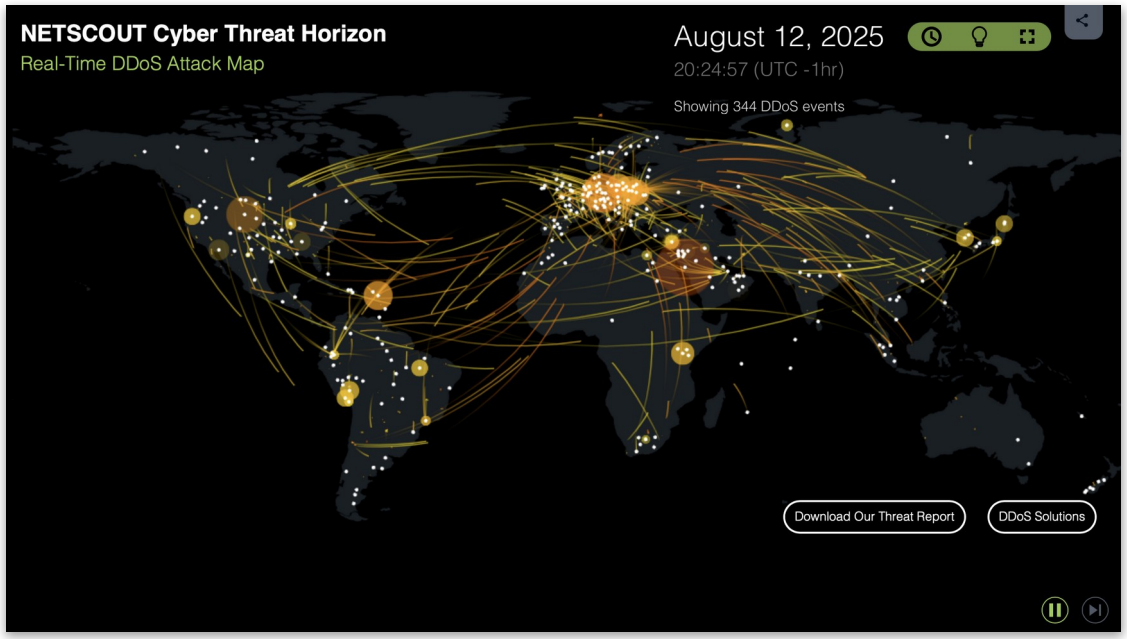
Guardians of the Connected World

+150T
Mitigación

+150M
Flujos/sec

1,5M
Mitigaciones (2H2025)

700
Clientes



800Tbps
Peering y Transito

8.088.463
DDoS Attacks (2H2025)

+3000
Empresas

+200
Paises

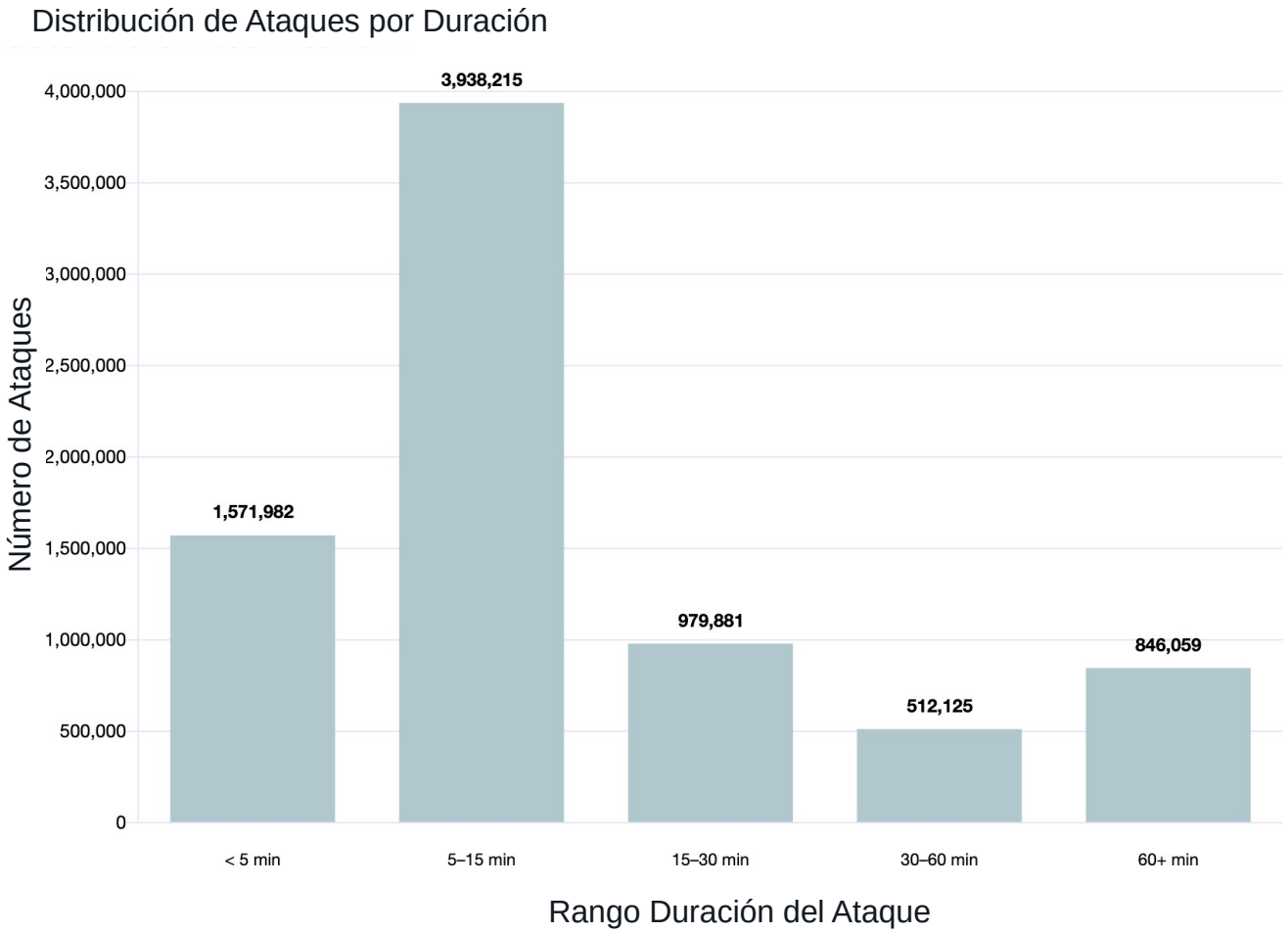
Lighthouse
DARPA

NETSCOUT®

Guardians of the Connected World

AIF
ATLAS

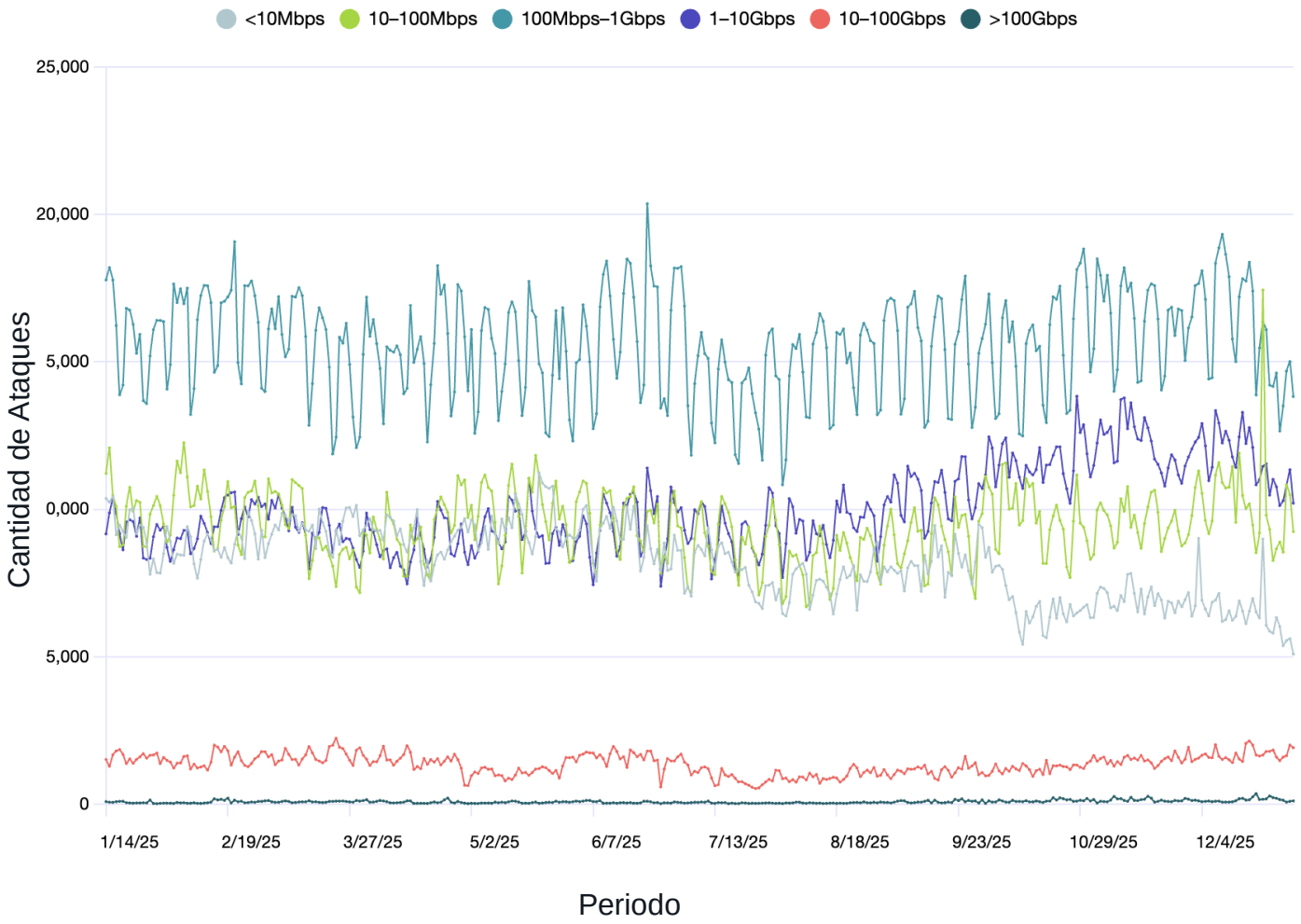
Tendencia de Ataques DDoS



Duración por Porcentaje	
< 5 min	19.88%
5-15 min	49.79%
15-30 min	12.39%
30-60 min	6.48%
60+ min	10.7%

