Organiza

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

Comité AEC Industrias y Servicios para la Defensa

AEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

5º Encuentro de la industria nacional del sector de Defensa

Madrid, 24 de Abril de 2025

Patrocinadores AEC:

AENOR

brains/ INTERNATIONAL SCHOOLS

HITACHI Inspire the Next

NIPPON GASES The Gas Professionals

Telefónica Tech

THALES

TRIGO Global Quality Solutions

"Ciber amenazas y ciber guerra, lo que no se ve y sus efectos"

Igor Unanue

CTO, Thales S21sec

Igor.unanue@thalesgroup.com

Ciber amenazas

Principales ciber amenazas

Ransomware

Malware

APT

Denegación de servicio (DDoS)

Ingeniería social

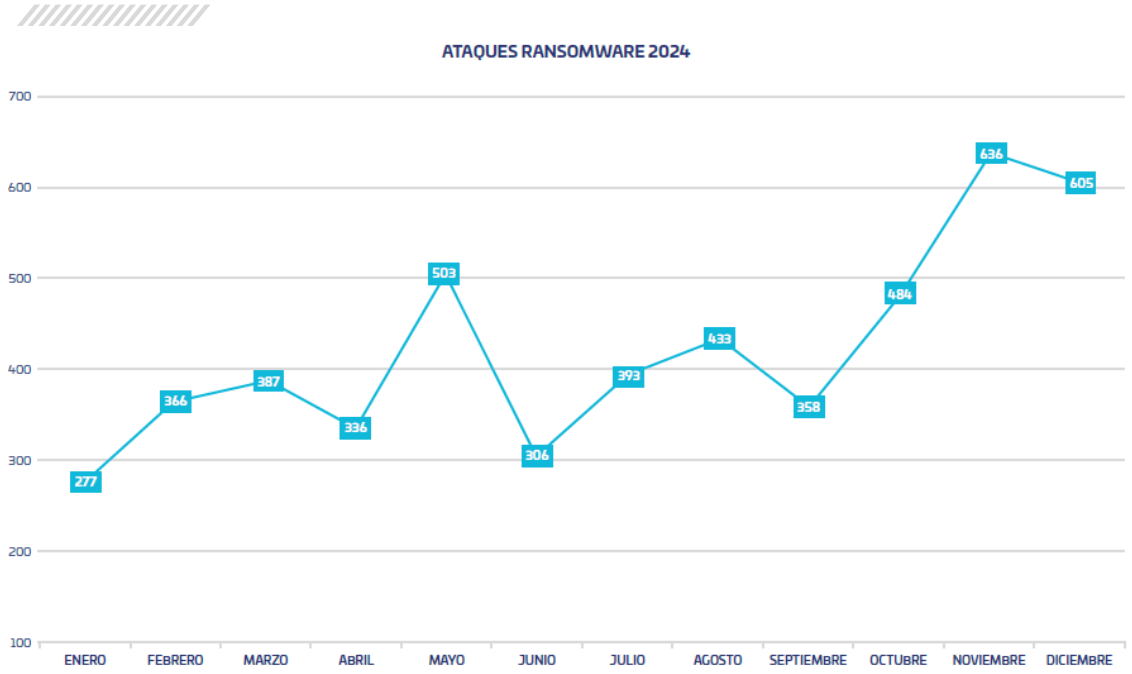
