YARIX

Informe Nacional Sobre el Panorama de Las Amenazas Cibernéticas

España 2025

TLP: GREEN* | FEBRERO DE 2026

TLP:GREEN: Divulgación limitada, los destinatarios pueden difundirla dentro de su comunidad. Las fuentes pueden utilizar TLP:GREEN cuando la información sea útil para aumentar la concienciación dentro de su comunidad en general. Los destinatarios pueden compartir la información TLP:GREEN con sus homólogos y organizaciones asociadas dentro de su comunidad, pero no a través de canales de acceso público. La información TLP:GREEN no puede compartirse fuera de la comunidad. Nota: cuando no se defina «comunidad», se asumirá que se trata de la comunidad de ciberseguridad/defensa. Fuente: **https://www.first.org/tlp/**

Descargo de responsabilidad: La información y las imágenes de este informe se han recopilado de fuentes disponibles públicamente, así como de fuentes cerradas supervisadas por el equipo de Inteligencia sobre Amenazas Cibernéticas de Yarix (YCTI, por sus siglas en inglés) (por ejemplo, foros, mercados y canales clandestinos de la Dark Web). En el caso de la información obtenida de fuentes cerradas, cualquier referencia en las imágenes del informe se ha ocultado o anonimizado intencionadamente.

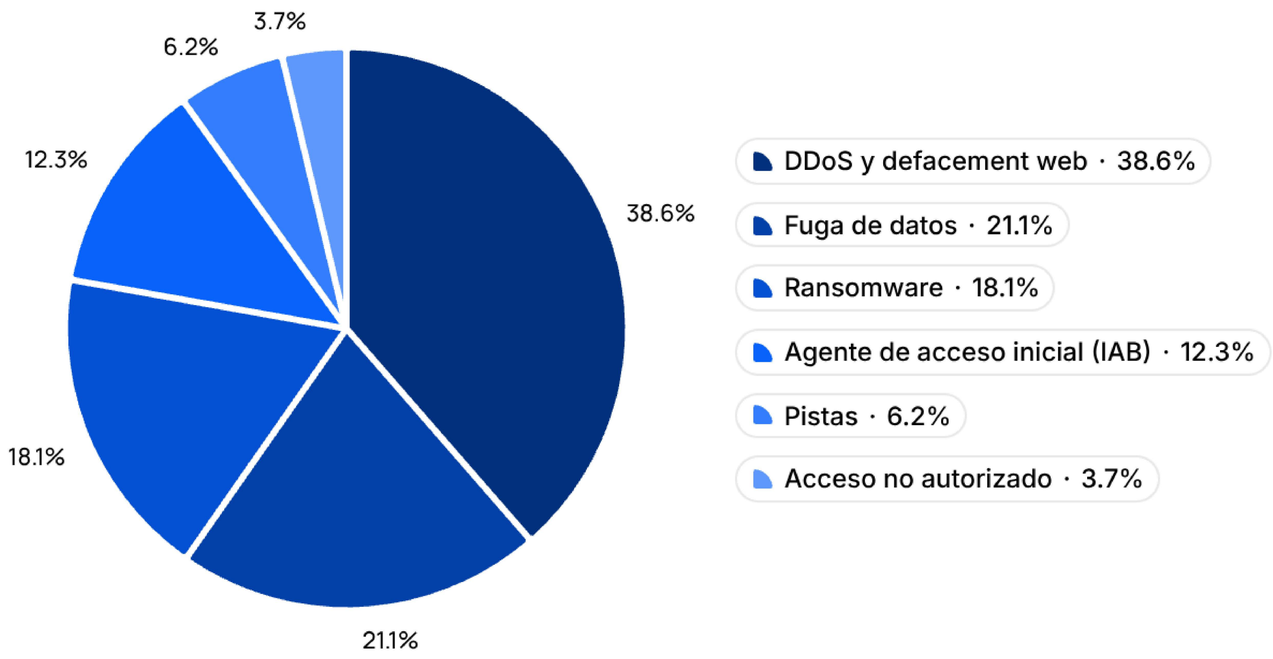
Índice

1. Resumen ejecutivo

En este informe, el equipo de Yarix Cyber Threat Intelligence (YCTI) ha analizado un conjunto de amenazas cibernéticas significativas dirigidas a empresas con sede en España, supervisadas a lo largo de 2025 (del 1 de enero al 31 de diciembre).

