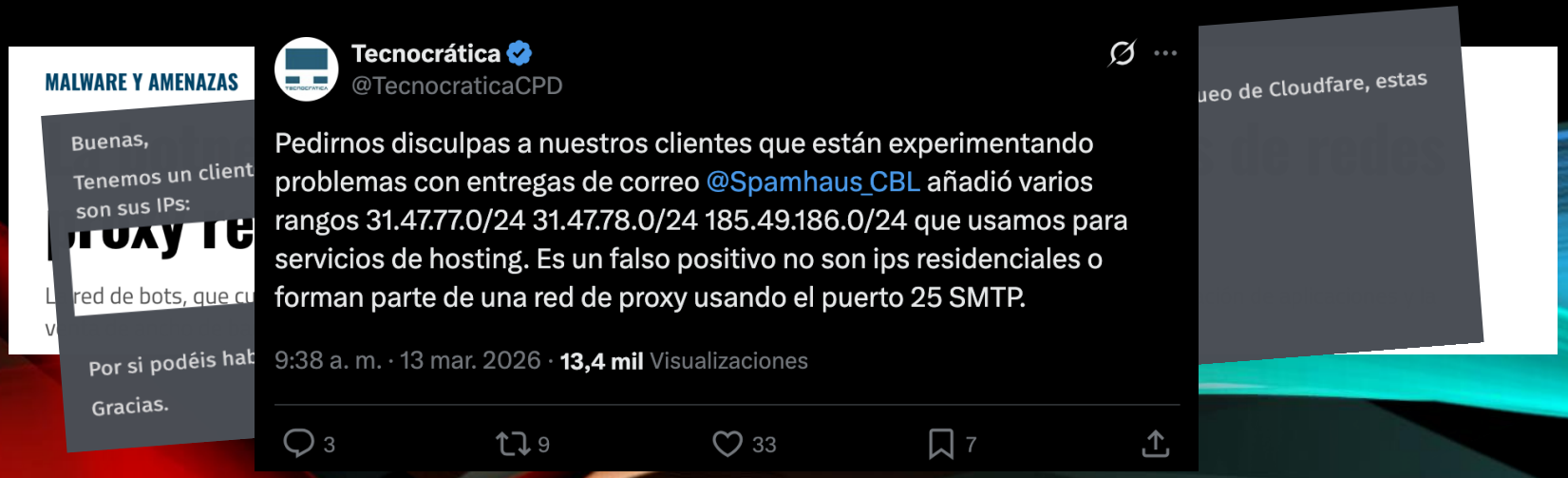


DMNTR
NETWORK SOLUTIONS

Qué hacer: ¡A los problemas soluciones!

A nivel de red…

- ~~Bloqueo de ASNs con proxies residenciales detectados~~
- ~~Geoblocking por país de origen~~
- ~~Bloqueo de rangos IP de providers conocidos por hospedar bots~~
- ~~Listas negras de IPs compartidas / feeds de threat intelligence~~



DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Qué hacer: ¡A los problemas soluciones!

- ~~Blo~~
- ~~Ge~~
- ~~Blo~~ ...ots
- ~~List~~ ...e

DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Qué hacer: ¡A los problemas soluciones!

Spamhaus
@spamhaus

Mostrar traducción

An individual, Zhenyun Sun (...te.company-information.service.gov.uk/officers/svz68...), is registering UK "fibre ISPs" at Companies House at an unusual rate. On the surface, they could pass for legitimate broadband providers. But look closer, and the picture soon changes 🕵️ ...

Some of these companies are assigned an ASN, sharing the same abuse contact: onesproxy[.]com. ⤵️

