CYTED PROGRAMA IBEROAMERICANO DE CIENCIA Y TECNOLOGÍA PARA EL DESARROLLO

UNITECNAR
FUNDACIÓN UNIVERSITARIA ANTONIO DE ARÉVALO

Ciberataques DDoS en 2024 y 2025

Ing. Héctor Espinoza Román, MSc, PhD

Fundación Universitaria Antonio de Arévalo – UNITECNAR

III Encuentro Iberoamericano de Blockchain y Ciberseguridad RIBCi-CYTED Cartagena 2025

Cartagena de Indias – Julio de 2025

BREVE PRESENTACIÓN

- Ingeniero, Escuela Superior Politécnica del Litoral, Guayaquil, Ecuador
- Master of Science, Swansea University, Swansea, Reino Unido
- Doctor, Universitat Politecnica de Catalunya, Barcelona, España
- Profesor Asociado, ESPOL, Ecuador
- Profesor Asistente, Universidad Tecnológica de Bolívar, Colombia
- Profesor Cátedra, Universidad de Cartagena, Colombia
- Diseñador Naval, COTECMAR, Colombia
- Profesor Titular, UNITECNAR, Colombia

Ciberataque

Cualquier tipo de actividad maliciosa que intente recopilar, interrumpir, denegar, degradar o destruir los recursos del sistema de información o la información en sí.

Any kind of malicious activity that attempts to collect, disrupt, deny, degrade, or destroy information system resources or the information itself.

Computer Security Resource Center (CSRC)

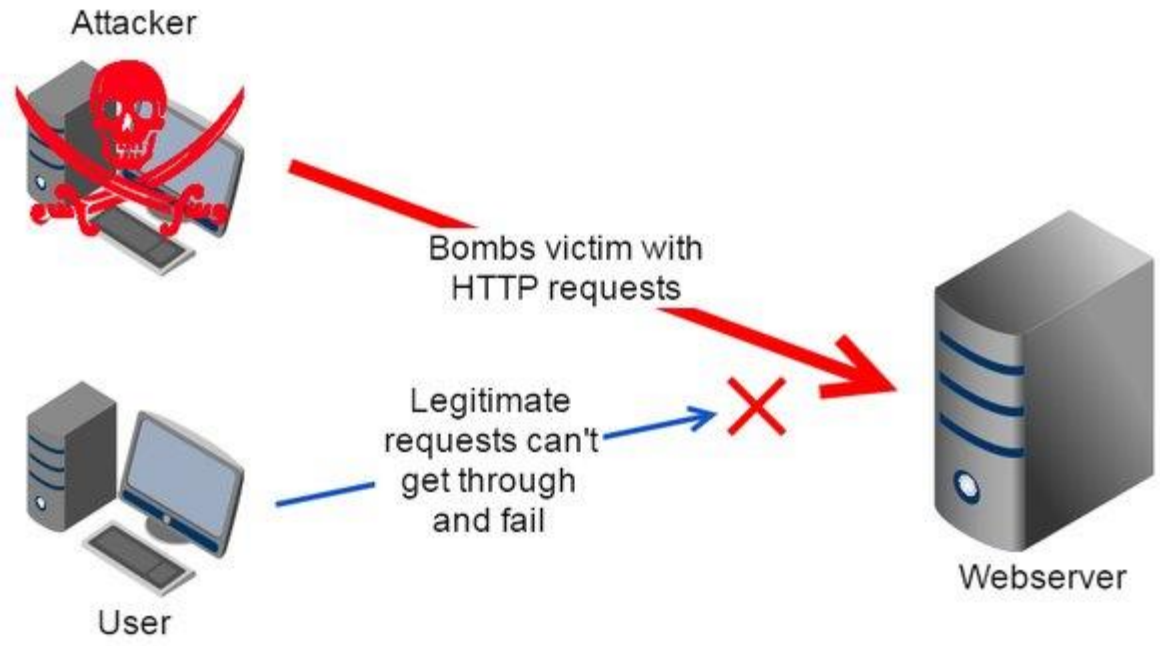
National Institute of Standards and Technology (NIST)

DoS

Denial of Service

Es un tipo de ciberataque que consiste en la prevención del acceso autorizado a los recursos o el retraso de operaciones críticas en el tiempo.