Zero-day exploit

Fuga de información

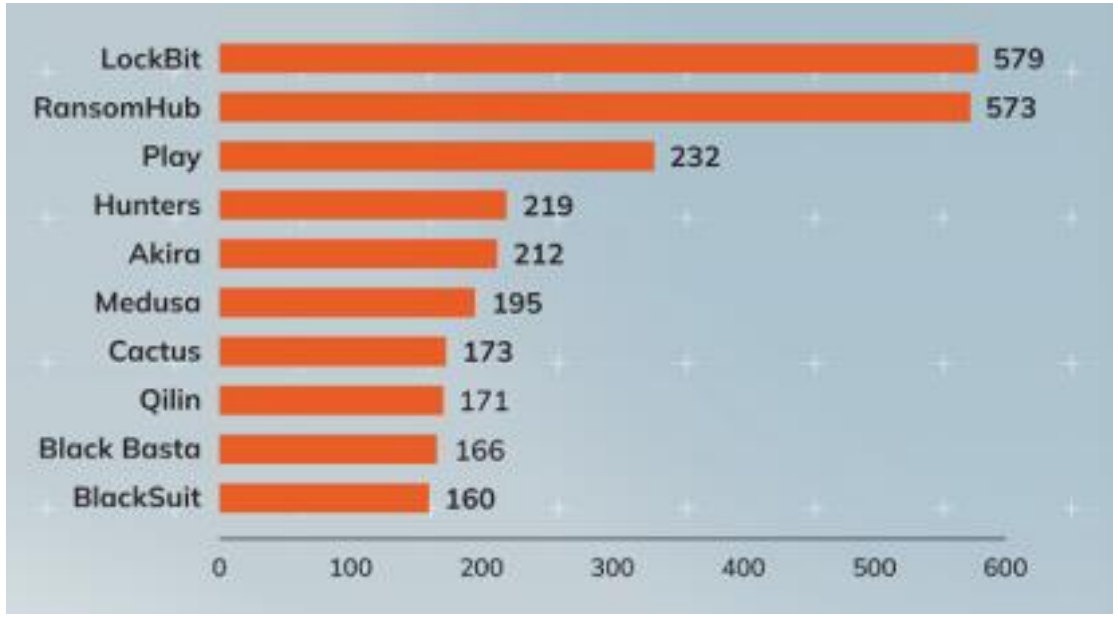
Ataque a proveedores

Top amenazas

Ransomware - 50,000$ a 800,000$ de media en extorsiones



Fuente: Thales S21sec - Threat Landscape Report 2024 H2



Fuente: Rapid7 - 2024 Threat Landscape Statistics

Top amenazas

Malware/Botnets – 27.968 C&C descubiertos, 19 millones de bots en más de 190 países

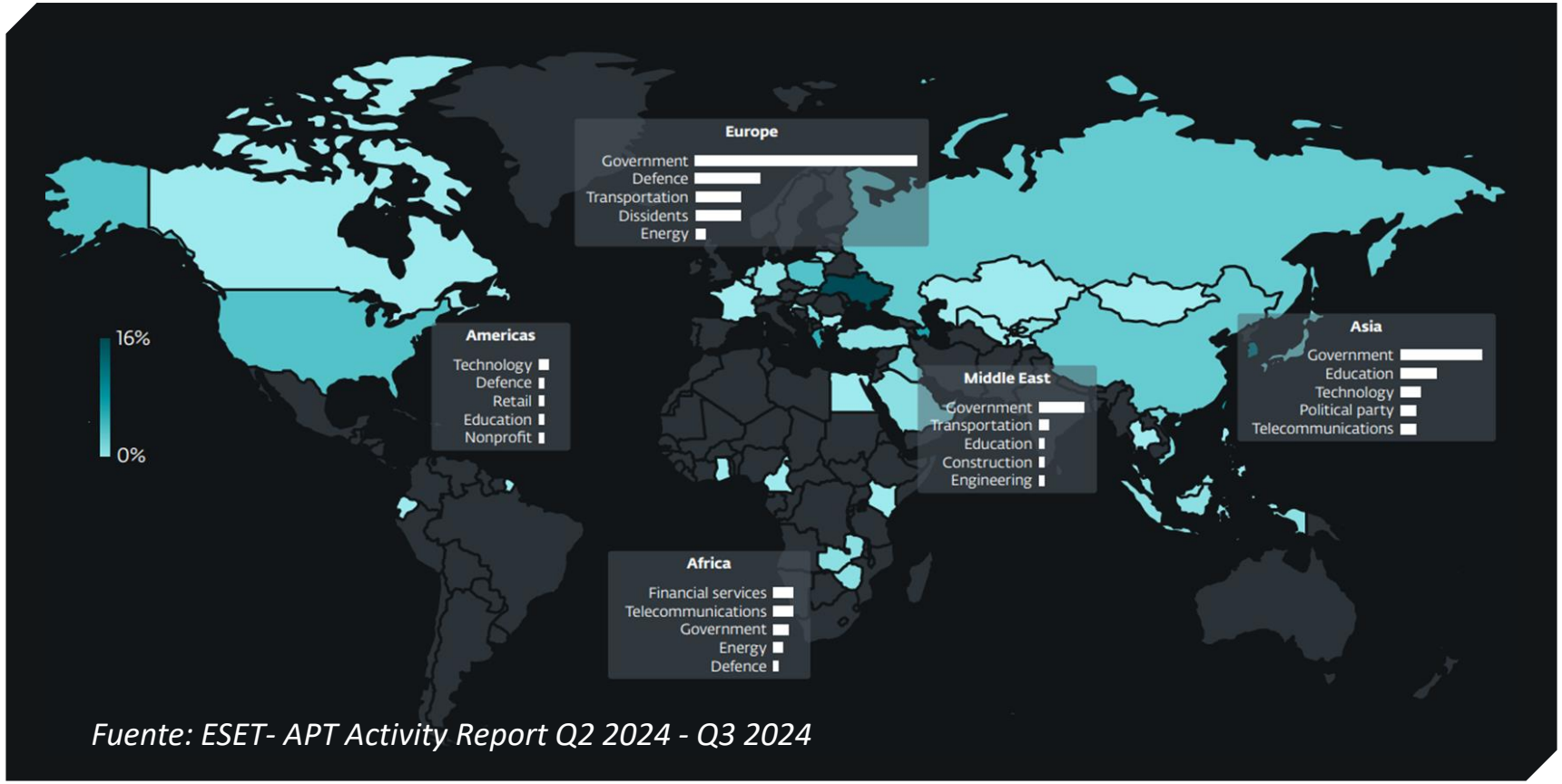
Rank	Country	Jan - Jun 2024	Jul - Dec 2024	% Change
#1	China	2,823	3,535	25%
#2	United States	2,702	2,286	-15%
#3	Russia	1,302	1,125	-14%
#4	Netherlands	737	782	6%
#5	Germany	742	657	-11%
#6	Bulgaria	715	544	-24%
#7	Singapore	332	382	15%
#8	Mexico	497	334	-33%
#9	United Kingdom	286	317	11%
#10	France	386	279	-28%