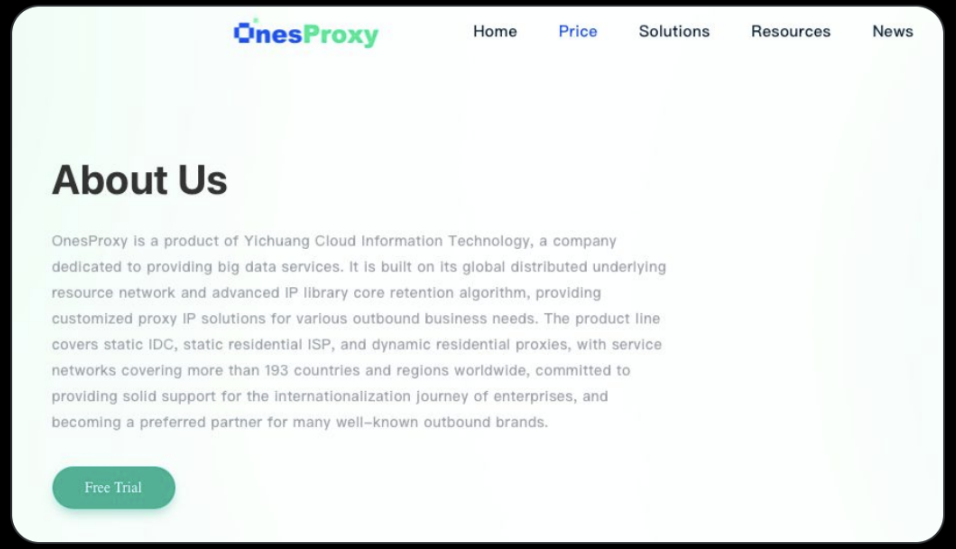
```
Abuse contact for 'AS203048' is 'xh@onesproxy.com'
Abuse contact for 'AS203054' is 'xh@onesproxy.com'
Abuse contact for 'AS203057' is 'xh@onesproxy.com'
Abuse contact for 'AS203075' is 'xh@onesproxy.com'
Abuse contact for 'AS203076' is 'xh@onesproxy.com'
Abuse contact for 'AS203094' is 'xh@onesproxy.com'
Abuse contact for 'AS203106' is 'xh@onesproxy.com'
Abuse contact for 'AS203109' is 'xh@onesproxy.com'
Abuse contact for 'AS203113' is 'xh@onesproxy.com'
Abuse contact for 'AS203146' is 'xh@onesproxy.com'
Abuse contact for 'AS203149' is 'xh@onesproxy.com'
```

3:35 p. m. · 19 mar. 2026 · **5.845** Visualizaciones

Spamhaus @spamhaus · 19 mar.

This same company openly markets itself as a Chinese provider of "residential proxies." These ASNs are registered at @ripencc as assigned to ISPs delivering fibre to UK homes.

One possible explanation is that this setup makes proxy traffic appear to originate from genuine residential broadband customers. But it may not necessarily be for malicious purposes. Instead, it could be targeting SEO and those who want to "cheat the system" by simulating traffic from a large pool of users for marketing or analytics purposes. ⤵️



2 5 14 2 mil

DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Qué hacer: ¡A los problemas soluciones!

BLOCK!!!

DMNTR
NETWORK SOLUTIONS

Qué hacer: ¡A los problemas soluciones!