69.7%

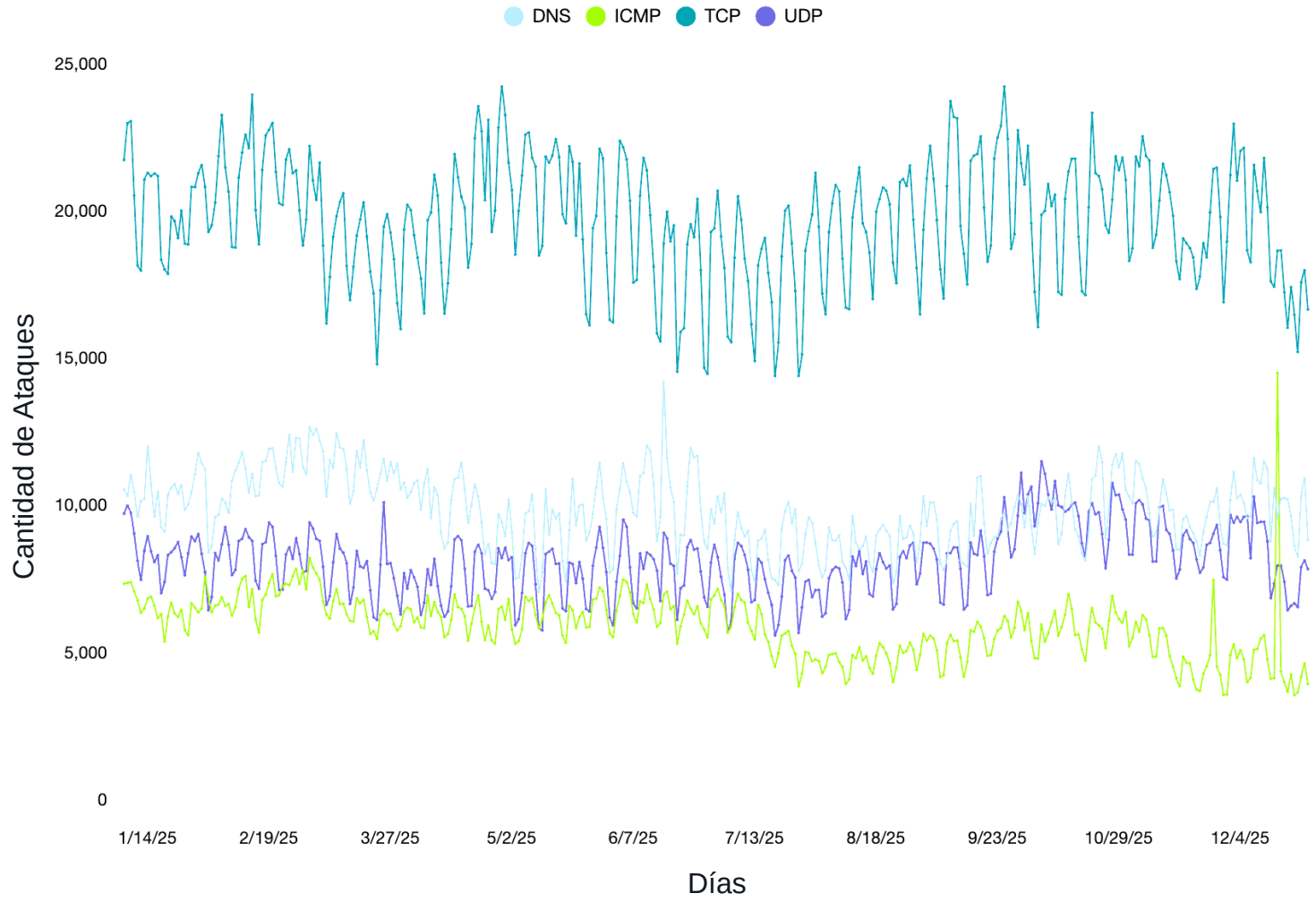
Tendencia de Ancho de Banda Ataques DDoS



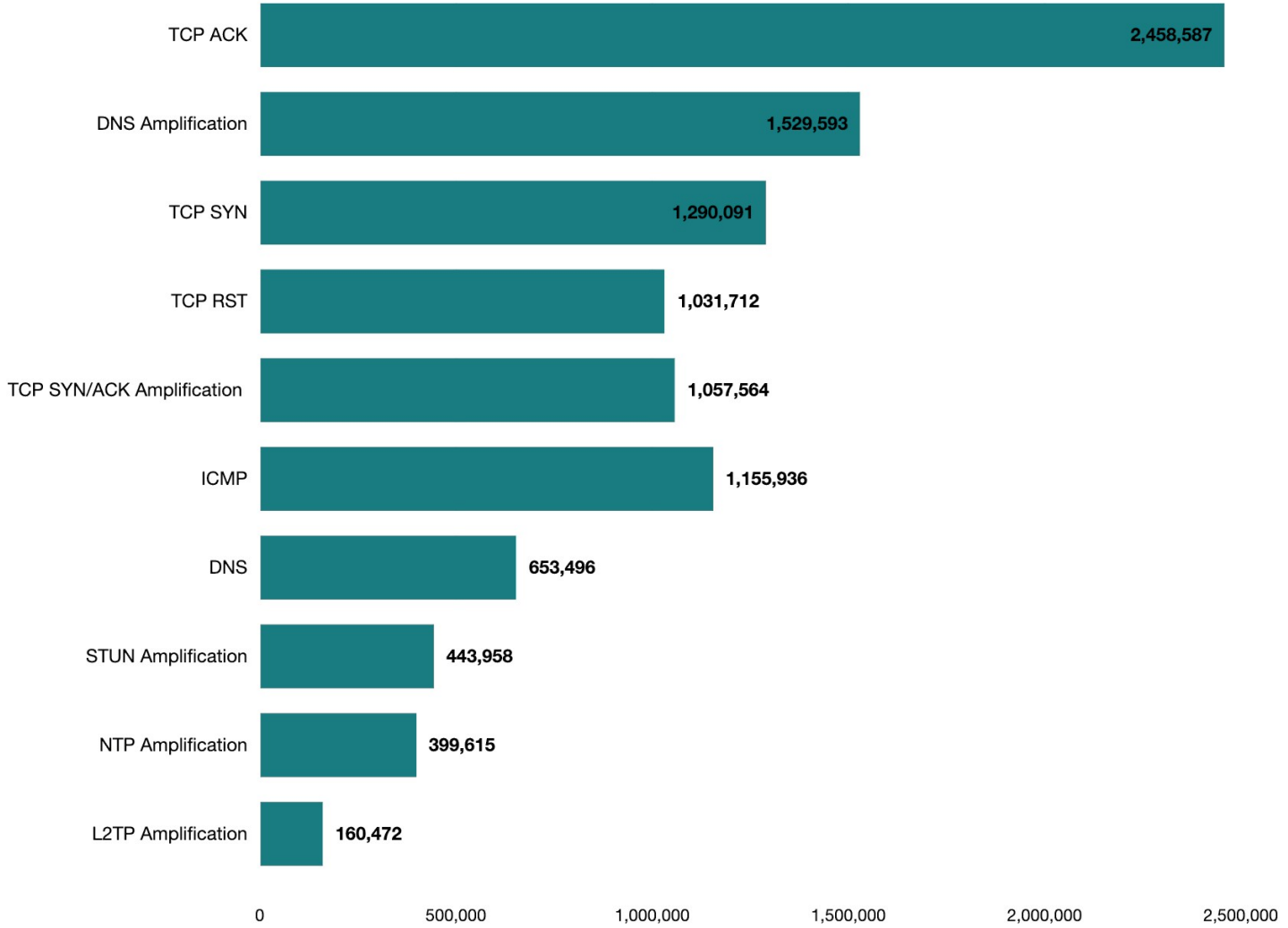
Ancho de Banda	
<10Mbps	16.5%
10–100Mbps	21.04%
100Mbps–1Gbps	35.04%
1–10Gbps	24.44%
10–100Gbps	2.79%
>100Gbps	0.19%

97%
80.5%
59.5%

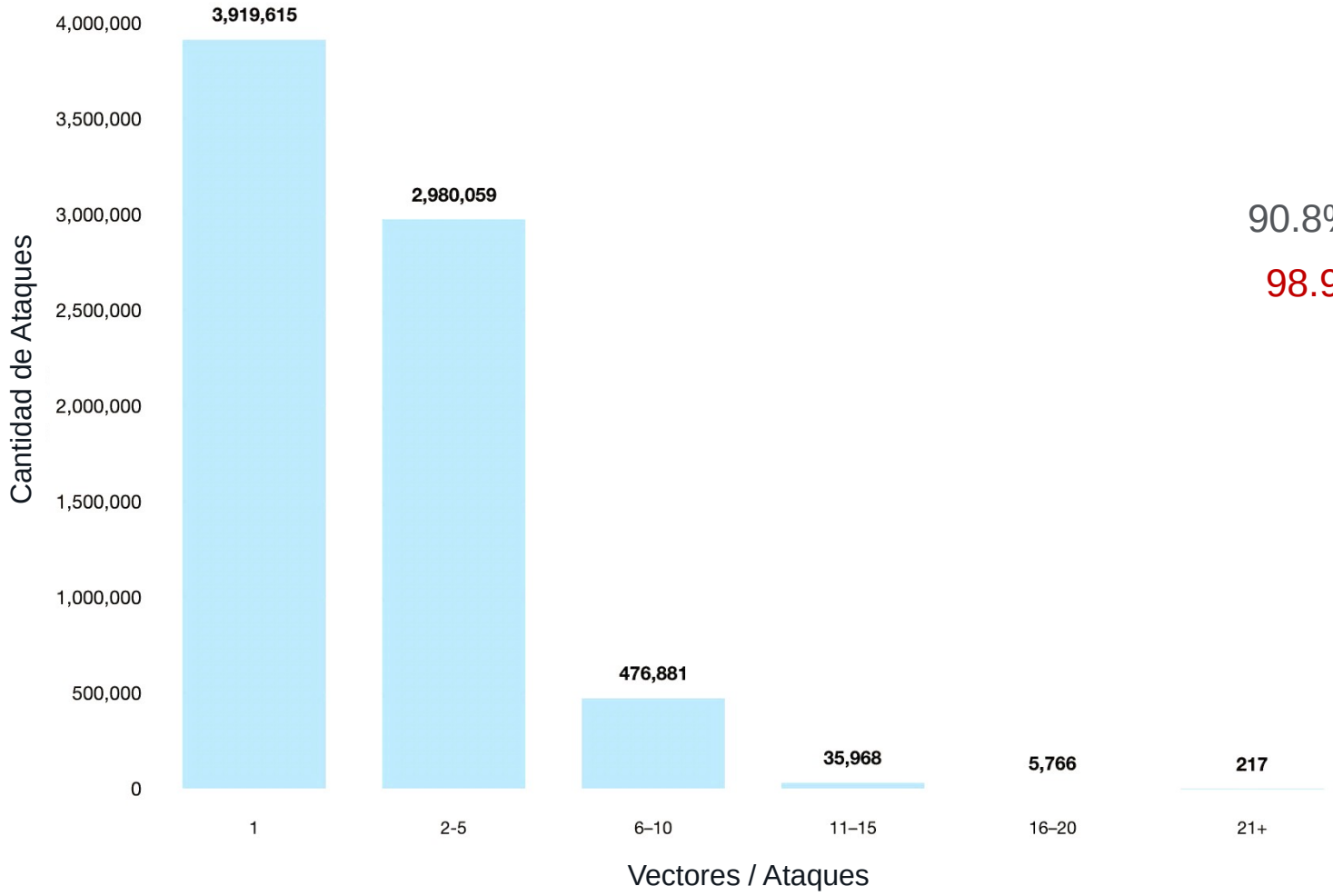
Tendencia de Vectores Ataques DDoS



Tendencia de Vectores Ataques DDoS



Distribución de los ataques por cantidad de vectores



Numero de Vectores	
1 Vector	48.76%
2–5 Vectors	42.06%
6–10 Vectors	8.08%
11–15 Vectors	0.8%
16–20 Vectors	0.28%
21+ Vectors	0.04%