Rank	Country	Jan - Jun 2024	Jul - Dec 2024	% Change
#11	Sweden	226	275	22%
#12	Finland	135	213	58%
#12	Morocco	-	213	New entry
#14	Argentina	223	172	-23%
#15	Japan	128	136	6%
#16	Canada	144	128	-11%
#17	Vietnam	149	122	-18%
#18	Korea (Rep. of)	107	110	3%
#19	Colombia	135	107	-21%
#20	Spain	-	100	New entry

Fuente: Spamhouse project- Botnet Threat Update 2024

Top amenazas

APT: Países y sectores objetivo



Fuente: ESET- APT Activity Report Q2 2024 - Q3 2024

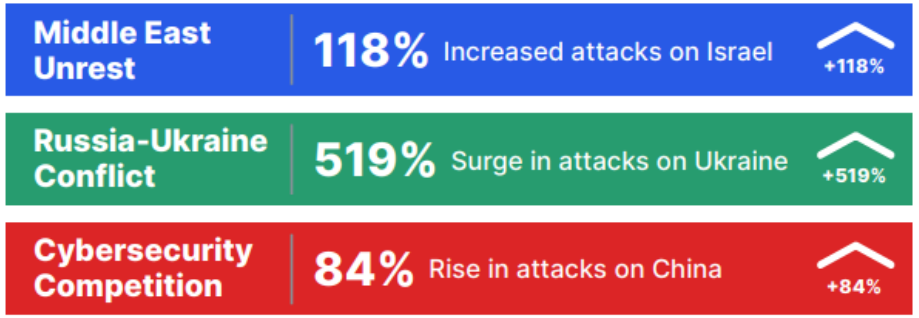
Top amenazas

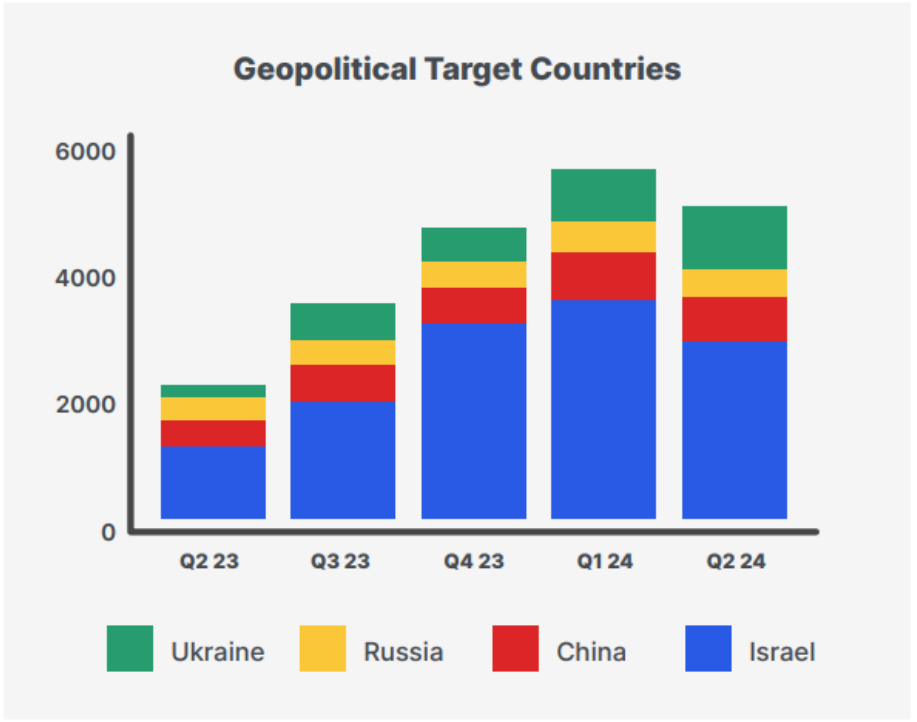
DDoS: Denegación de Servicio Distribuido

Ataque más importante: web de juegos online con **4.7 millones de RPS** desde **1.700 IPs** de Canada, India y EEUU

En telecomunicaciones aumentó un **548%** y en el sector sanitario **236%** respecto al primer semestre

Una web de entretemiento de China sufrio 4.2 millones de RPS desde 2.600 IPs de China y EEUU provocando **5 horas** de desconexión





Fuente: Thales Imperva - 2024-DDoS-Threat-Landscape-Report

Ciber guerra

Tipos de ciber guerra

7 tipos de ataque

Espionaje

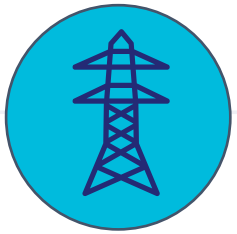
- Uso de **botnets** o ataques de **phishing**.
- Exfiltrar **información confidencial.**

Sabotaje

- **Robar** o **destruir** información.
- Aprovecharse de **amenazas internas.**

Denegación de Servicio

- **Interrumpir** operaciones y sistemas críticos.
- **Bloquear** el acceso a sitios web.



Red Eléctrica

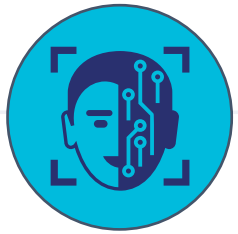
- **Desactivar sistemas críticos**.
- Interrumpir las **comunicaciones.**

Ataques de propaganda

- Intentos de **controlar** a las personas.
- Intentar que la gente pierda la **confianza** en su país.

Efectos económicos

- Atacar las redes de **instituciones económicas**
- Robar dinero o **impedir** que se pueda acceder a fondos.