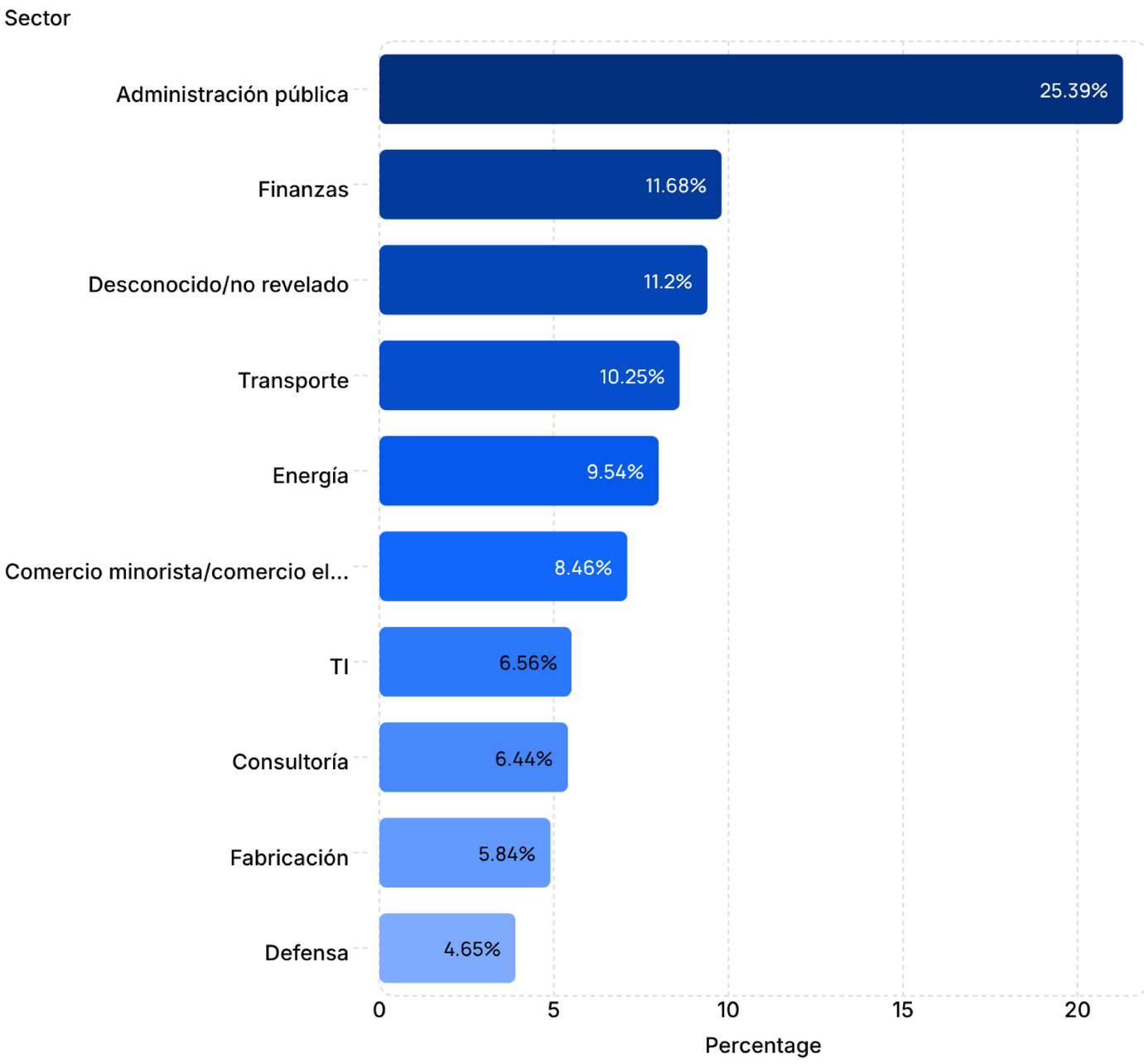
Las estadísticas presentadas en el informe se refieren a toda la muestra analizada. Por su parte, en la sección 3. *Ciberataques dirigidos a organizaciones españolas - 2025*, solo se incluye una submuestra representativa de cinco ciberamenazas relevantes observadas.