90.8%

98.9%

Objetivos por Mercado

Operdores de Redes Fijas y Móviles

Centro de Datos

Operadores de Redes de Satelite

Educación

Vendedores

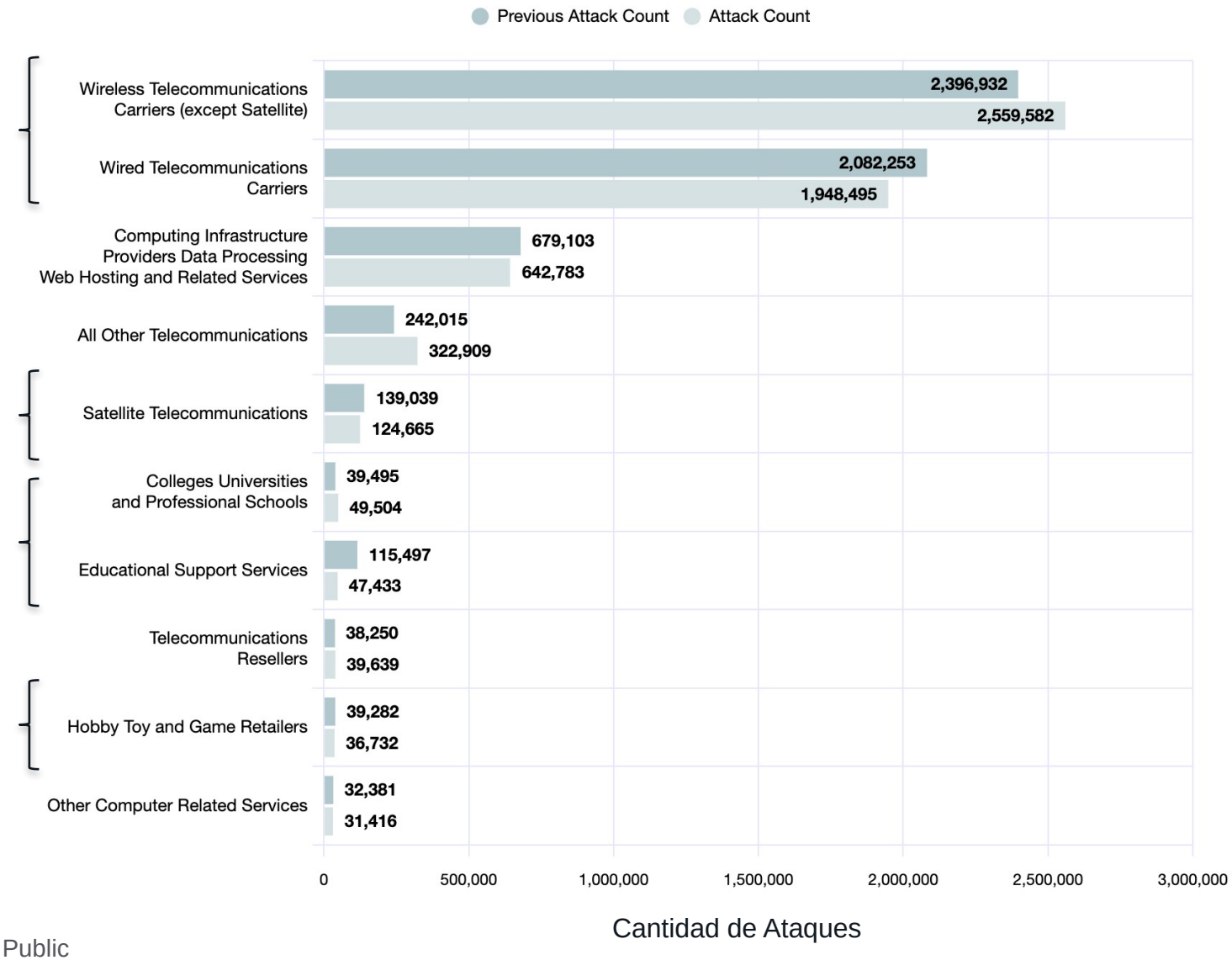
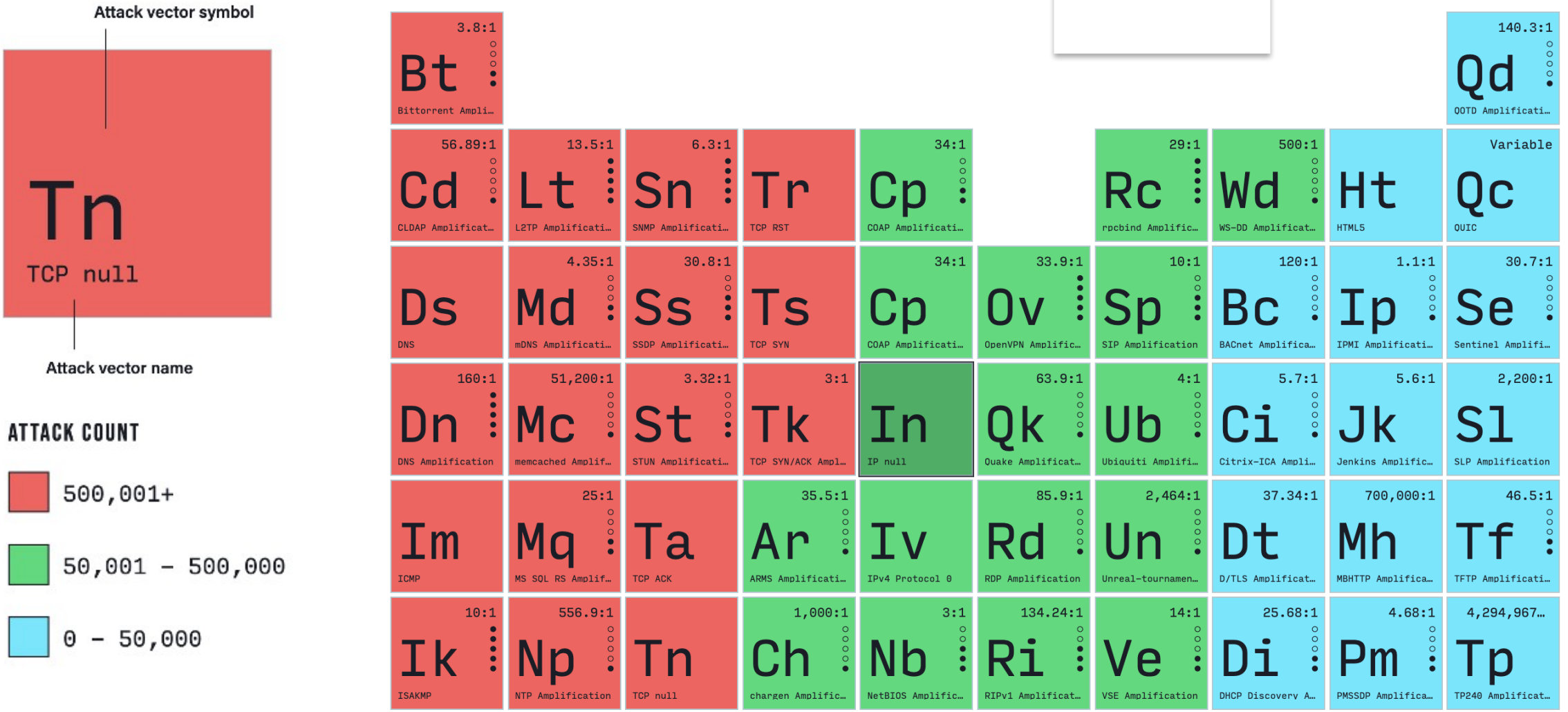
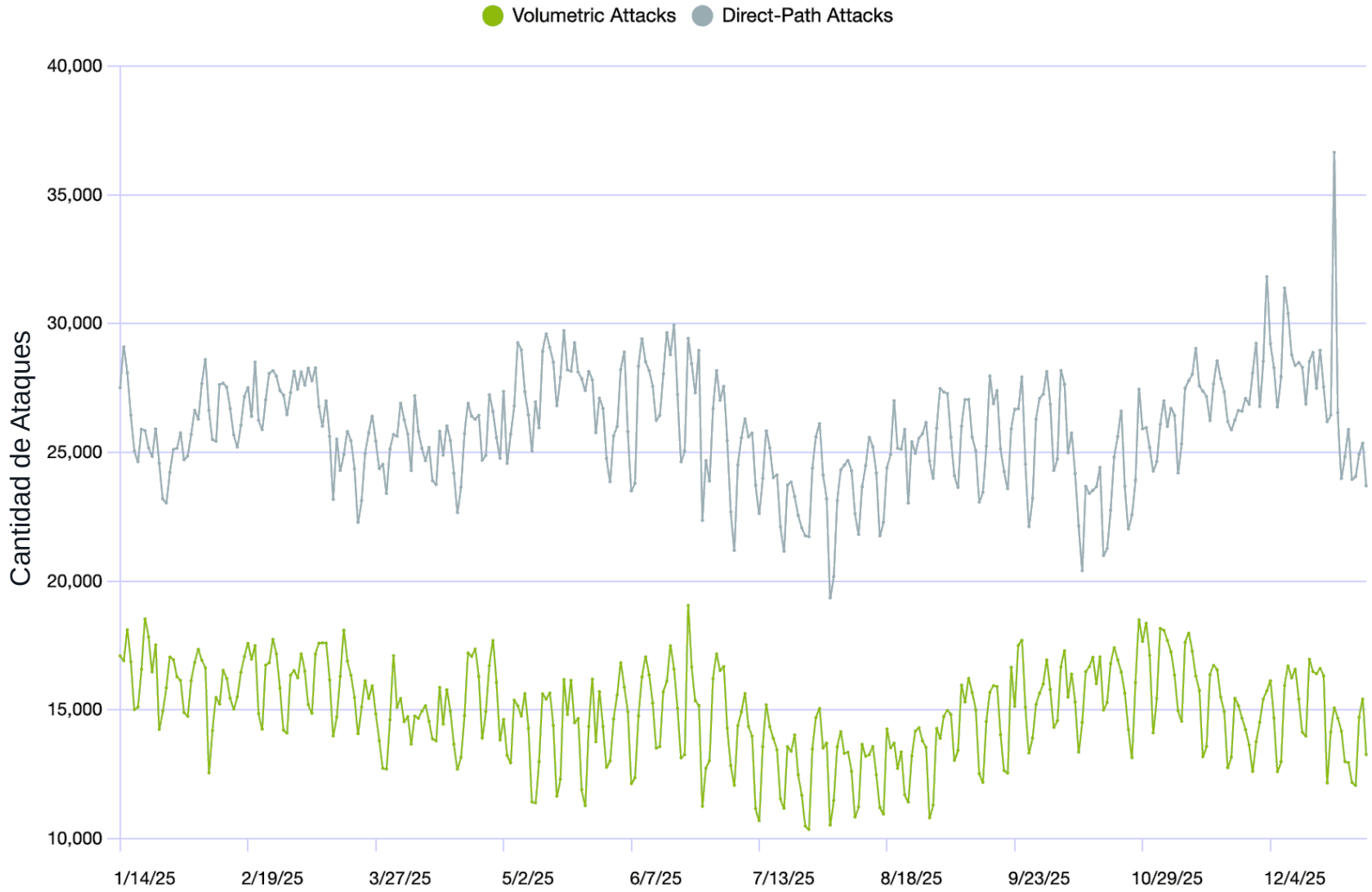