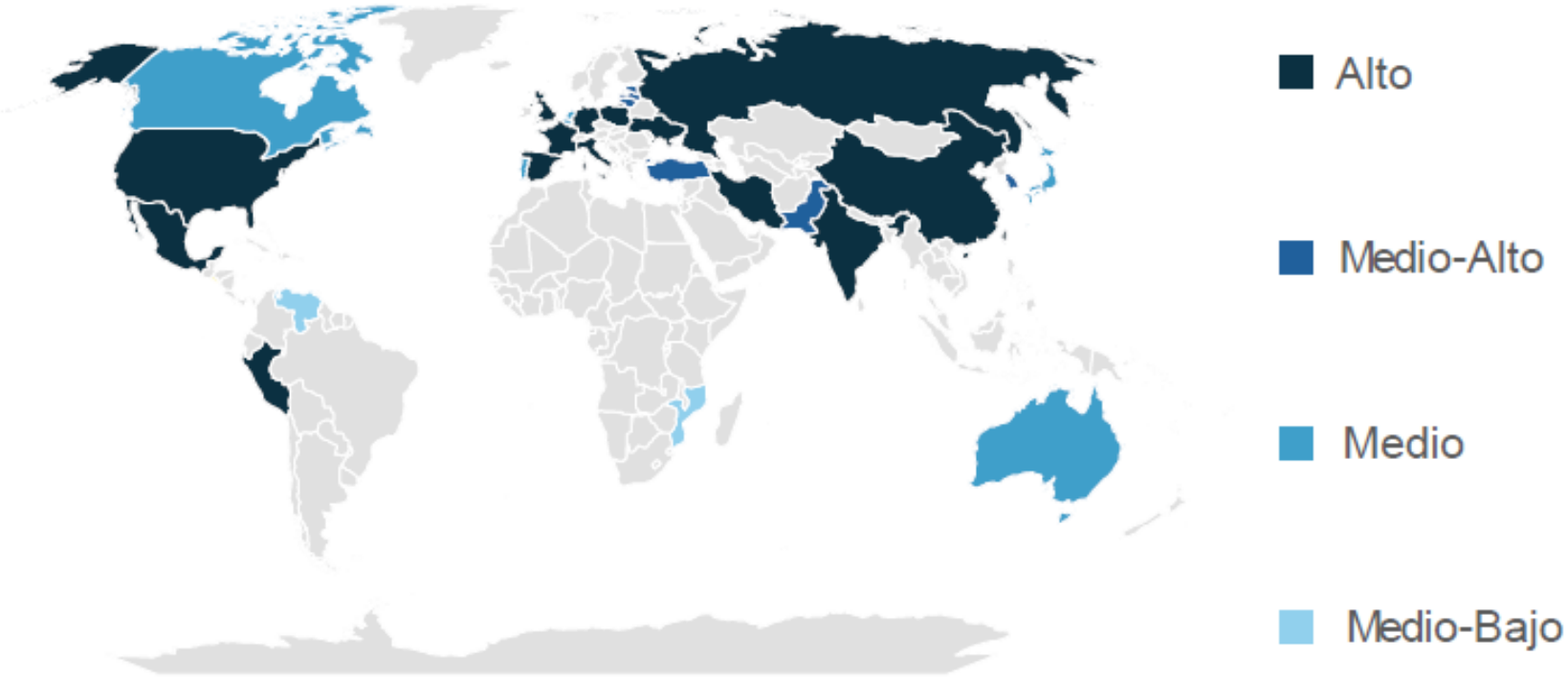


Ataques sorpresa

- **Ataque masivo inesperado.**
- Preparar el terreno para un **ataque físico.**

Impacto Ciber de los Conflictos Políticos

Nivel de relación entre Ciberataques y Geopolítica



Fuente: Thales S21sec - Threat Landscape Report 2024 H2

Ejemplo de operaciones de ciber guerra

Información que se hizo pública

1

Virus Stuxnet

Un gusano que atacó el programa nuclear iraní. El **malware** afectó a los sistemas de adquisición de datos y control de supervisión. Según la mayoría de los informes, el ataque **dañó gravemente** su capacidad para fabricar armas nucleares.

2

Soldado de Bronce

En 2007, Estonia trasladó una estatua relacionada con la Unión Soviética, el Soldado de Bronce, del centro de su capital, Tallin, a un cementerio militar cercano. Después sufrió varios ciberataques importantes en los meses siguientes. Los sitios web del gobierno estonio, los medios de comunicación y los bancos se vieron sobrecargados de tráfico debido a **ataques masivos de DDoS**.

3

Hackeo a Sony Pictures

Tras el estreno de la película "La Entrevista", que presentaba una imagen negativa de Kim Jong-un, se produjo un ataque contra Sony Pictures. El ataque se atribuye a hackers del gobierno norcoreano. El FBI encontró **similitudes con ataques de malware anteriores** de Corea del Norte, incluyendo código, algoritmos de cifrado y mecanismos de borrado de datos.

4

Fuerzas Ucranianas

Crowdstrike afirmó que el grupo ruso de cibercrimen organizado Fancy Bear atacó a las fuerzas militares y artillería ucranianas entre 2014 y 2016. El malware se propagó a través de una **aplicación de Android infectada** utilizada por la unidad de artillería del obús D-30 para gestionar los datos de objetivos.

Conflictos internacionales

Situaciones geopolíticas y guerras provocan ciberataques

Guerra entre Ucrania y Rusia

Una campana notable de APT28 consistió en correos electrónicos de phishing disfrazados de anuncios de coches.