Teniendo en cuenta los tipos de eventos detectados, el equipo de YCTI observó lo siguiente:



En cuanto a la distribución de los sectores afectados por el número total de ciberamenazas registradas contra organizaciones españolas, el equipo de YCTI identificó 24 sectores afectados (incluidos los sectores marcados con la voz Desconocido/no revelado). A continuación se muestra la lista de los 10 sectores más afectados en España:

1. Administración pública (21,3 %)
2. Finanzas (9,8 %)
3. Desconocido/no revelado (9,4 %)
4. Transporte (8,6 %)
5. Energía (8,0 %)
6. Comercio minorista/comercio electrónico (7,1 %)
7. TI (5,5 %)
8. Consultoría (5,4 %)
9. Fabricación (4,9 %)
10. Defensa (3,9 %)



Teniendo en cuenta la cronología del total de ataques registrados en 2025 contra entidades en España, el equipo de YCTI observó una distribución relativamente uniforme a lo largo de la mayor parte de los meses del año, con un pico significativo en las amenazas registradas durante marzo (10,6 %) y agosto (13,4 %) y entre octubre (9,9 %) y noviembre (16,9 %).

Este informe ofrece un análisis en profundidad de las ciberamenazas dirigidas a empresas y organizaciones en España. En concreto:

Sección 2: Panorama de amenazas - España - 2025 Describe los detalles de las ciberamenazas dirigidas a organizaciones españolas, incluyendo una cronología de los ataques y los sectores más afectados.

Sección 3: Ciberataques dirigidos a organizaciones españolas - 2025 Ofrece una descripción detallada de las amenazas cibernéticas más significativas registradas por el equipo CTI.

Sección 4: Análisis en profundidad de las amenazas de ransomware en España - 2025 Ofrece una visión detallada de la amenaza de ransomware a la que se enfrentan las organizaciones españolas, con estadísticas sobre los sectores y el tamaño de las entidades afectadas.

Sección 5: Resumen de las actividades hacktivistas contra organizaciones españolas - 2025 Ofrece un análisis detallado de las actividades hacktivistas dirigidas contra organizaciones españolas en 2025. También incluye un resumen de los actores implicados en las amenazas y los sectores más afectados por las amenazas hacktivistas. Además, la sección destaca los factores geopolíticos clave para comprender mejor las posibles motivaciones y el panorama general que se esconde tras las amenazas hacktivistas en España.

Por último, el informe incluye observaciones sobre las seis categorías principales de ciberamenazas observadas y ofrece hipótesis sobre posibles escenarios de riesgo en España para 2026.