CSRC, NIST

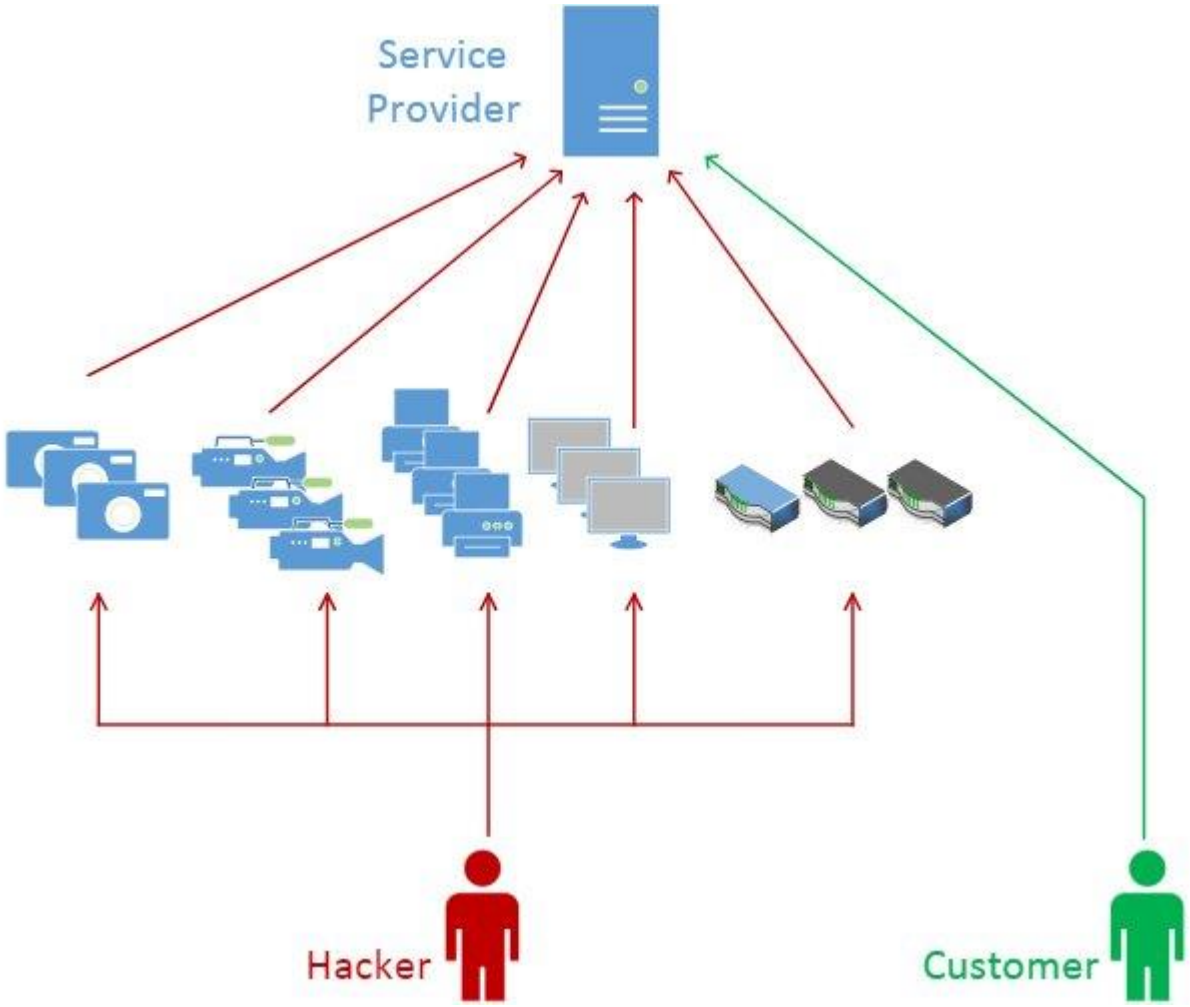


DDoS

Distributed Denial of Service

Es un tipo de DoS que usa varias computadoras para realizar el ataque.

CSRC, NIST



RDoS/RDDos

Ransom Denial of Service

Ransom Distributed Denial of Service

Es un tipo de DoS/DDoS que involucra extorsión.