Estos correos se utilizaron para instalar malware, siendo los principales objetivos los diplomáticos de las embajadas ucranianas. Estas operaciones ponen de manifiesto la sofisticación y el alcance de las actividades cibernéticas patrocinadas por el Estado durante el conflicto.

Conflicto Israel-Palestina

Campañas de los grupos hacktivistas tienen un trasfondo internacional, y se dedican a atacar a los Estados considerados enemigos del Estado que defienden, lo que genera sobre todo ataques DDoS y propaganda en línea.

Los grupos pro-Palestina tienden a atacar Estados europeos y Norteamérica, atacando sitios web gubernamentales, pero también de empresas nacionales, interrumpiendo su actividad y disponibilidad en línea.

Conflictos internacionales

Situaciones geopolíticas y guerras provocan ciberataques

China y EEUU

A diferencia de otros conflictos, en la dimensión ciber de estos rivales no intervienen grupos populares de hacktivistas, sino que la mayoría de las campañas están patrocinadas por el Estado.

China, el grupo APT Salt Typhoon logró penetrar en varios proveedores de telecomunicaciones de Estados Unidos para llevar a cabo sus campañas de espionaje, habiendo penetrado también en proveedores de telecomunicaciones de otros países.

Pakistán, India y Corea del Norte

Pakistán ha lanzado varios ataques contra la India dirigidos a infraestructuras críticas e instituciones gubernamentales. Los ciberataques los llevan a cabo varias APTs paquistaníes, como APT 36, SideCopy APT y RusticWeb APT, que se cree que han trabajado juntas. En cuanto a India, con APT SideWinder, a su vez ha llevado a cabo campañas de ciberespionaje.

EE. UU., Gran Bretaña y Corea del Sur alertaron del lanzamiento por parte de hackers norcoreanos de una campaña global de ciberespionaje, atribuyendo la campaña a APT45.

Cómo defenderse

Thales es uno de los mayores actores

Colaborando con organizaciones públicas, reguladores y LEAs

Galileo GPS

Integrating cybersecurity into the European Next-Gen GPS providing crypto components, Security Operation Centers…

European Union

Trusted partner of the EU, collaborating in Galileo GPS, Eurocontrol, Presidency of the EU Cybersecurity Organization

French MoD

Tight collaboration with French MoD for cybersecurity matters, from consultancy, auditing and technology providing.

NATO

Providing NATO members with unique "Cosmic Top Secret" tactical IP encryptor of the market

OneSky

Providing and securing the largest Air Traffic Control System ever, covering 11% of the planet (Australia)

ESA

First worldwide demonstration of a Satellite Hacking, to raise awareness of importance of cybersecurity is space

Somos Thales Cyber Services

Llevamos la ciberseguridad a sistemas críticos a nivel global…

…centrándonos en 7 verticales clave…

Servicios financieros

Sistemas de producción críticos

Automoción y Transporte

Aeroespacial

Espacio

Defensa

Gobiernos y Estados

… aprovechando las mejores tecnologías

La confianza como facilitadora de la transformación digital

ADN **Dual IT-OT** para una conectividad segura

Clouds como corazón de los sistemas más modernos

… solventando los desafíos de los clientes en materia de ciberseguridad

21 países

con Ciber Consultoría y Centros de Competencia

11 SOCs

Dando cobertura a IT y OT, regulados y no-regulados

1 portfolio

- Consultoría
- Detección y Respuesta
- Ciber Integración

Organiza

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

Comité AEC Industrias y Servicios para la Defensa

AEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Plataforma Federada de Threat Intel

Otras herramientas ad-hoc de Thales

Equipo interno de Threat Intel

Publicación de vulnerabilidades Zero-day

Equipo interno de Counter Threat Intel

Plataforma de Threat Intelligence

Potenciar la defensa proactiva con Threat Intel en tiempo real, detección avanzada e inteligencia accionable.