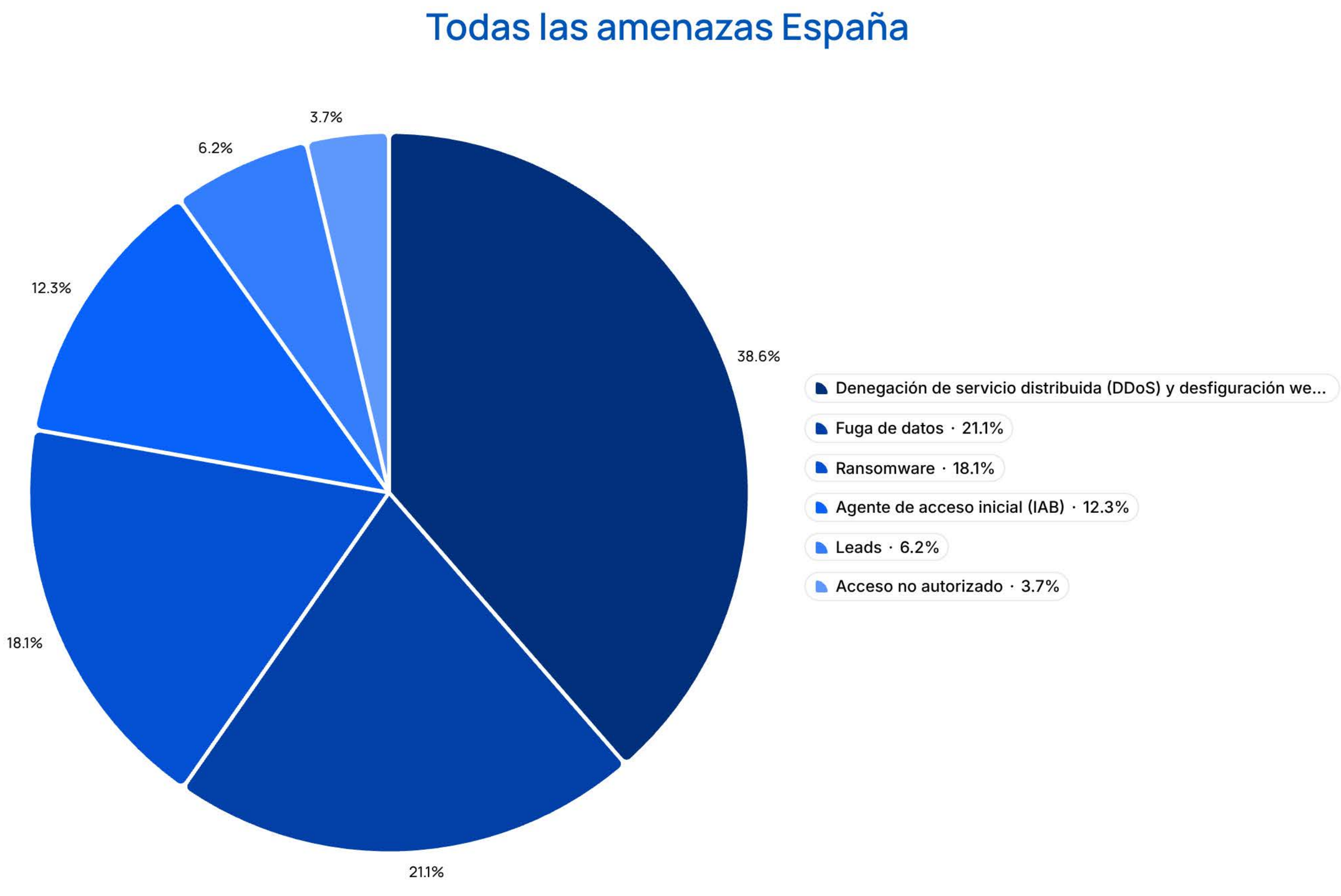
2. Panorama de amenazas: España, 2025

A continuación se presentan los datos recopilados por el equipo de Yarix Cyber Threat Intelligence (YCTI) sobre las amenazas cibernéticas observadas contra organizaciones en España durante 2025.

2.a. Tipos de amenazas observadas

El equipo YCTI llevó a cabo un análisis de las amenazas cibernéticas registradas durante 2025 dirigidas a organizaciones españolas.

La tabla siguiente enumera las seis categorías principales a las que pertenecen las amenazas observadas, junto con sus correspondientes incidencias expresadas en puntos porcentuales.



Macro Categorías de amenazas cibernéticas observadas

Ransomware

Tipo de software malicioso que bloquea el acceso a los sistemas informáticos mediante el cifrado de datos, con el objetivo de obtener un rescate de la víctima a cambio de recuperar el acceso a los sistemas. Si la víctima no paga el rescate solicitado en el plazo establecido, los datos dejarán de ser accesibles y se perderán de forma permanente. Los grupos de ransomware también han adoptado el denominado método de doble extorsión, en el que, además de hacer inaccesibles los sistemas, si no se paga el rescate, publican los datos exfiltrados en la Dark Web, poniéndolos a disposición de la comunidad ciberdelincuente.