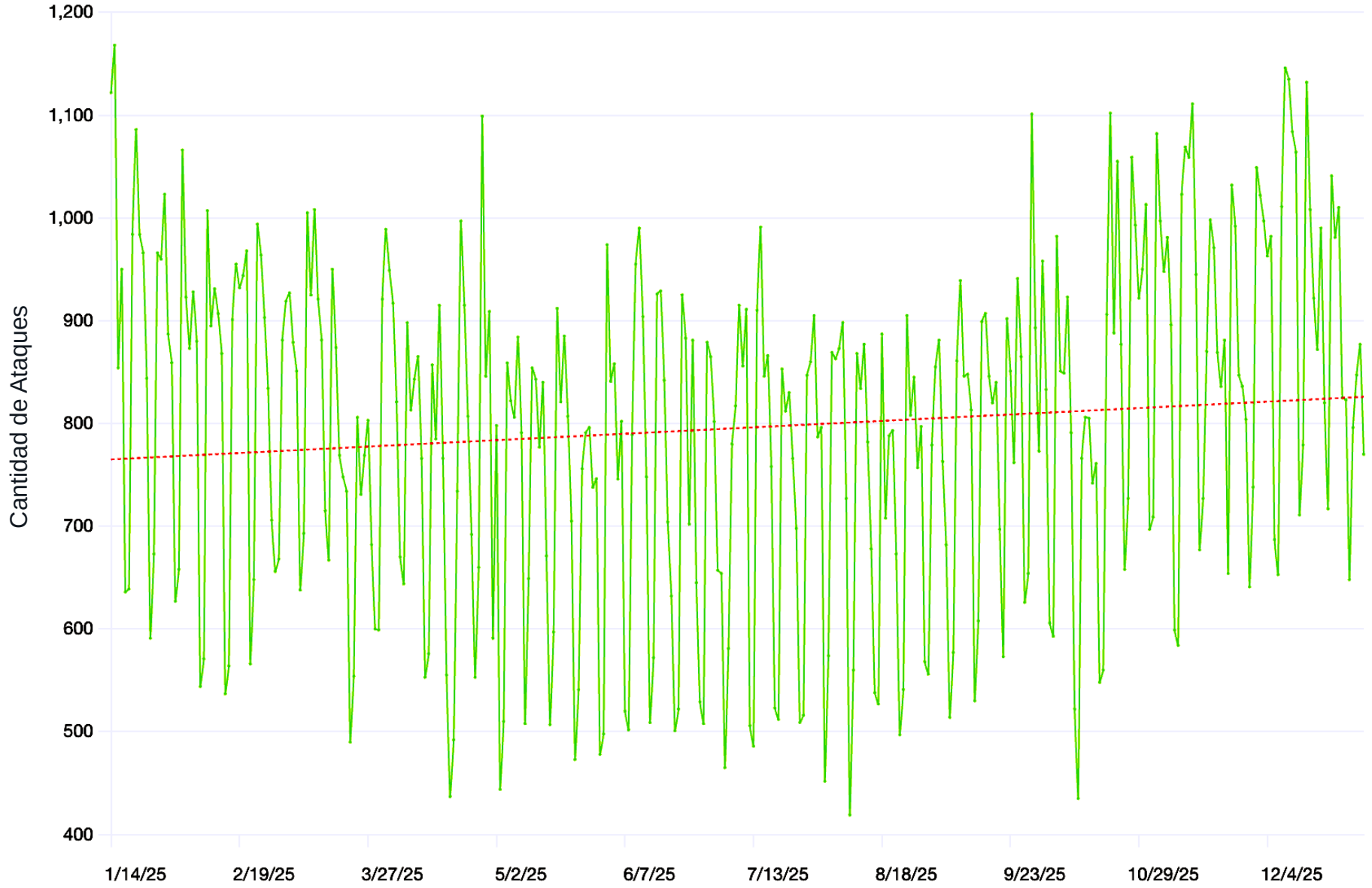
Tabla Periódica de Vectores



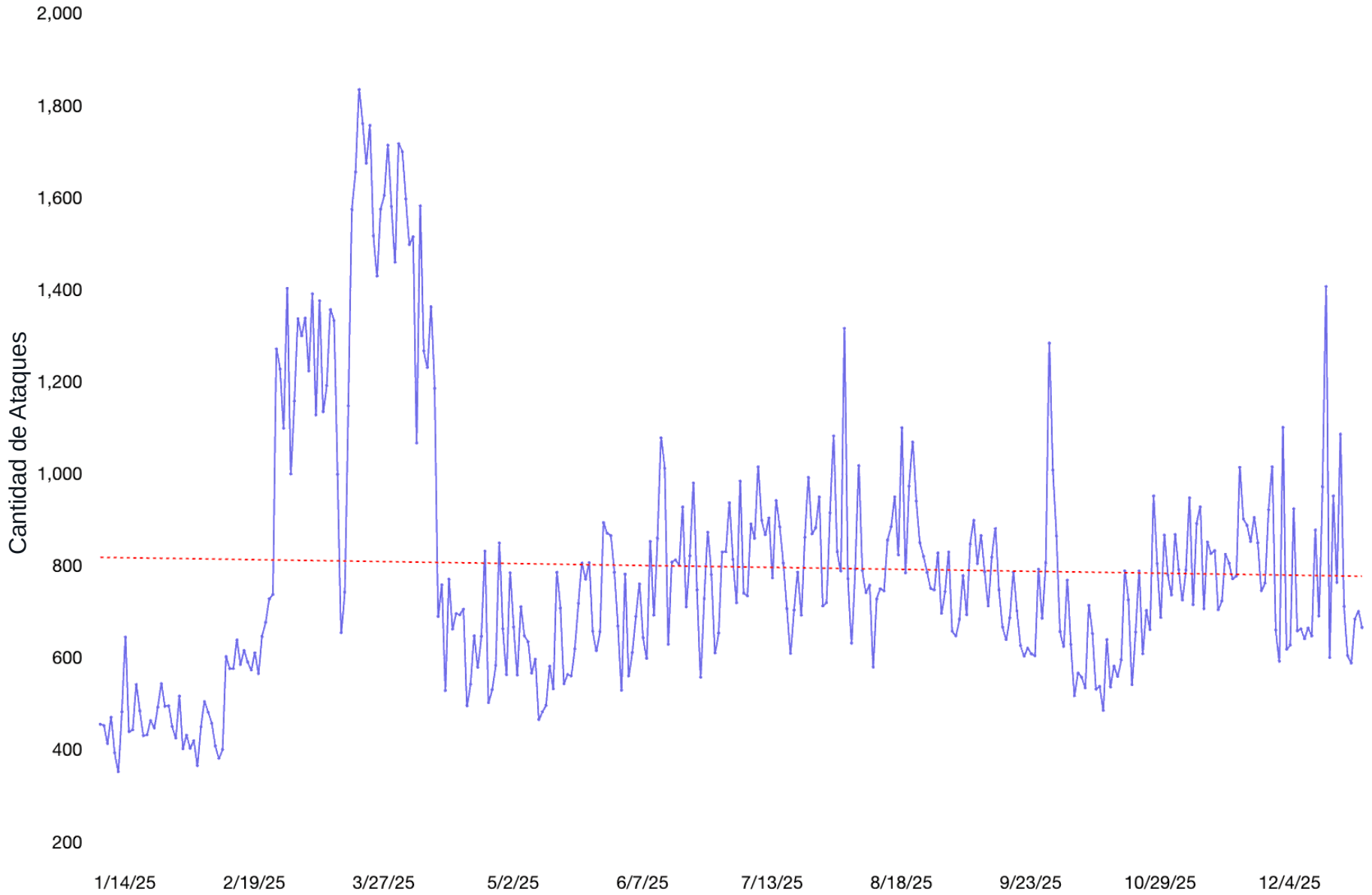
Ataques Reflexión/Amplificacion respecto a Direct-Path



Ataques Carpet Bombing Diarios



Ataques DNS Water Torture



España

Duración Media **56,08 Minutos**

Frecuencia 74263 Ataques

Cinco Industrias más Atacadas

RANK	VERTICAL	FREQUENCY	AVERAGE DURATION
1	Telecommunications Resellers	28,852	10 Minutes
2	Wired Telecommunications Carriers	26,816	34 Minutes
3	Wireless Telecommunications Carriers (except Satellite)	2,970	21 Minutes
4	Computing Infrastructure Providers Data Processing Web Hosting and Related Services	1,728	51 Minutes
5	All Other Professional Scientific and Technical Services	543	758 Minutes

España

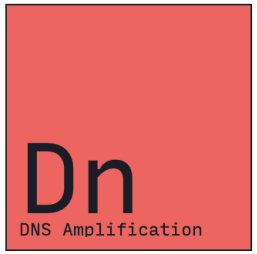
Ataques Multivector

1. ARMS Amplification
2. CLDAP Amplification
3. COAP Amplification
4. DNS Amplification
5. ICMP
6. MS SQL RS Amplification
7. NTP Amplification
8. NetBIOS Amplification
9. RIPv1 Amplification
10. SNMP Amplification
11. SSDP Amplification
12. STUN Amplification
13. TCP ACK
14. TCP SYN/ACK Amplification
15. UDP
16. VSE Amplification
17. WS-DD Amplification
18. chargen Amplification
19. mDNS Amplification
20. memcached Amplification
21. rpcbind Amplification

Vectores más Usados

Cantidad de Ataques

35,470

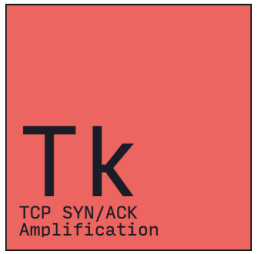


Cantidad de Ataques

20,114

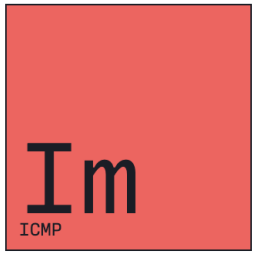
Cantidad de Ataques

19,148



Cantidad de Ataques

14,025



Cantidad de Ataques

9,845

AISURU: Del Agotamiento de los Anlaces al Agotamiento de Infraestructuras

Impacto en la capacidad(bps)

Ataques públicos asociados de hasta 31,4 Tbps

Presión sobre el tránsito y el peering

- Bombardeo en alfombra UDP y aleatorización para evadir filtros
- TCP Rotación de Flags
- Riesgo directo sobre enlaces y servicios expuestos

Perfil operativo

TurboMirai Botnet en CPE/IoT vulnerables

Tráfico desde IPs residenciales legítimas

Menor eficacia de reputación/geobloqueo

- Necesidad de clasificación dinámica basada en telemetría

Impacto en la infraestructura(pps)

Eventos asociados hasta 14.1Gpps

Presión sobre colas, buffers, tarjetas de linea, TCAM,…

Riesgo de degradación en el reenvío y tráfico colateral

- El impacto puede comenzar antes de la desviación total hacia la nube

Mitigación eficaz= Control local inmediato + Escalado coordinado a mitigación cloud

AISURU CRONOLOGÍA DE ATAQUE

Microataques devastadores

Aisuru alcanza su punto máximo casi al instante. Los ataques de registro duran minutos o segundos (por ejemplo, 31,4 Tbps duraron 35 segundos; 29,7 Tbps duraron 69 segundos).

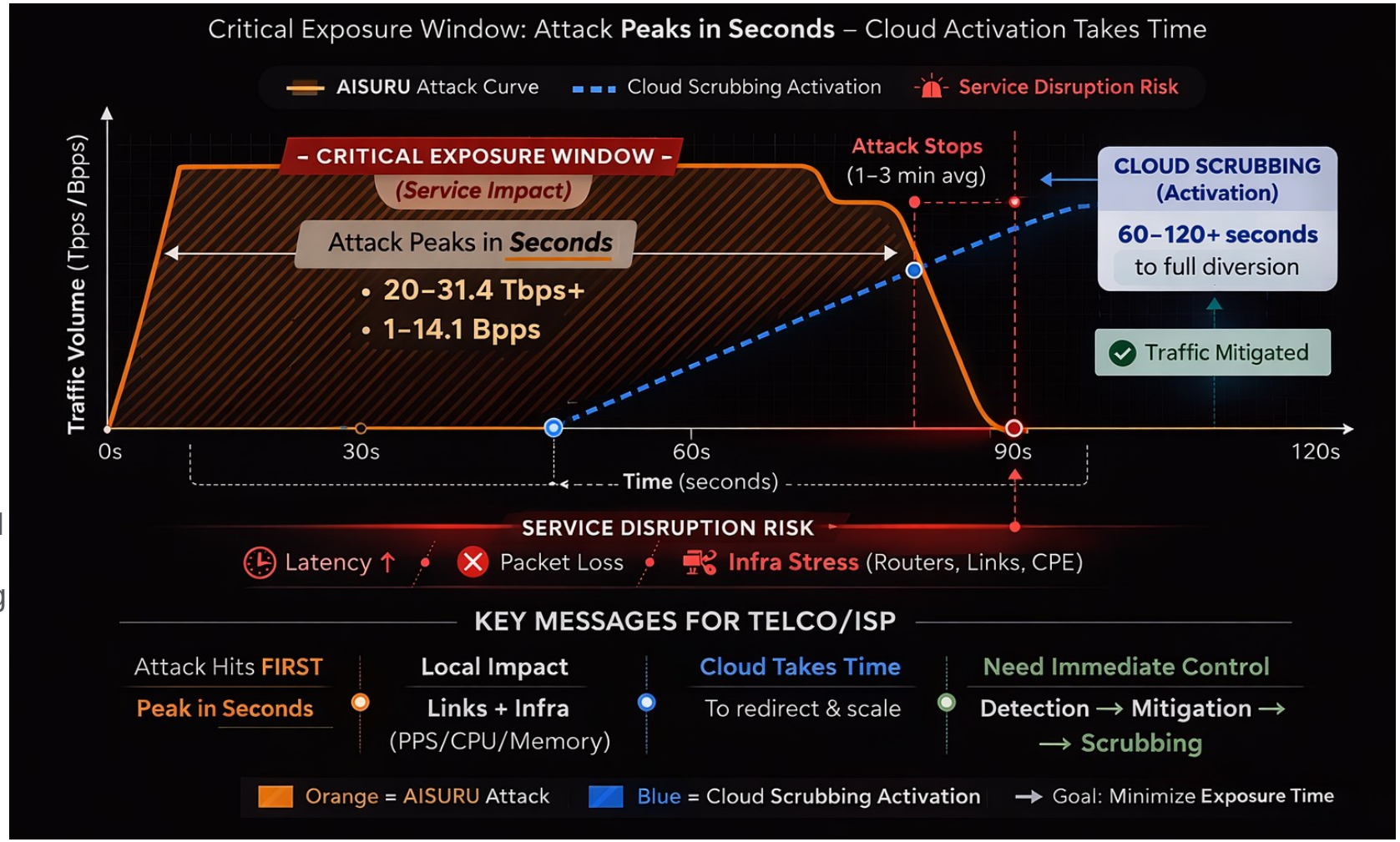
El Retraso Global en el Enrutamiento

Confiar exclusivamente en Cloud Scrubbing requiere descubrimiento, anuncio de ruta y redirección del tráfico. Este proceso físico introduce una latencia inherente.