- Ataque primero
- Extorsión primero

ENISA 2024

Héctor Espinoza Román

*DoS en las Noticias 2025 (NTT Data)

Radware's Cyber Threat Report: Web DDoS attacks surge 550% in 2024

Geopolitics, a growing threat surface, and AI tech drive bigger, longer, and more intense attacks.

Feb. 26, 2025

CrowdStrike: Cyber threats skyrocket as attackers think like businesses

Nadine Hawkins February 27, 2025 08:01 AM

European Cyber Report 2025: 137% more DDoS attacks than last year - what companies need to know

NEWS PROVIDED BY
Link11 GmbH →
05 Mar, 2025, 12:33 GMT

SHARE THIS ARTICLE

Eleven11bot Captures 86,000 IoT Devices for DDoS Attacks

by Jeffrey Burt on March 5, 2025

DDoS y Capas del modelo OSI

Muy común en:

L3 (Network Layer): IP, ICMP

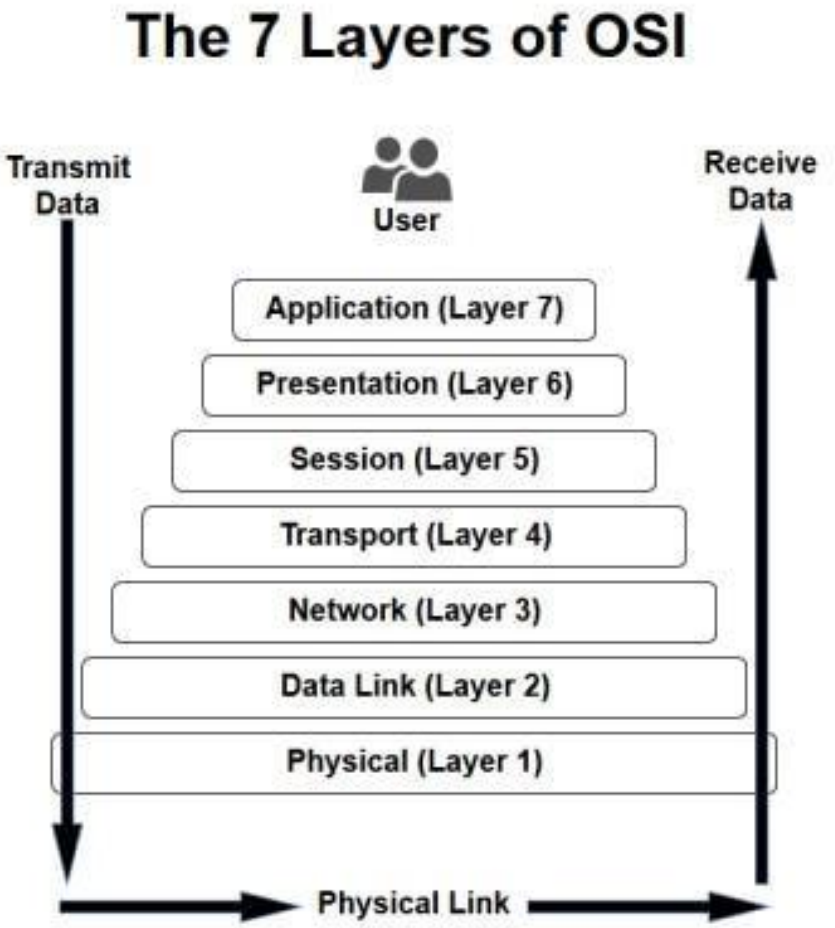
L4 (Transport Layer): TCP, UDP

L7 (Application Layer): HTTP, NTP, DNS

Menos comunes en:

L5 (Session Layer)

L6 (Presentation Layer)



Tipos de DDoS

Flooding

- Volumétricos: saturan el ancho de banda (UDP flood, ICMP flood)
- Protocolo: debilidades en el protocolo (SYN flood, ACK flood)
- Aplicación: (HTTP flood, Slowloris)

Crashing

- Software: bugs (buffer over-flow, zero-day)
- Protocolo: (ping de la muerte, Teardrop)

Recursos Internos

- Estado: Slowloris, SlowHTTPTest
- Computacionales: RUDY, HashDoS

Héctor Espinoza Román

Empresas golpeadas por DDoS

Trasporte

Bancos

Telecomunicaciones

Ventas online

Salud

Servicios gubernamentales

Juegos Online

DDoS en Japón

Recomendaciones del 4 de Febrero de 2025

National Center of Incident Readiness and Strategy for Cybersecurity

Empresas: tomar medidas contra DDoS

Usuarios: configurar sus dispositivos IoT (routers, cámaras IP) para evitar que se infecten de malware ... botnet.