Análisis de Botnets Privados

- Visibilidad de Dark & Deep Web
- OSINT (Open Source Intelligence)

+1k Grupos APT monitoreados

307M Credenciales robadas

420K Tarjetas de crédito

9.7K Malware cada día

11K Familias de Malware

3.5M Archivos analizados

Phishing

- Threat Hunting & Takedown
- OSINT & Threat Intelligence

3.3B URLs analizadas

3.8K URLs monitoreadas

Vulnerabilidades Zero-day

- Monitoreo de Exploits
- Vulnerability Intelligence & CVE

81 Publicadas, todas de ICS/OT

Beneficios para nuestros clientes

513K IoC únicos en nuestras **propias sandbox**

20M Relaciones contextuales

40% De los incidentes se detectan gracias a **nuestra plataforma de Threat Intel**

43% IoCs propietarios accionables

58% IoAs propietarias accionables

*2024 updated

Organiza

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

Comité AEC Industrias y Servicios para la Defensa

AEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

Counterintel Unit (CTIU)

Equipo de investigación dedicado

- Investigación y análisis de bandas.
- Acceso a bandas y al panel de control de botnets.

Investigaciones más relevantes

- **Dridex** - 2014 a 2016
- **Trickbot + Ryuk** – Desde 2017
- **Vidar** – Desde 2021

Reconocimientos

FBI, Europol and Civil Guard have dismantled the cybercriminal organization that created this "malware" with the help of the Spanish company specializing in cybersecurity S21sec.

ABC Tecnología

Nuestro ecosistema de Threat Intel integra **herramientas propias (Sandbox), investigación y fuentes de terceros**, y mapea los TTP utilizados por los ciberdelincuentes.

Esta inteligencia **alimenta múltiples servicios, como Threat Hunting, la respuesta a incidentes, Red team, el SOC y el EDRaaS**, al tiempo que permite la creación de reglas de detección personalizadas para diversos stacks.