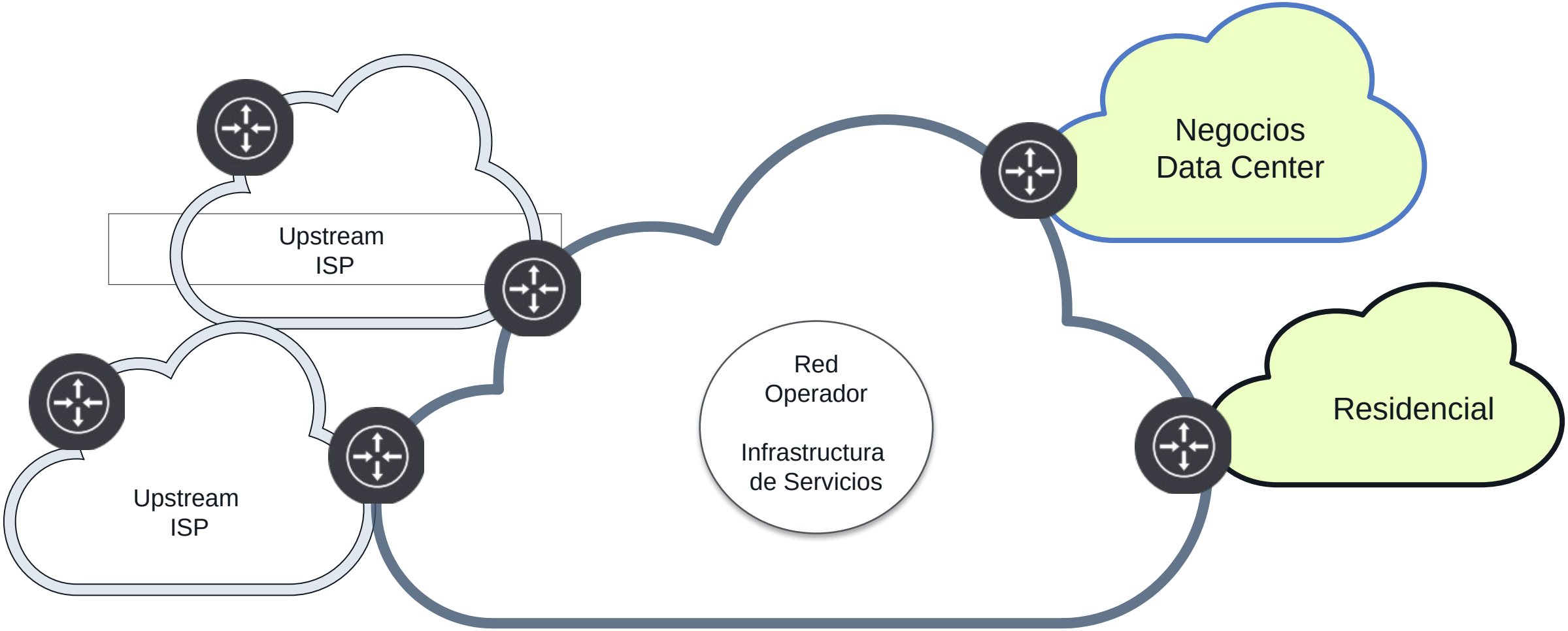
Daños irreversibles

Durante la ventana de latencia (0s - 60s+), el tráfico de 14,1 Gpps ya ha saturado los búferes y ha provocado reinicios de watchdog en routers locales.

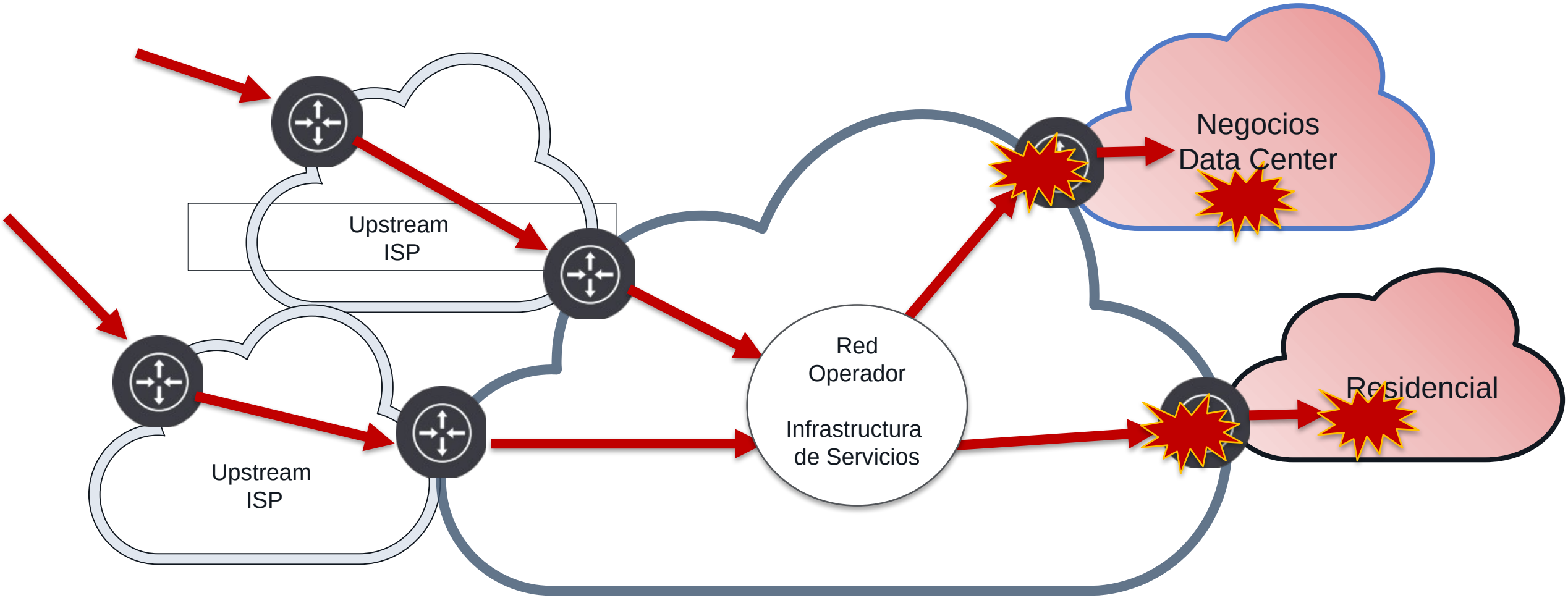
La latencia de mitigación es ahora tan destructiva como el volumen del ataque. La mitigación en las instalaciones ya no es opcional: es el único mecanismo capaz de sobrevivir a Segundo Zero