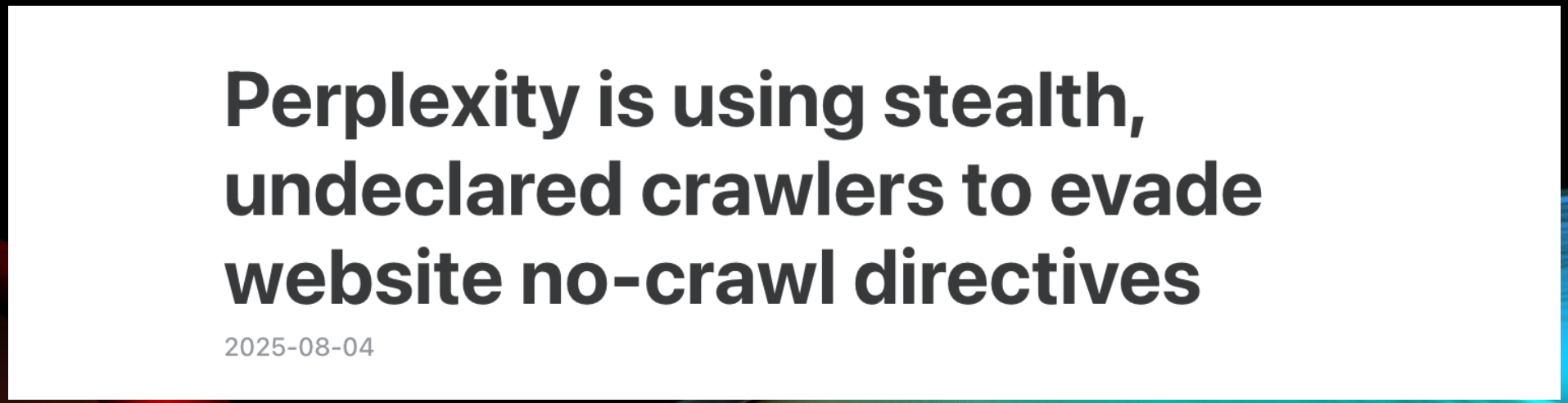
A nivel de servidor…

- **robots.txt actualizado** con todos los crawlers de IA conocidos
- **ModSEC:** Reglas AntiIA implementadas a nivel servidor
- **Honeypots:** URLs trampa para detectar crawlers que ignoran robots.txt

Qué hacer: ¡A los problemas soluciones!

A nivel de servidor…

- ~~**robots.txt actualizado** con todos los crawlers de IA conocidos~~
- **ModSEC:** Reglas AntiIA implementadas a nivel servidor
- **Honeypots:** URLs trampa para detectar crawlers que ignoran robots.txt



Qué hacer: ¡A los problemas soluciones!

A nivel de servidor…

- ~~**robots.txt actualizado** con todos los crawlers de IA conocidos~~
- ~~**ModSEC:** Reglas AntiIA implementadas a nivel servidor~~
- **Honeypots:** URLs trampa para detectar crawlers que ignoran robots.txt

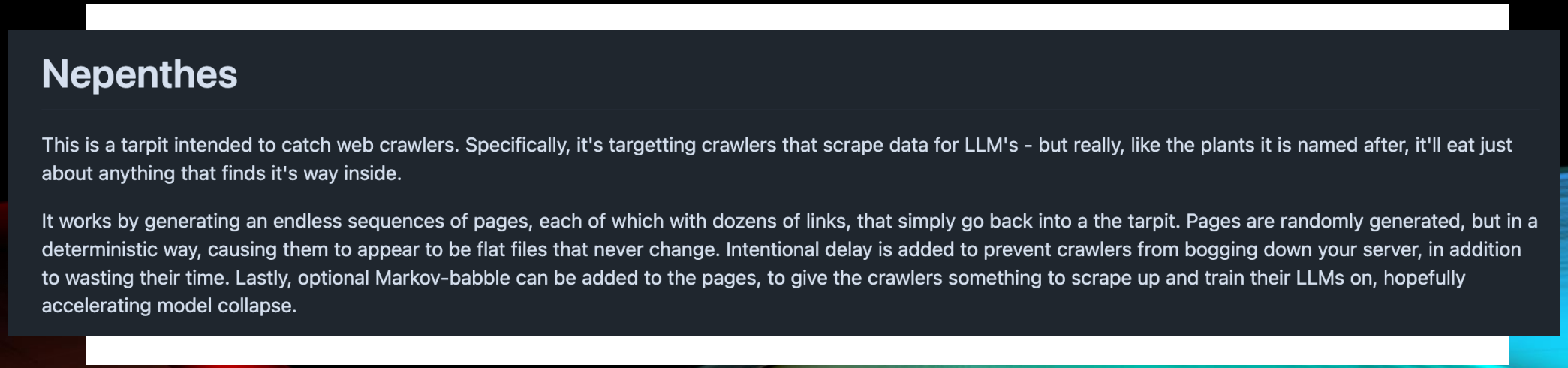
Perplexity is using stealth, undeclared crawlers to evade website no-crawl directives

2025-08-04

Qué hacer: ¡A los problemas soluciones!

A nivel de servidor…

- **robots.txt actualizado** con todos los crawlers de IA conocidos
- **ModSEC:** Reglas AntiIA implementadas a nivel servidor
- **Honeypots:** URLs trampa para detectar crawlers que ignoran robots.txt



DMNTR
NETWORK SOLUTIONS

Qué hacer: ¡A los problemas soluciones!