11 SOCs a nivel Global

SOC Madrid

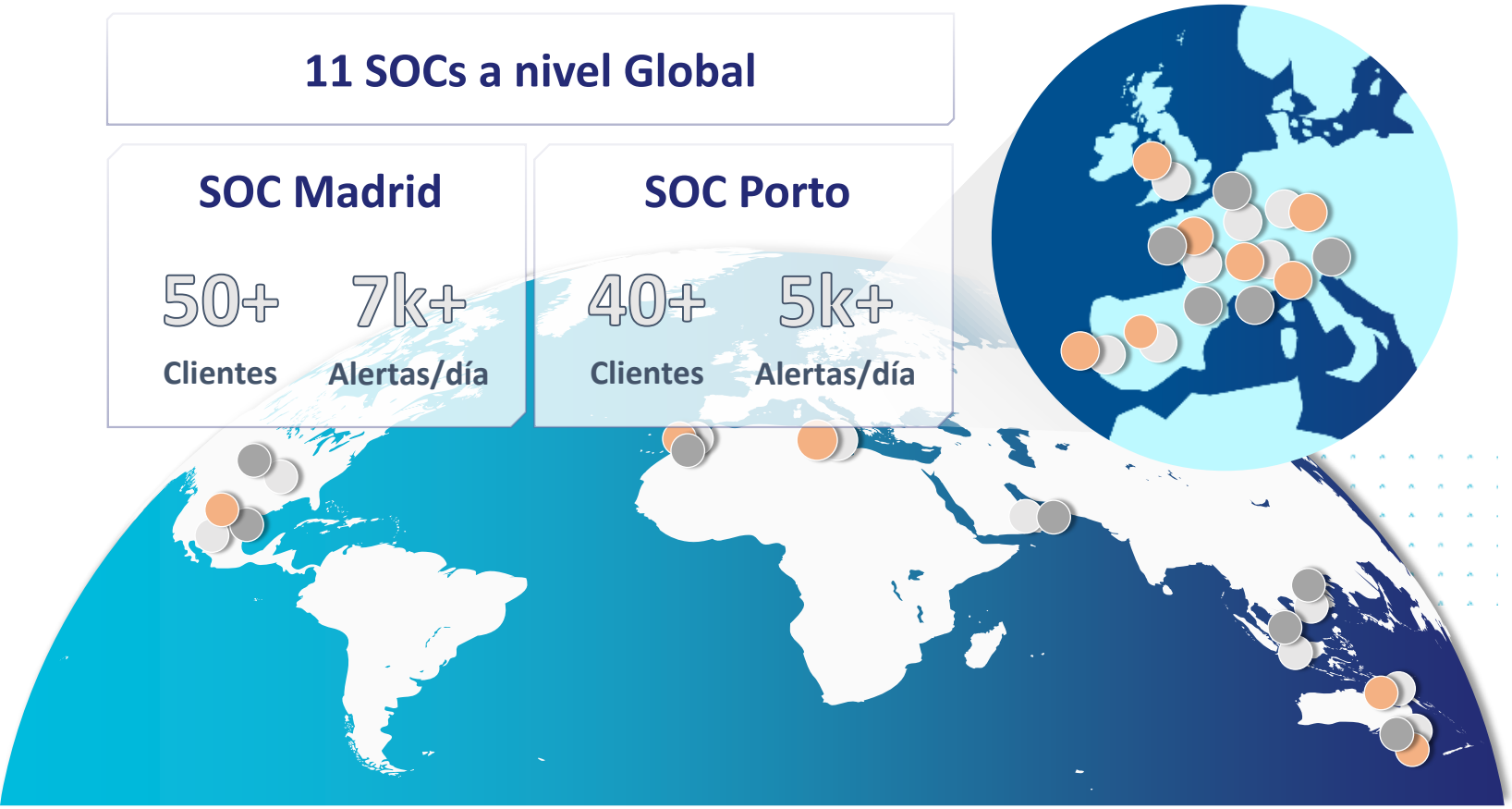
50+ Clientes

7k+ Alertas/día

SOC Porto

40+ Clientes

5k+ Alertas/día



Equipos locales atienden a sus clientes + DR para otro equipo.

Datacenters redundantes.

Las mismas tecnologías para el servicio.

Herramientas unificadas, procesos optimizados y procedimientos estandarizados.

CERTIFICACIÓN DE CONFORMIDAD CON EL ens Esquema Nacional de Seguridad Categoría ALTA RD 311/2022

AENOR SEGURIDAD INFORMACIÓN ISO/IEC 27001

AENOR GESTIÓN CONTINUIDAD NEGOCIO ISO 22301

NIS2 Directive

DORA Digital Operational Resilience Act

Red Nacional de SOC

CSIRT.es

CERT.PT Centro Nacional de Cibersegurança PORTUGAL

FIRST

CERTIFIED BY TI TRUSTED INTRODUCER

Organiza

GOBIERNO DE ESPAÑA MINISTERIO DE DEFENSA

Comité AEC Industrias y Servicios para la Defensa

AEC ASOCIACIÓN ESPAÑOLA PARA LA CALIDAD

CONSULTORÍA

Riesgos, Gobernanza y Cumplimiento

- Estrategia, asesoramiento e implementación
- CISOaaS
- Simulación y Gestión de Crisis
- Capacitación y entrenamiento

Servicios Ofensivos

- Penetration testing
- Red teaming & purple teaming
- Auditorías Técnicas

INTEGRACIÓN

Servicios

- Arquitectura y diseño
- Integración, implementación y gestión