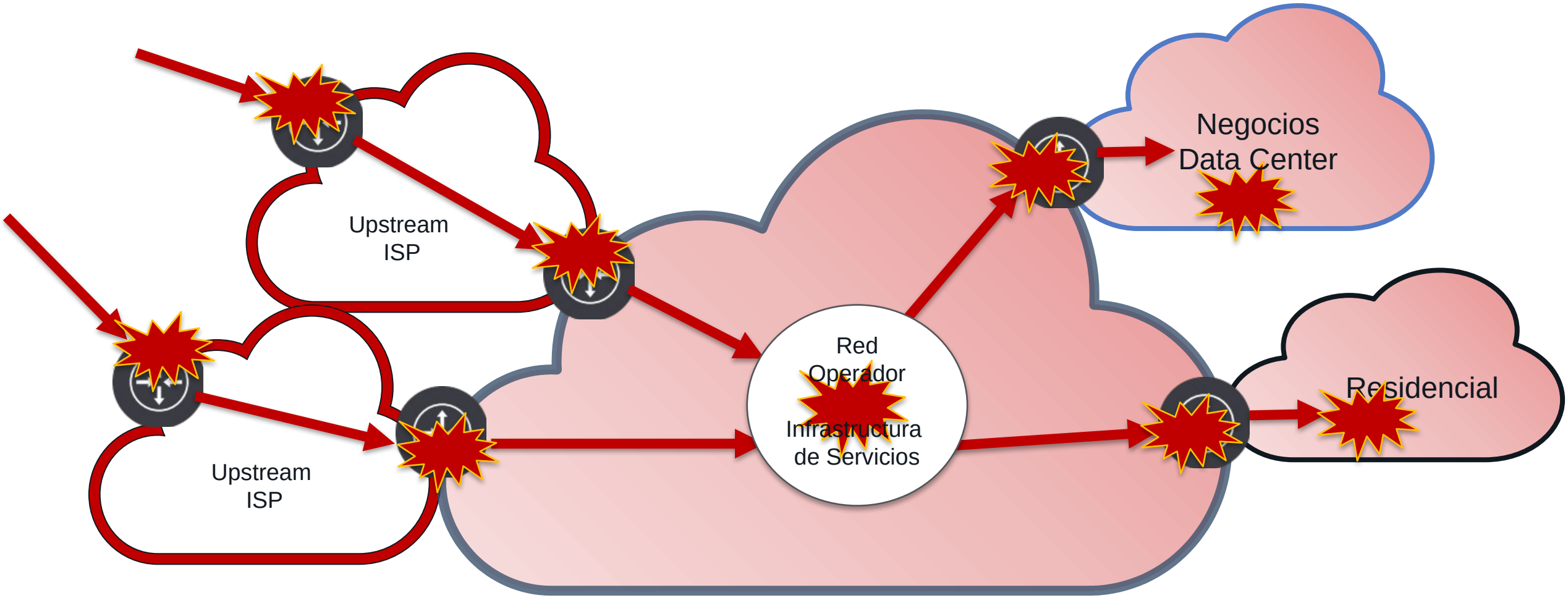
Ataque Tradicional



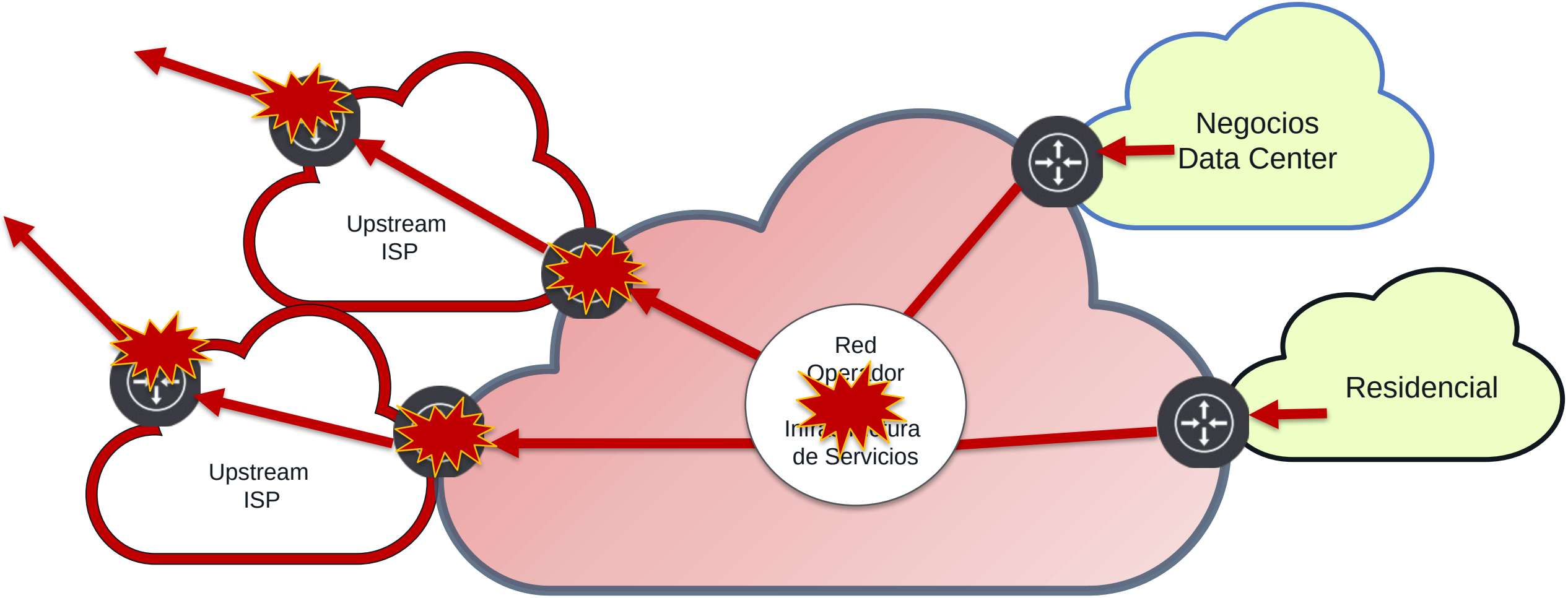
Ataque Tradicional



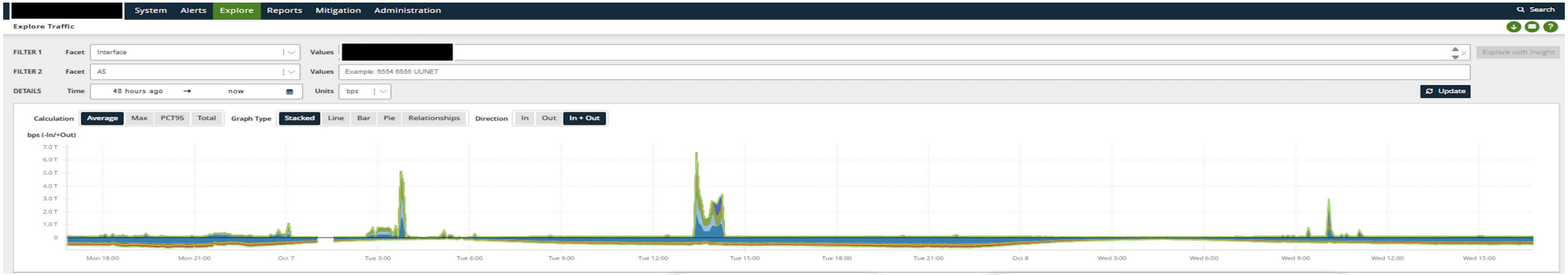
Ataque Hipervolumétrico

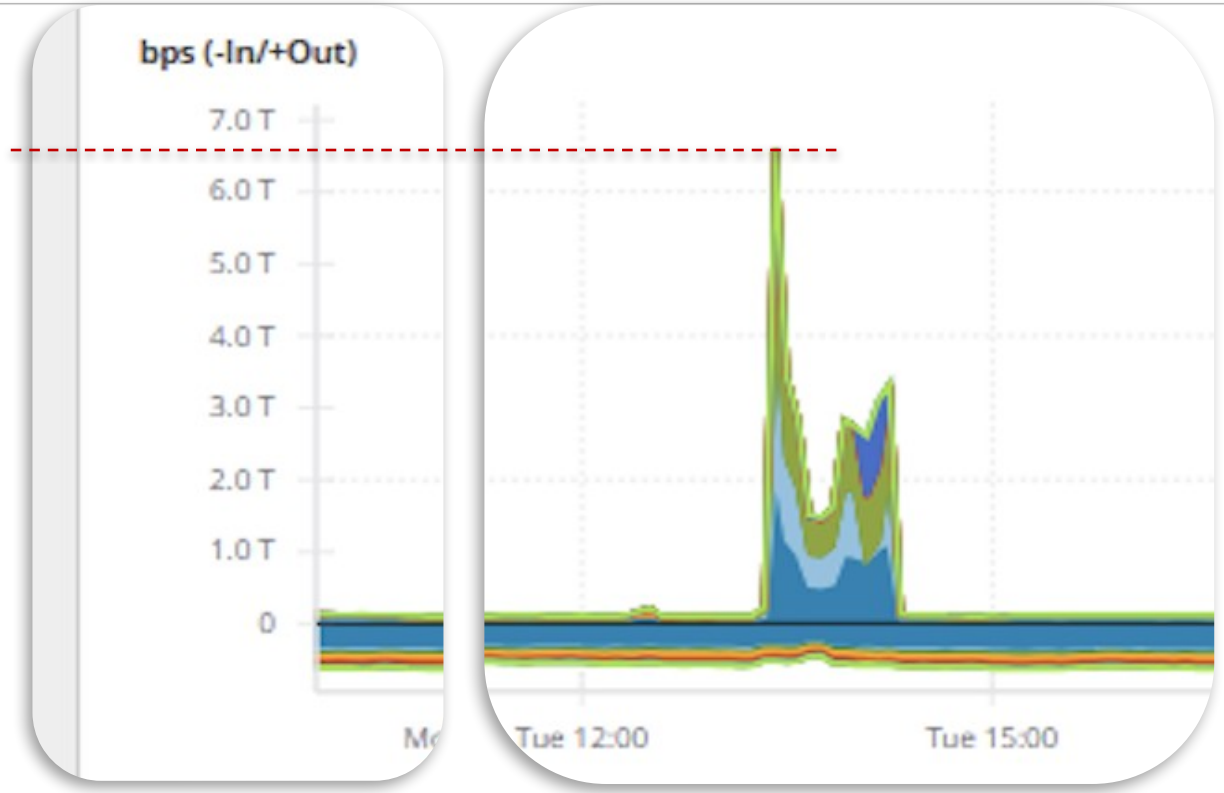


Ataque Hipervolumétrico (Fuente)



Ejemplo Tráfico Salida





1Q2026 BOT

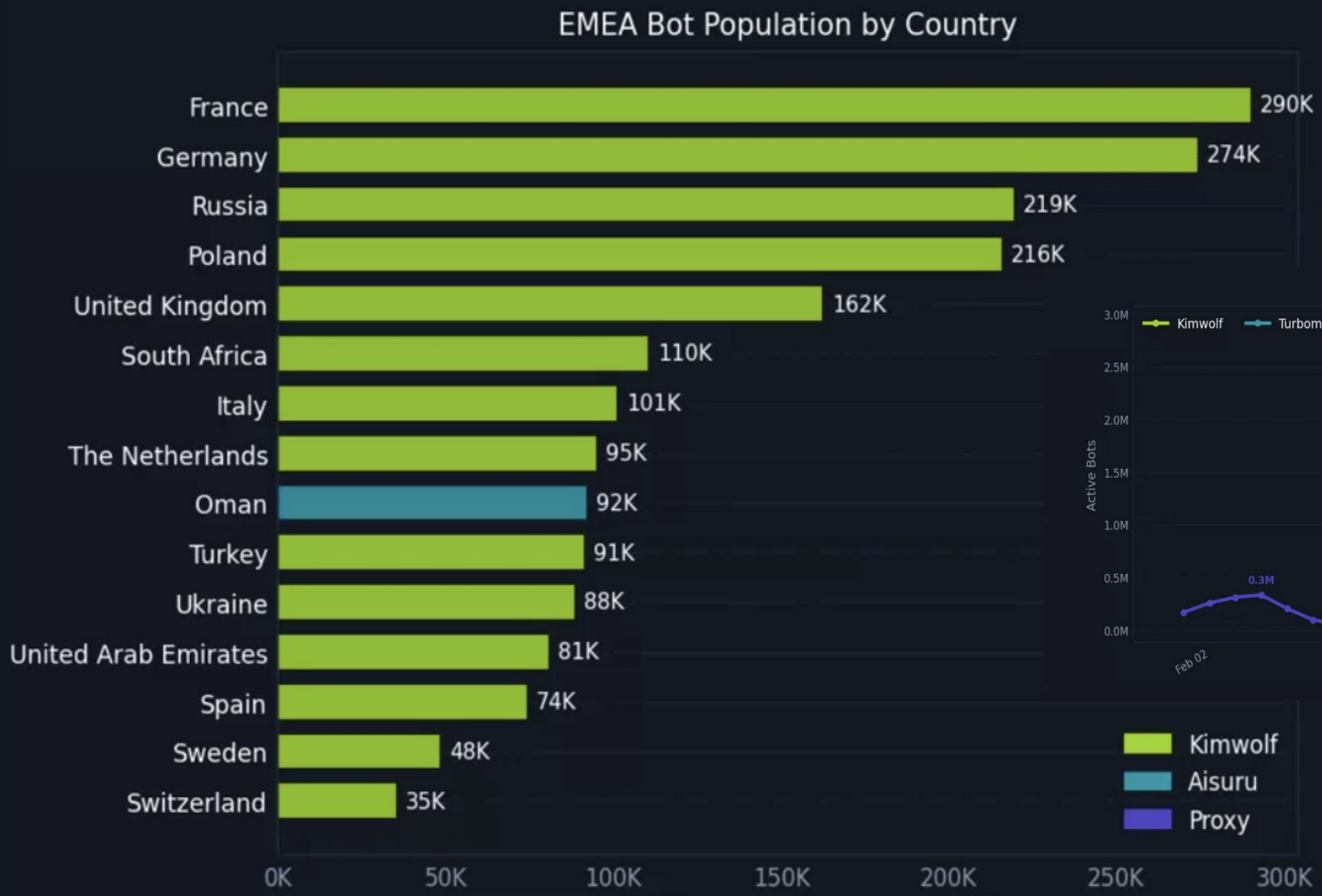
WIRED SECURITY POLITICS THE BIG STORY BUSINESS SCIENCE CULTU

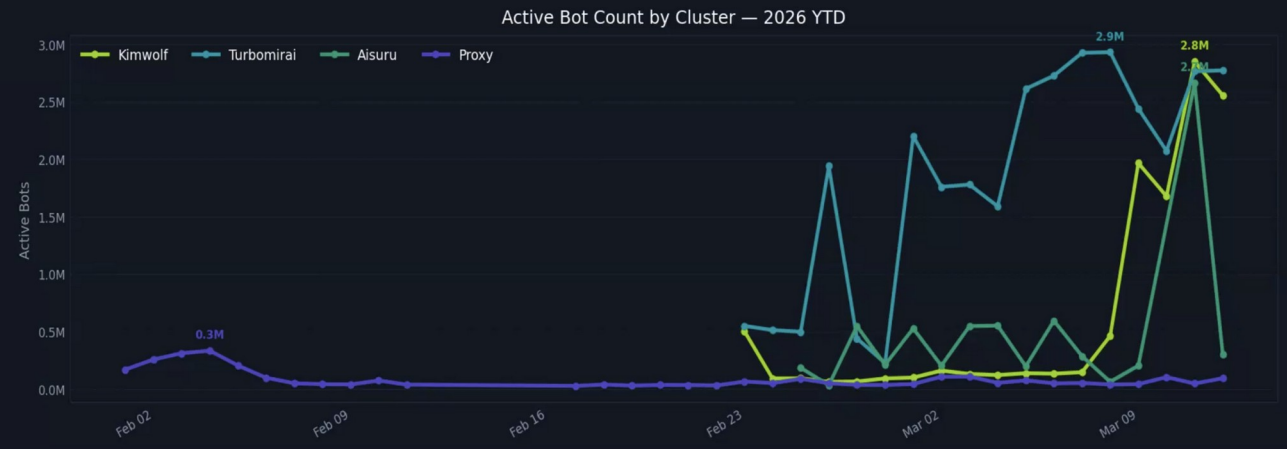
ANDY GREENBERG SECURITY MAR 19, 2026 8:07 PM

US Takes Down Botnets Used in Record-Breaking Cyberattacks

The Aisuru, Kimwolf, JackSkid, and Mossad botnets had infected more than 3 million devices in total, many inside home networks, according to the US Justice Department.