A nivel de clientes…

- Filtrado de tráfico bot en server-side tagging
- Plugins específicos antiscrapping
- Segmentación de tráfico real vs automatizado en dashboards
- Alertas de picos de tráfico anómalos

DMNTR
NETWORK SOLUTIONS

Lo que mejor nos funciona: WAF (a veces no…)

WAFs cloud (el tráfico pasa por ellos):

- **Cloudflare:** Bot Management, AI Labyrinth, AI Crawl Control, **Pay Per Crawl**. Protege más del 20% de la web. Plan Free con protección básica.
- **Akamai:** El veterano. App & API Protector + Bot Manager. 400+ investigadores de seguridad. El más caro pero el más completo para grandes empresas.
- **Imperva:** Near-zero false positives, el 90% de clientes despliegan en modo bloqueo directo. Híbrido cloud + on-prem. Los del Bad Bot Report que usamos en la charla.
- **Fastly:** Next-Gen WAF con SmartParse. Fuerte en API protection.
- **AWS WAF:** Pay-as-you-go si ya estás en AWS.
- **Sucuri:** Popular en WordPress/CMS. Más básico pero asequible.

Lo que mejor nos funciona: WAF (a veces no…)

WAFs

- **Cloudfl**
  20% de
- **Akama**
  El más
- **Imperv**
  Híbrido
- **Fastly:**
- **AWS W**
- **Sucuri:**

más del

guridad.

lirecto.

DMNTR
NETWORK SOLUTIONS

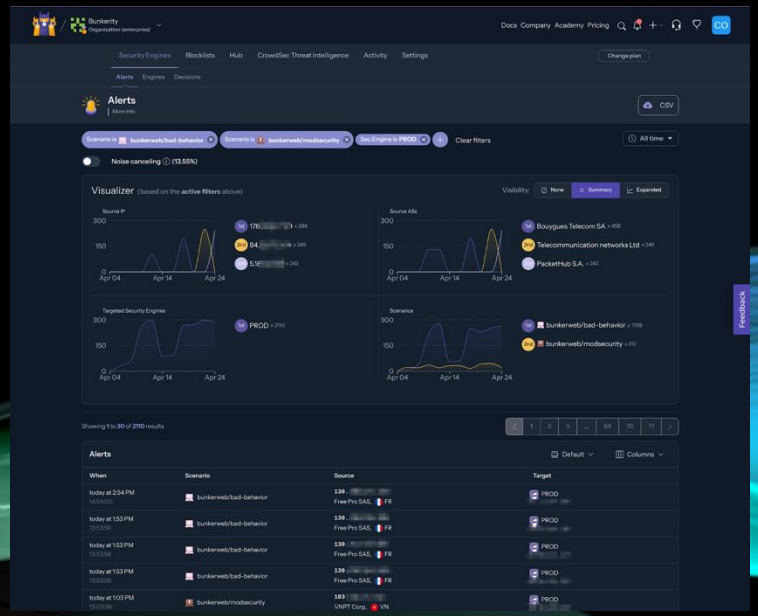
CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Lo que mejor nos funciona: WAF

WAFs ON-PREM (el tráfico solo pasa por tí):

- **ModSecurity** + OWASP CRS: El clásico. El más desplegado del mundo.
- **Coraza:** El sucesor moderno de ModSecurity en Go.
- **SafeLine:** Interfaz web moderna, detección semántica con IA, anti-bot con fingerprinting.
- **BunkerWeb:** Nginx dockerizado con CRS integrado. "Like-Cloudflare pero tuyo".

- **F5 BIG-IP ASM / Advanced WAF**
- **Imperva WAF Gateway (on-prem)**
- **Fortinet FortiWeb**
- **Barracuda WAF**
- **Wallarm**
- **Radware AppWall**



DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Lo que mejor nos funciona: WAF

WAFs ON-PREM (el tráfico sigue pasando por tí):

- **Mantenimiento:** requieren mantenimiento continuo (upgrades, actualización de reglas, falsos positivos, etc).
- **Necesidad de monitorización continua:** Equipo dedicado a monitorizar, no es difícil que elimines visitas legítimas sin querer (jodemos al 5%...).
- **Bugs:** Al ser productos "de nicho" la comunidad es pequeña y a veces andas a cabezazos con un bug…
- **Dedicar un equipo a ello:** no queda otra que tener a gente encima…
- **Nadie dijo que la soberanía tecnológica fuera fácil…**

Lo que está llegando…

¿Cambio de paradigma?

Google está roto y provoca el

Durante 20 años Google nos dio enlaces, pero ha decidido romper con el pasado. Ahora quiere que compres sin visitar ni una sola web

- Presenta el 'Universal Commerce Protocol', un estándar para que su IA compre por ti sin visitar la web del vendedor
- Gemini deja de ser un chatbot que responde para convertirse en un asistente que ejecuta acciones

DMNTR
NETWORK SOLUTIONS

Lo que está llegando…

¿Cambio de paradigma?