Tecnologías de terceros

- Licencias independientes
- Soporte y Gestión

Para entornos Cloud, OT, Sistemas embebidos, IA, Normativas, etc.

DETECCIÓN Y RESPUESTA

Threat Intelligence

- Cyber Threat Intelligence
- Digital Risk Protection Services (DRPS)
- External or Internal Attack Surface Management
- Gestión de vulnerabilidades

Otros

- Servicios de Cloud Gestionada (AUS)
- Servicios NOC (UK)
- CNAPP/SASE/CASB/CSPM
- Servicios operados DDOS
- Gestión de IAM, HSM, PAM, otros.

Servicios de Detección y Respuesta

- Managed Detection & Response (MDR) – *SOC totalmente gestionado, SOC híbrido, SOC regulado*
- Advanced Threat Hunting
- DFIR Retainer u On-demand
- Apoyo en la Gestión de Crisis

Para entornos Cloud, OT, Sistemas embebidos, IA, Normativas, etc.

Sectores estratégicos

133 Administración Pública

123 Servicios Financieros, Seguros y Fintech

63 Consumo & Retail

Consultoría **45**

Medios y Comunicación **10**

124 Tecnología y Telecomunicaciones

93 Industria & Manufactura

68 Sanidad, Farmacia & Biotech

Energía y Servicios **57**

42 Automoción y Transporte

¿PREGUNTAS?

MUCHAS GRACIAS

linkedin.com/in/igor-unanue-buenetxea-b95ab326

Igor.unanue@thalesgroup.com