1Q2026 BOT





Los Bots Masivos No Son Nuevos

Insights from the analysis of the Mariposa botnet

Publisher: IEEE Cite This PDF

Prosenjit Sinha ; Amine Boukhtouta ; Victor Heber Belarde ; Mourad Debbabi All Authors

14 Cites in Papers

658 Full Text Views

Abstract

Document Sections

I. Introduction

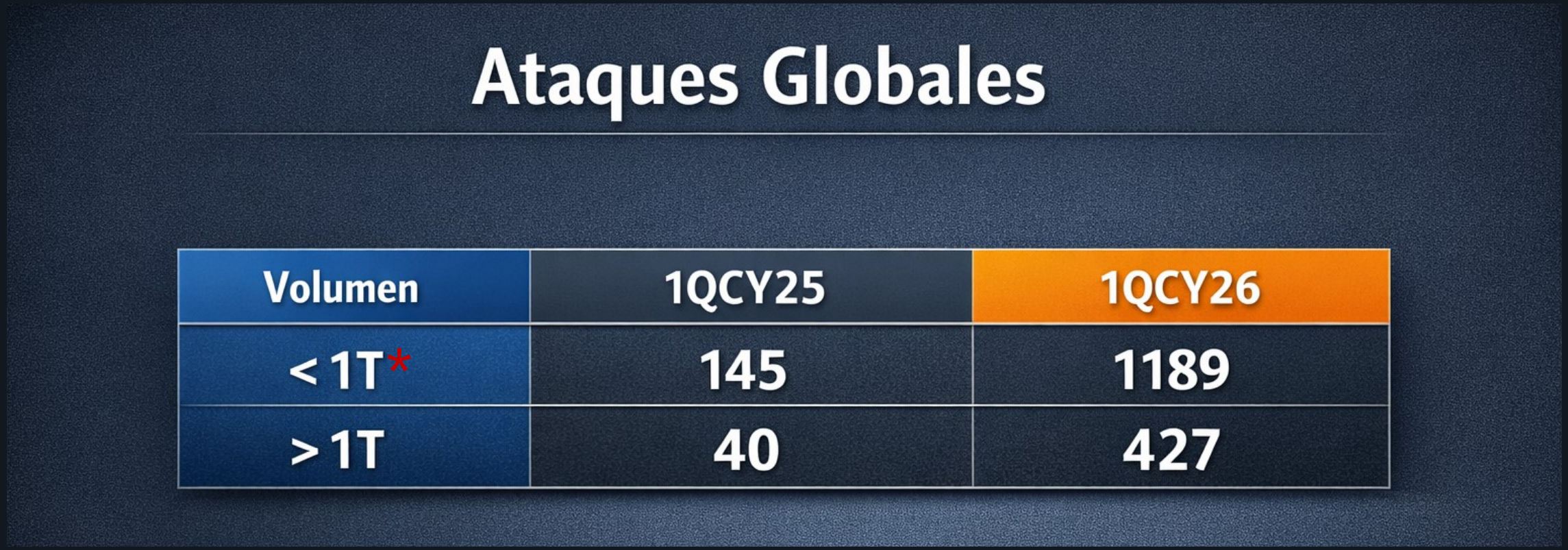
II. Overview of the Mariposa Botnet

III. Behavioral Network Analysis

IV. Static & Dynamic Analysis

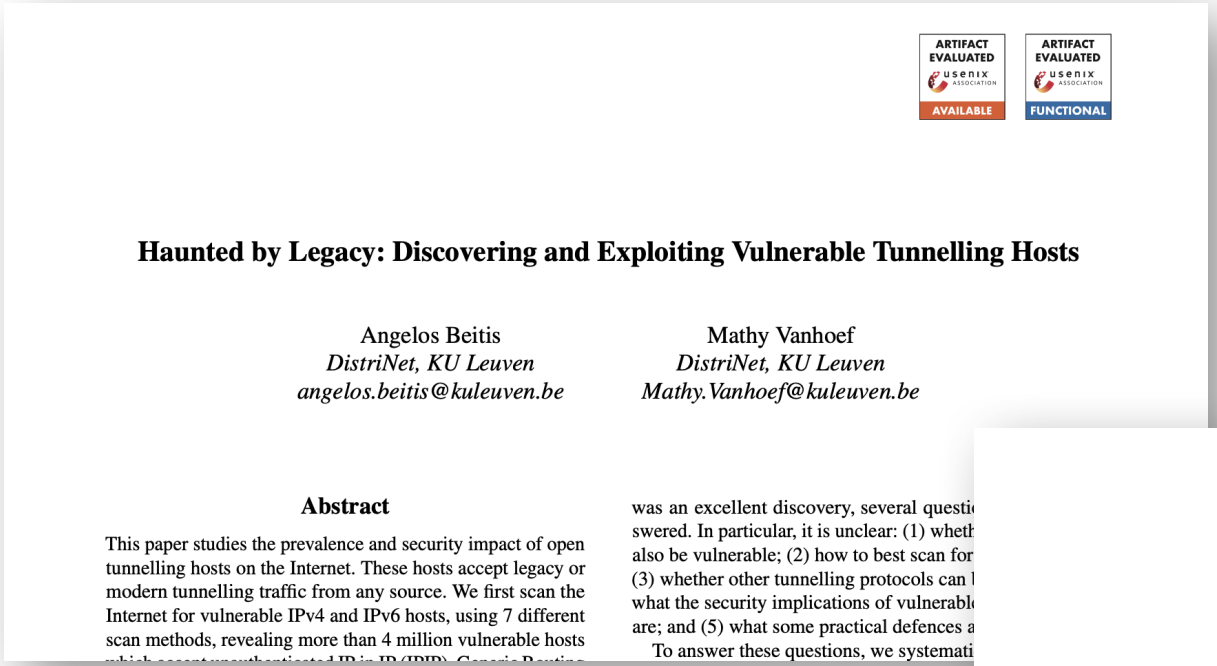
Abstract:
Nowadays, botnets are among the topmost network threats by combining innovative hacking capabilities. This is due to the fact that they are constantly improved by hackers to become more resilient against detection and debugging techniques. In this respect, we analyze one of the most prominent botnets, namely Mariposa which infected more than 13 million computers that are located in more than 190 countries. In this regard, we analyze the botnet architecture, components, commands and communication. In this setting, we detail the obfuscation and anti-debugging techniques it uses. Moreover, we detail the infection and code-injection techniques into legitimate processes. In addition, we explain the spreading mechanisms that are employed in Mariposa as well as the underlying communication protocols. More importantly, we analyze the injected bot code. This is accomplished by a reverse engineering exercise that uses both a network analysis together with reverse-engineering analysis. The insights from this work are meant to illustrate the know-how used in current botnet technologies and enable the elaboration of analysis, detection and prevention techniques.

La Era Terabit Comenzó en 2018 y Popularizada en 2025



* Ataques 500Gbps < x < 1Tbps

Explotando Terminaciones de Túneles



ARTIFACT EVALUATED usenix ASSOCIATION AVAILABLE

ARTIFACT EVALUATED usenix ASSOCIATION FUNCTIONAL

Haunted by Legacy: Discovering and Exploiting Vulnerable Tunnelling Hosts

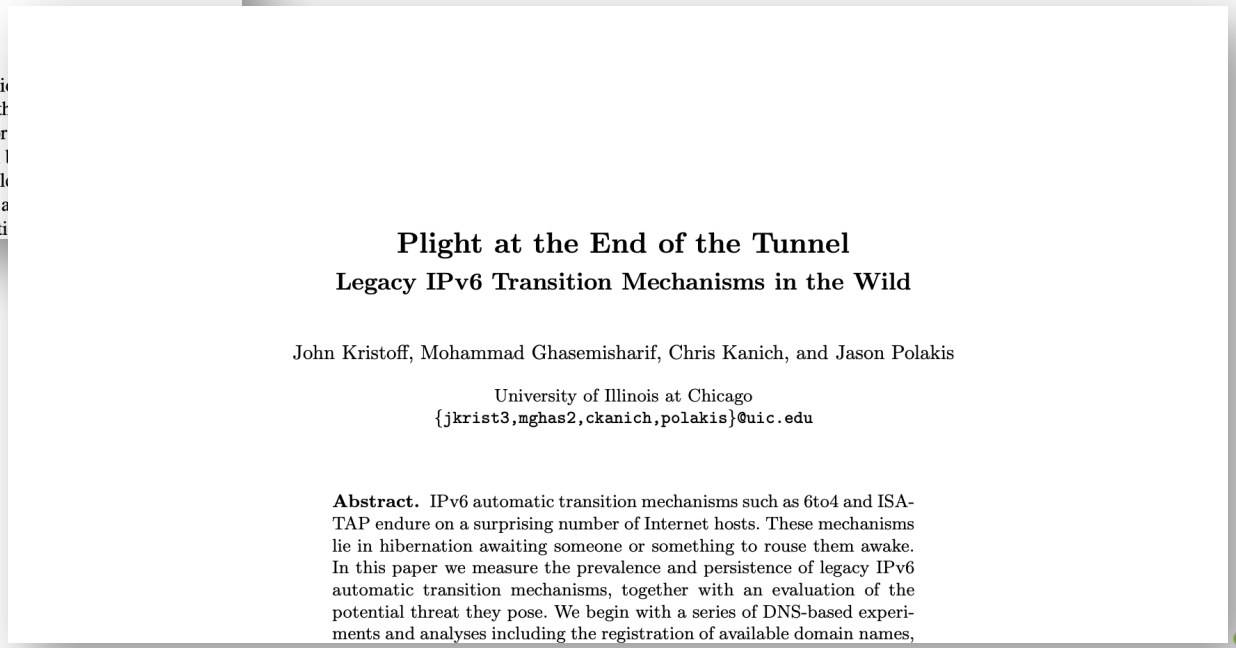
Angelos Beitis
DistriNet, KU Leuven
angelos.beitis@kuleuven.be

Mathy Vanhoef
DistriNet, KU Leuven
Mathy.Vanhoef@kuleuven.be

Abstract

This paper studies the prevalence and security impact of open tunnelling hosts on the Internet. These hosts accept legacy or modern tunnelling traffic from any source. We first scan the Internet for vulnerable IPv4 and IPv6 hosts, using 7 different scan methods, revealing more than 4 million vulnerable hosts

was an excellent discovery, several questi
swered. In particular, it is unclear: (1) wheth
also be vulnerable; (2) how to best scan for
(3) whether other tunnelling protocols can
what the security implications of vulnerabl
are; and (5) what some practical defences a
To answer these questions, we systemati



Plight at the End of the Tunnel

Legacy IPv6 Transition Mechanisms in the Wild

John Kristoff, Mohammad Ghasemisharif, Chris Kanich, and Jason Polakis

University of Illinois at Chicago
{jkrist3,mghas2,ckanich,polakis}@uic.edu

Abstract. IPv6 automatic transition mechanisms such as 6to4 and ISA-TAP endure on a surprising number of Internet hosts. These mechanisms lie in hibernation awaiting someone or something to rouse them awake. In this paper we measure the prevalence and persistence of legacy IPv6 automatic transition mechanisms, together with an evaluation of the potential threat they pose. We begin with a series of DNS-based experiments and analyses including the registration of available domain names,