Las medidas son costosas y consumen tiempo.

- Mitigación del daño
- Preparación y Respuesta
- Prevención de participación

DDoS en Japón

Mitigación del daño

- Bloquear IPs no esperadas (internacionales)
- Desplegar equipos y servicios : WAF, IDS/IPS, UTM
- Utilizar CDN y esconder la IP del servidor de origen
- Usar otras medidas anti-DDoS de los proveedores de internet
- Implementar servidores redundantes

DDoS en Japón

Preparación y Respuesta

- Separar los sistemas en función de su importancia
- Monitorear el tráfico durante momentos de paz
- Configurar alertas cuando se detecten anormalidades

Prevención de participación

- Tomar medidas con resolvedores abiertos (Servidores DNS – recursive queries)
- Aplicar parches de seguridad
- Chequear la configuración de los filtros (IP Spoofing)

ENISA THREAD LANDSCAPE 2024

European Union Agency for Cybersecurity

<u>Prime threats:</u>

- Ransomware
- Malware
- Social Engineering
- Threats against data
- **Threats against availability: DDoS**
- Information manipulation

ENISA THREAD LANDSCAPE 2024

Actores:

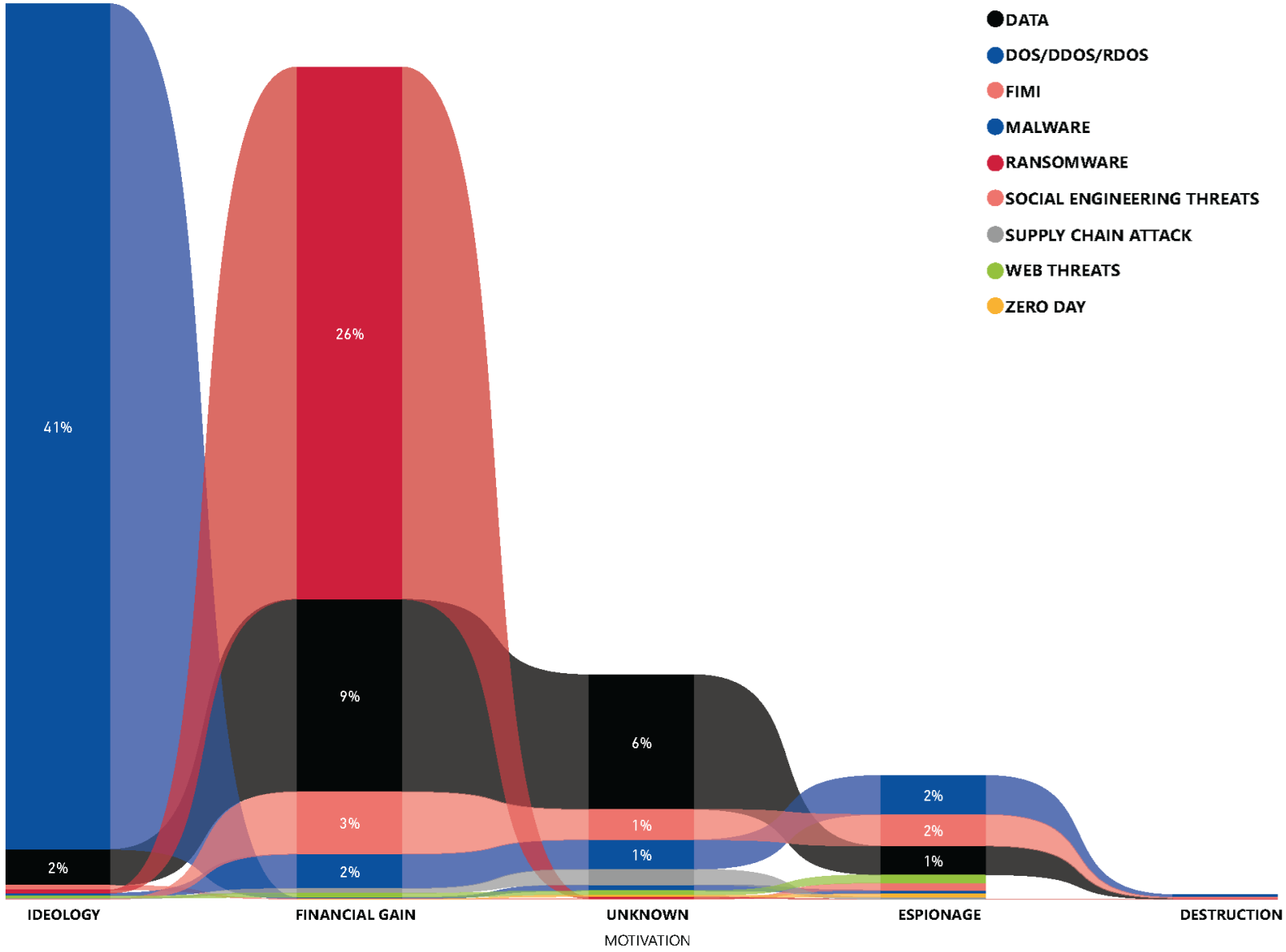
- State-nexus actors
- Cybercrime actors and hacker-for-hire actors
- Private Sector Offensive actors (PSOA)
- Hacktivists