Google está roto y provoca el

Durante 20 años Google nos dio enlaces, pero ha decidido romper con el pasado. Ahora quiere que compres sin visitar ni una sola web

- Presenta el 'Universal Commerce Protocol', un estándar para que su IA compre por ti sin visitar la web del vendedor
- Gemini deja de ser un chatbot que responde para convertirse en un asistente que ejecuta acciones

DMNTR
NETWORK SOLUTIONS

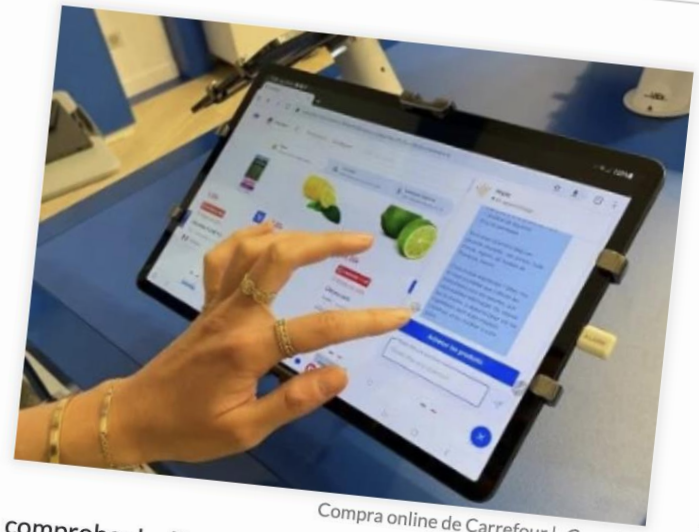
Lo que está llegando…

¿Cambio de paradigma?

Carrefour, primer minorista europeo en ofrecer compras en ChatGPT

Permite a los usuarios de la plataforma de IA acceder a las ofertas y servicios del retailer sin salir de su interfaz

26/03/2026



Compra online de Carrefour | *Carrefour*

infoRETAIL.- **Carrefour** ha dado hoy un nuevo paso en su estrategia de transformación digital al permitir que los usuarios de **ChatGPT** accedan directamente a las ofertas y servicios de la compañía de distribución sin salir de su interfaz.

Con este servicio, lanzado inicialmente en el mercado francés, Carrefour se convierte en el **primer minorista europeo en ofrecer compras en ChatGPT**, tal y como ha confirmado el propio grupo.

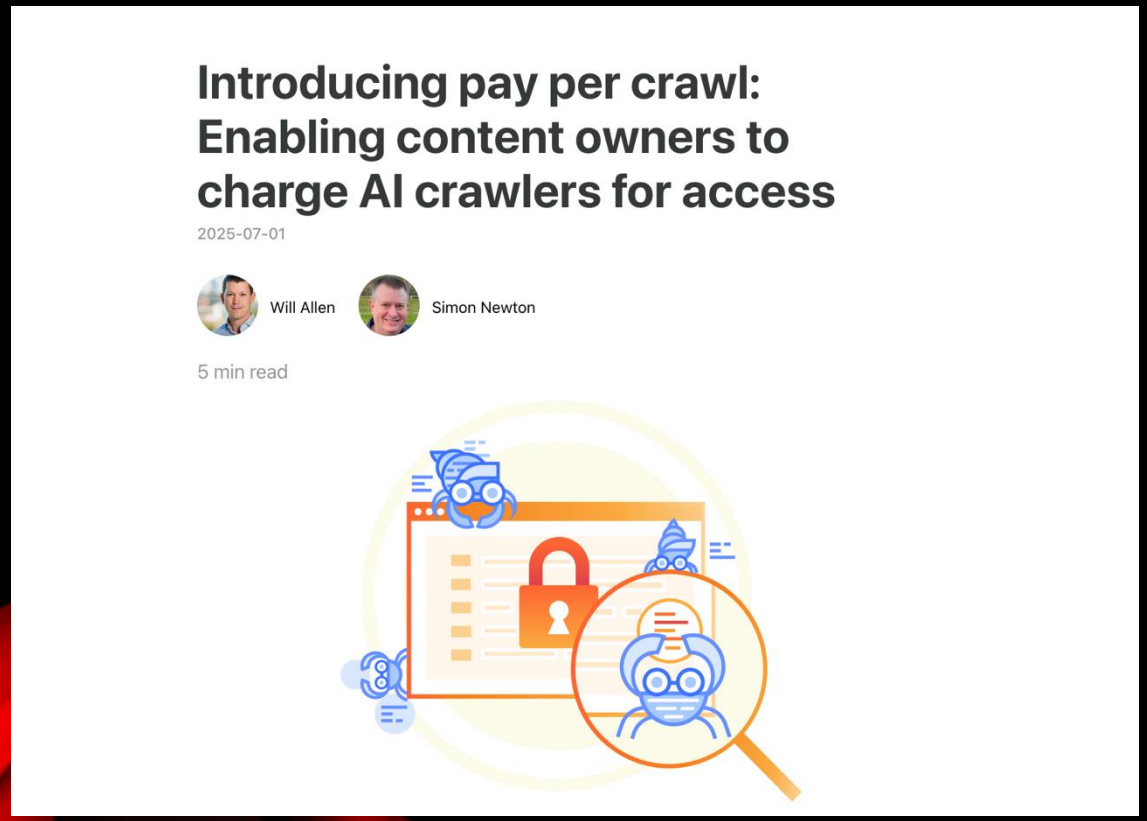
Así, a partir de hoy, los usuarios pueden conversar con ChatGPT para obtener ideas de **recetas**, comprobar la **disponibilidad** de productos en la tienda o **crear una cesta de la compra** según sus necesidades y **elegir un método de entrega**, antes de finalizar y pagar el pedido en el portal *online* de Carrefour.

DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO

Lo que está llegando…

¿Pay per crawl?



Introducing pay per crawl: Enabling content owners to charge AI crawlers for access

2025-07-01

Will Allen Simon Newton

5 min read

HTTP 402

RFC 2068 (1997): HTTP/1.1 original. 402 Payment Required This code is reserved for future use.

RFC 2616 (1999): "Reserved for future use".

RFC 7231 (2014): no existe convención de uso estándar y diferentes sistemas lo usan en diferentes contextos.

RFC 9110 (2022): Sigue "Reserved for future use".

DMNTR NETWORK SOLUTIONS

Lo que está por llegar… (o ha llegado ya…)

¿Agentes? ¿Comercio agéntico?

1. **Agentes autónomos**
- El tráfico de IA agéntica creció un 7.851% en 2025.

2. Comercio agéntico
- El tráfico de IA a sitios de retail en EEUU creció un 805% en el Black Friday 2025. Ekamoira

3. Protocolos abiertos para agentes
- Agentic Commerce Protocol (ACP), Universal Commerce Protocol (UCP), x402…
- Estándares para que los agentes descubran productos, negocien y compren.
- Ya hay un Draft Experimental en el IETF para descubrir recursos x402 vía DNS TXT records…

4. El fin del modelo "human or bot"
- El comportamiento de un agente legítimo comprando y el de un bot de fraude puede ser idéntico.

Ya no vale "*bot = malo, humano = bueno*". Necesitamos evaluar intención.

Lo que está por llegar… (o ha llegado ya…)

Multiplicación de Tráfico

Cada compra que se delega a un agente multiplica por 1.000x las peticiones.

Los operadores vamos a tener que redimensionar para un internet donde una persona genera el tráfico de mil.

"Una persona comprando una cámara visita 5 webs. Un agente de IA haciendo lo mismo visita 5.000. En 10 segundos."

Hoy facturas un puerto de 1 Gbps. Mismo cliente, mismos usuarios -> necesitará 10, no porque haya crecido su empresa.
Porque sus empleados han descubierto los agentes.

DMNTR
NETWORK SOLUTIONS

CUANDO EL 90% DE TU TRÁFICO NO ES REAL

Lo que está por llegar… (o ha llegado ya…)