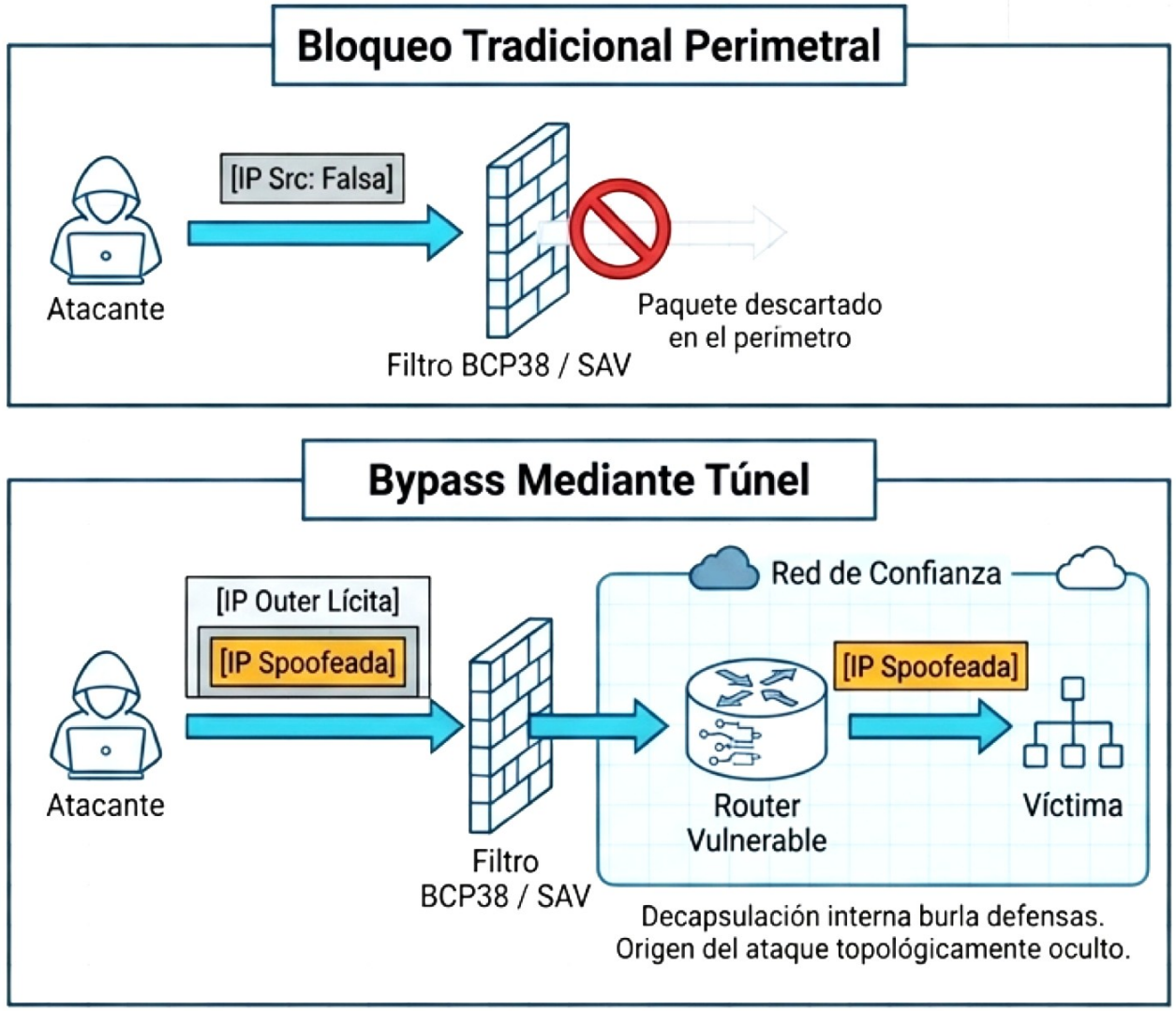
Spoofing IP

Escala Validada: ~1.86M de hosts comprobados con capacidad de forwarding asimétrico.

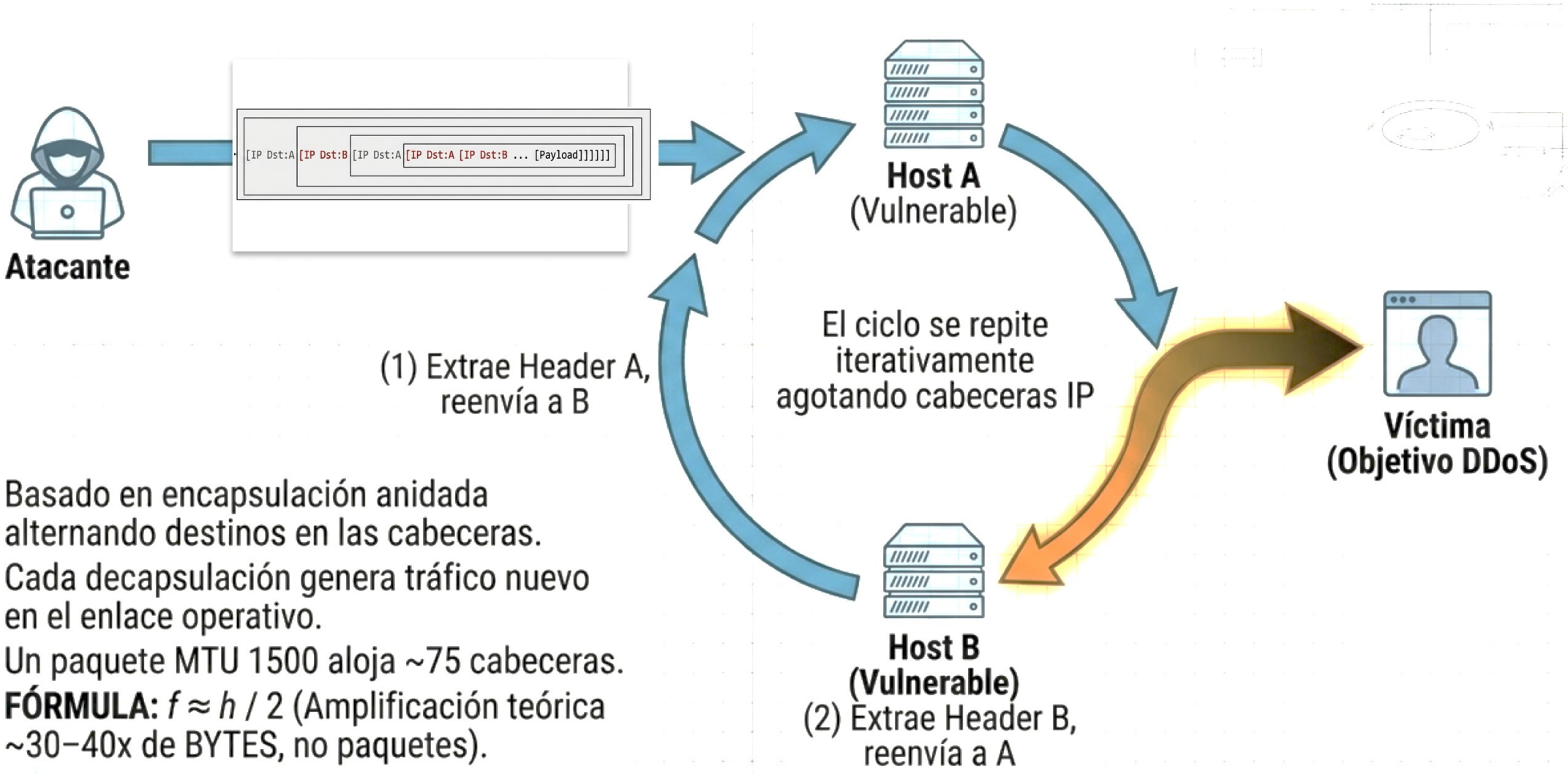
Evasión de Defensas: El tráfico encapsulado sortea exitosamente controles SAV (Source Address Validation) y BCP38 en el perímetro.

Ausencia de Reesritura: A diferencia de los proxies NAT, el nodo vulnerable no modifica las cabeceras; la IP origen 'spoofeada' se mantiene intacta.

Ocultación Estructural: Invalida supuestos de segregación topológica y destruye la viabilidad de los procesos de traceback.

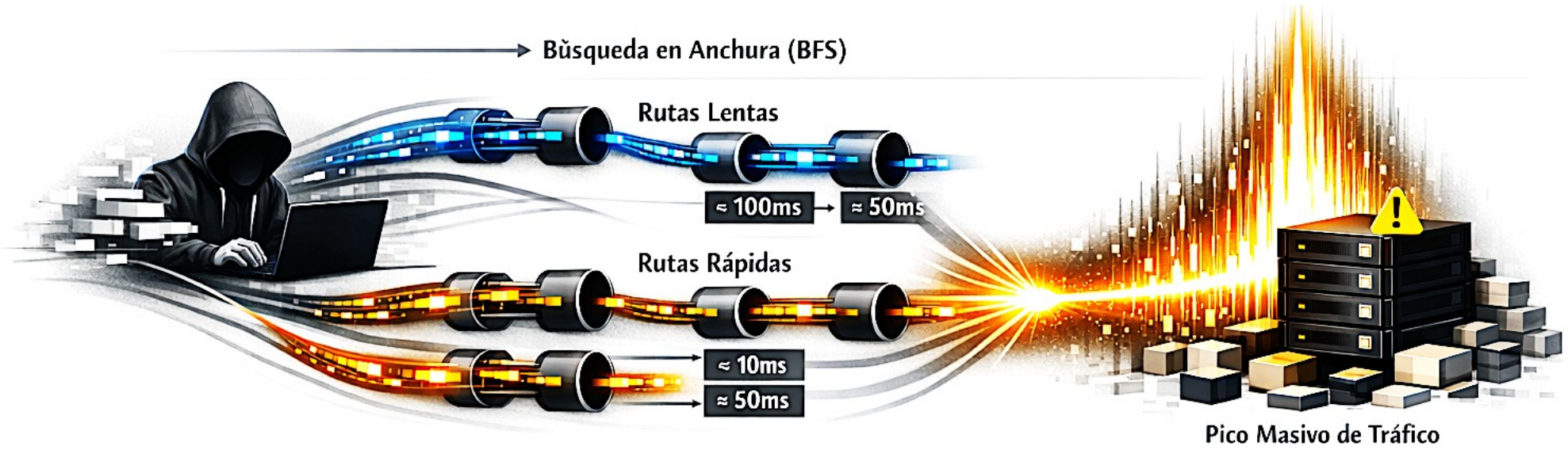


Amplificación Ping-Pong



- Basado en encapsulación anidada alternando destinos en las cabeceras.
- Cada decapsulación genera tráfico nuevo en el enlace operativo.
- Un paquete MTU 1500 aloja ~75 cabeceras.
- **FÓRMULA:** $f \approx h / 2$ (Amplificación teórica ~30–40x de BYTES, no paquetes).

Tunnelled Temporal Lensing (TuTL)

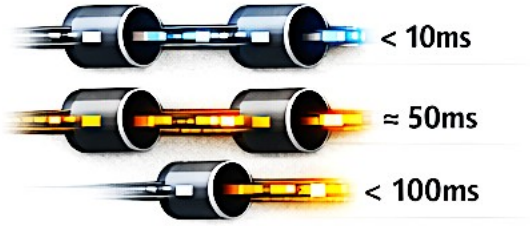


Encapsulación Múltiple

MTU Limitada

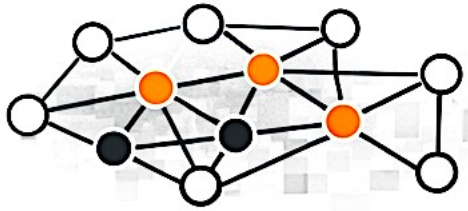
Routing Protocols: GRE, IPIP, 4in6, 6in4
MTU Limitation < 1500 Bytes

Diferentes Latencias



Afecta a GRE, IPIP, 4in6 y 6in4

Algoritmo BFS Optimizado



Gracias

Equipo Iberia:

- Javier Conty
- Miguel Villada

www.netscout.com

Tha

Residential Proxy Relay (Kimwolf)

El atacante ya no es el origen visible.

Usuario legítimo accediendo al servicio

Atacante oculto usando infraestructura residencial comprometida.

- El origen aparente es **legítimo**
- El atacante queda oculto
- Bloquear rompe usuarios reales

La IP ya no es una señal de confianza.

www.ne