Héctor Espinoza Román

ENISA THREAD LANDSCAPE 2024

Motivaciones:

- Financiera
- Espionaje
- Destrucción
- Ideológicas
- Desconocida



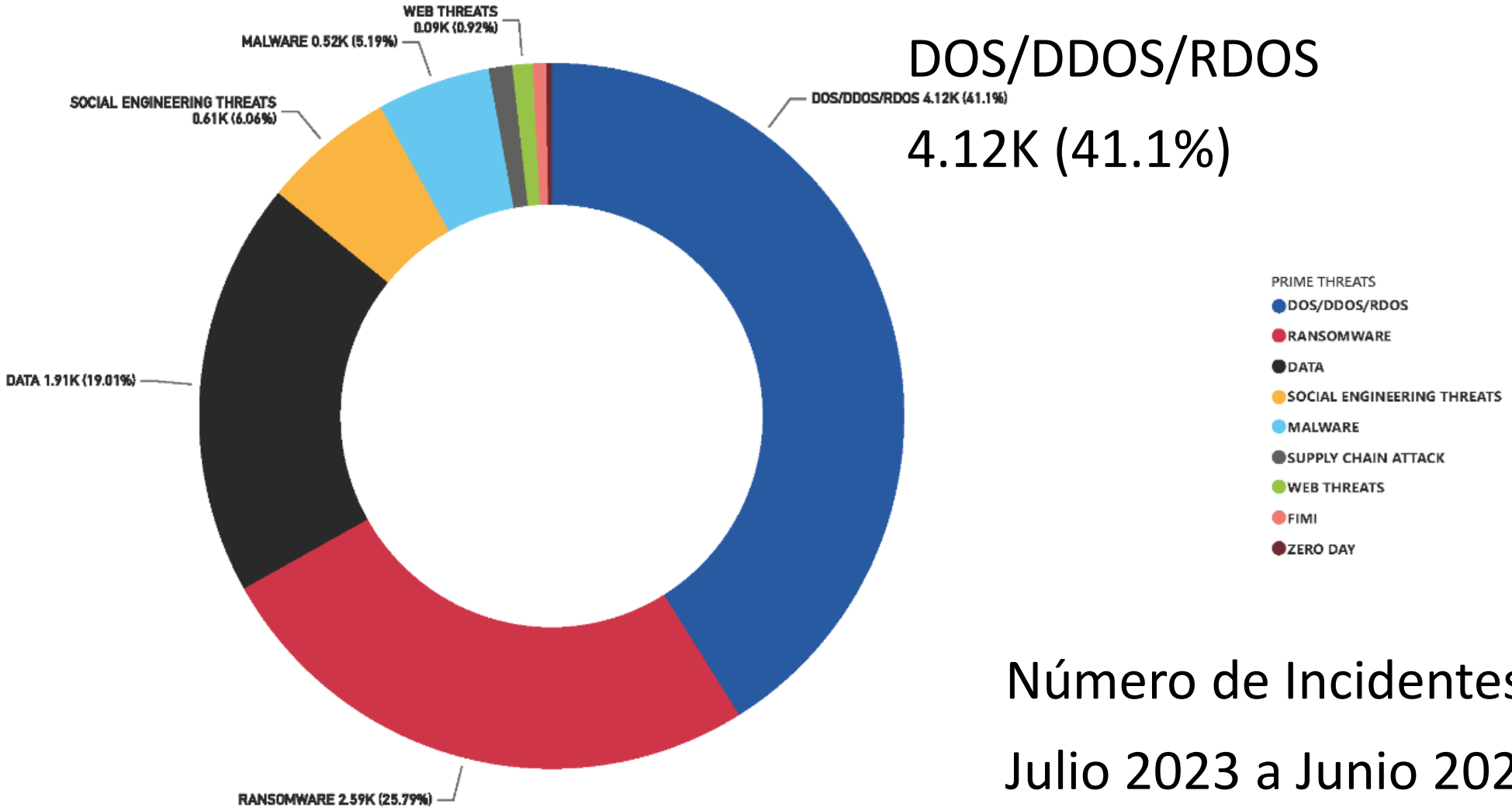
ENISA THREAD LANDSCAPE 2024

DDoS:

- Disponibilidad del Sistema y Datos
- No es amenaza nueva (lleva más de 25 años)
- Relevante a día de hoy
- Impacto limitado y simbólico
- Predominancia de ataques a L3 y L4

Héctor Espinoza Román