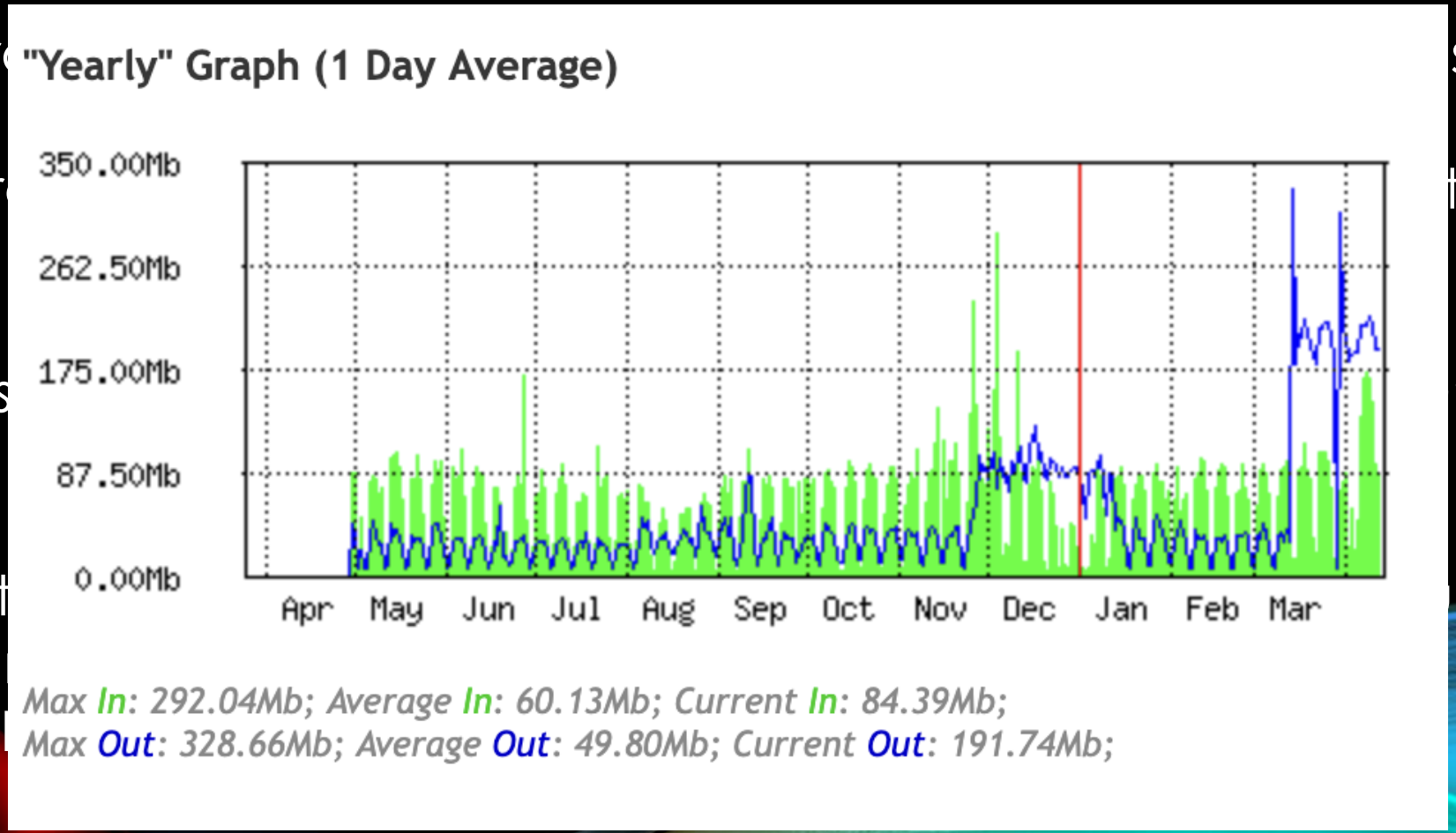
Multiplicación de Tráfico

Cada compr s peticiones.

Los operador t donde una

"Una pers te de IA

Hoy fact arios ->



DMNTR
NETWORK SOLUTIONS

Los retos…

Redimensionar infraestructura para un tráfico que **crece x8 más rápido** que tus clientes humanos.

Ofrecer servicios de protección anti-bot **sin romper el SEO ni el comercio agéntico** de tus clientes.

Detectar crawlers que falsean identidad, rotan IPs residenciales y se disfrazan de tus propios usuarios.

Definir políticas de peering y tránsito diferenciadas para tráfico de IA cuando ni siquiera podemos identificarlo de forma fiable.

Convertir la visibilidad que tenemos sobre el tráfico en un servicio de valor añadido antes de que Cloudflare lo haga por nosotros.

Otras soluciones…

GRACIAS

@weareDMNTRs

https://t.me/gentedeIT

DMNTR
NETWORK SOLUTIONS