ENISA THREAD LANDSCAPE 2024



DOS/DDOS/RDOS

4.12K (41.1%)

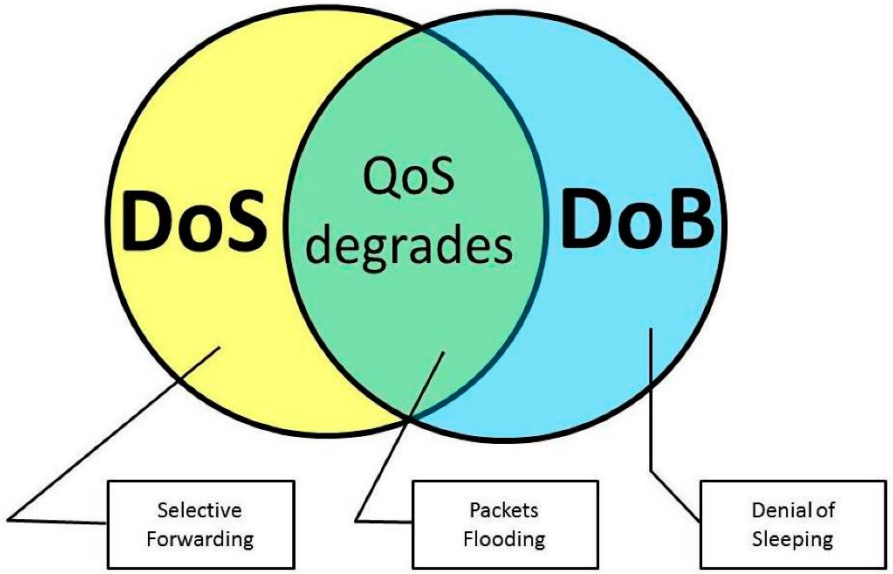
Número de Incidentes

Julio 2023 a Junio 2024

ENISA THREAD LANDSCAPE 2024

Tendencias y Novedades:

- DDoS-as-a-Service
- DDoS-for-Hire
- Triple: encriptación, filtrado y DDoS
- Uso de DDoS como cortina de humo para otros ataques
- Ataques a dispositivos pueden agotar su batería DoB
- Ataques multi-vectoriales



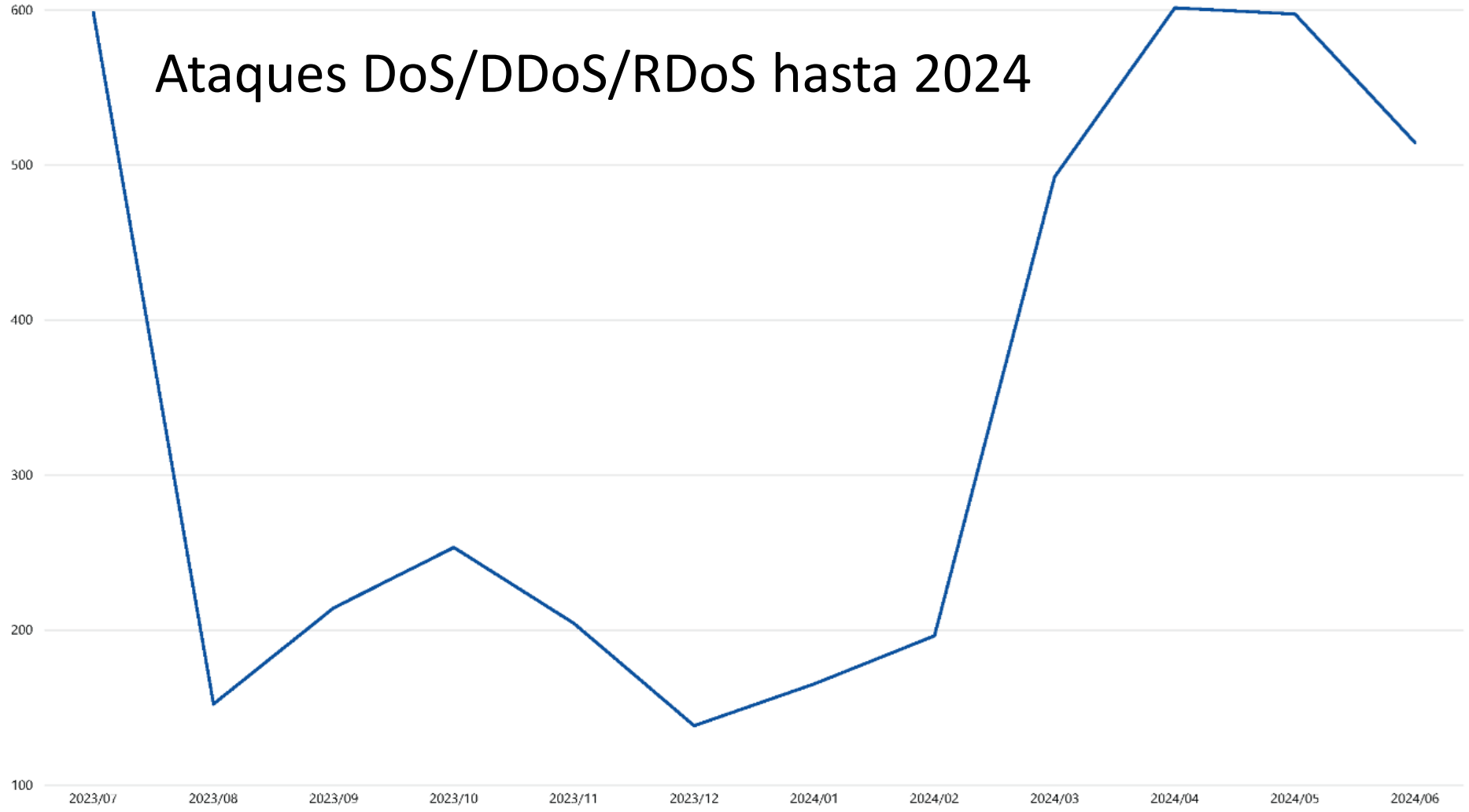
ENISA THREAD LANDSCAPE 2024

<u>Tendencias y Novedades:</u>

- Ataques hiper-volumétricos
- Ataques de hasta 2.6 Tbps (2023)
- *Ataque de 6.5 Tbps (2025, Cloudflare)*
- Ataques promedio de 500 Mbps
- Ataques de 3 minutos a 9 horas
- Ataques promedio de 1 hora
- Europol cerró 48 sitios de DDoS-as-a-service

Héctor Espinoza Román

ENISA THREAD LANDSCAPE 2024



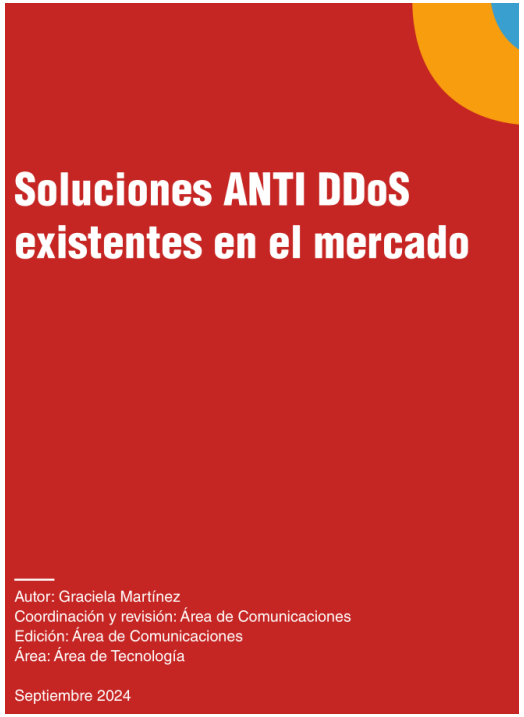
Soluciones anti-DDoS (LACNIC 2024)

Comerciales:

- Cloudflare
- Akamai
- AWS Shield
- Google Cloud Armor
- Imperva Incapsula
- Arbor Networks NETSCOUT
- F5 Networks

Código Abierto:

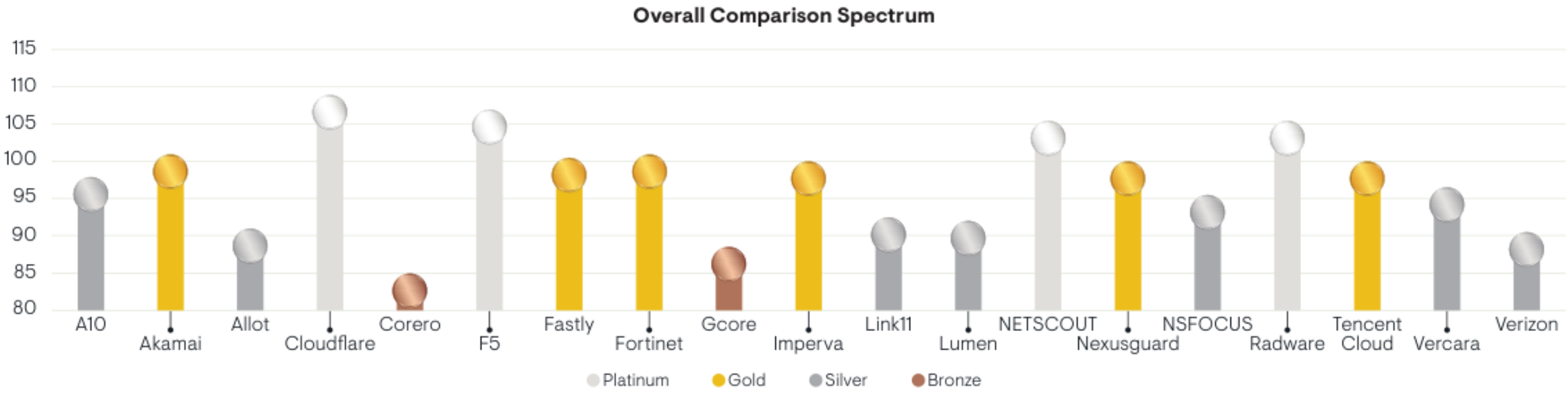
- HAProxy
- Gatekeeper
- FastNetMon



lacnic
www.lacnic.net

Héctor Espinoza Román

Mitigación DDoS (EMA PRISM Report



CONCLUSIÓN

- Variedad de actores involucrados.
- Ataque vigente con historia de muchos años.
- Variedad de sectores afectados.

- Servidores y usuarios más identificados y con cadena de responsabilidades.
- ¿Existe la posibilidad de reducir considerablemente los ataques *DoS mediante modificaciones estructurales?

GRACIAS

hector.espinoza@unitecnar.edu.co

UNITECNAR
FUNDACIÓN UNIVERSITARIA ANTONIO DE ARÉVALO

RIBCI - Red Iberoamericana de Blockchain y Ciberseguridad

CYTED
PROGRAMA IBEROAMERICANO DE CIENCIA
Y TECNOLOGÍA PARA EL DESARROLLO