Denegación de servicio distribuida (DDoS) y defacement web

Los ataques DDoS consisten en que uno o varios actores maliciosos bloquean el tráfico a un servidor, servicio o red aprovechando dispositivos comprometidos, como ordenadores o dispositivos IoT, que se convierten en «bots» o «zombis». Estos bots forman una botnet controlada de forma remota por el atacante para saturar el sistema de la víctima con tráfico, provocando la interrupción del servicio. Dado que cada bot es un dispositivo legítimo de Internet, puede resultar difícil distinguir el tráfico de ataque del tráfico normal. El defacement web se refiere a la alteración no autorizada de la página de inicio o las páginas internas de un sitio web, sustituyéndolas por mensajes de los atacantes. Esta intrusión puede provocar interrupciones en el servicio y dañar la reputación de la organización.

Agente de acceso inicial (IAB)

Los ciberataques suelen incluir una fase de reconocimiento preparatoria dirigida a la víctima. Durante esta fase, los actores maliciosos recopilan datos relevantes, como las tecnologías utilizadas, la información expuesta públicamente y datos económicos y organizativos (por ejemplo, altos cargos, dirección, personal). Además de esta información, los actores maliciosos recurren a foros conocidos y mercados negros de la Dark Web para comprar y vender puntos de acceso relacionados con sus objetivos de interés. Estos puntos de acceso son vendidos por una categoría específica de ciberdelincuentes conocidos como intermediarios de acceso inicial (IAB), cuya función es vender puntos de entrada al perímetro de ciberseguridad de empresas y organizaciones.

Acceso no autorizado

Acceso no autorizado a los sistemas informáticos de una organización, empresa o individuo, con la intención de interrumpir su funcionamiento y/o extraer datos. Este tipo de actividad se lleva a cabo generalmente con fines de espionaje político o industrial, pero también puede ser utilizada por grupos hacktivistas para promover causas ideológicas o sociales.

Data Leakage (Fuga de datos)

Pérdida de datos como resultado de vulnerabilidades del sistema o debido a una operación llevada a cabo por uno o más actores maliciosos. Por lo general, los datos robados se distribuyen de forma gratuita o a cambio de una tarifa a través de ventas individuales o subastas públicas en la Dark Web. En algunos casos, los datos se comparten con periodistas de investigación o medios de comunicación para difundirlos aún más y causar un mayor daño a la reputación de la víctima.

Leads

En el cibermundo clandestino, los «leads» se refieren a la información robada de los clientes, como la información de identificación personal, los datos de las tarjetas de crédito, las credenciales de inicio de sesión y los historiales médicos. Estas pistas son valiosas para los ciberdelincuentes para el robo de identidad, el fraude y los ataques dirigidos, como el phishing. A menudo se comparten, venden o intercambian libremente en los mercados clandestinos.

2.b. Distribución sectorial de todas las amenazas cibernéticas registradas

Teniendo en cuenta la distribución de los sectores afectados por todas las amenazas cibernéticas monitorizadas contra organizaciones españolas, el equipo de YCTI observó 24 sectores afectados, incluidos los sectores Desconocido/no revelado y Otros):

1. Gobierno 21,3 %
2. Finanzas 9,8 %
3. Desconocido 9,4 %
4. Transporte 8,6 %
5. Energía 8,0 %
6. Comercio minorista 7,1 %
7. Tecnologías de la información 5,5 %
8. Consultoría 5,4 %
9. Fabricación 4,9 %
10. Defensa 3,9 %
11. Hostelería 3,7 %
12. Salud 3,4 %
13. Educación 1,9 %
14. Agricultura y producción alimentaria 1,7 %
15. Sociedad civil 0,8 %
16. Entretenimiento 0,8 %
17. Construcción 0,7 %
18. Servicios técnicos 0,7 %
19. Fuerzas del orden 0,7 %
20. Automoción 0,6 %
21. Noticias - Medios de comunicación 0,5 %
22. Inmobiliario 0,4 %
23. Multisectorial 0,1 %
24. Otros 0,1 %

A continuación se muestra un desglose de las amenazas clasificadas en las seis categorías de amenazas clasificadas por el equipo CTI, junto con su impacto en los respectivos sectores.

2.b.i. Ataques DDoS y desfiguración web

La amenaza de DDoS y desfiguración web representó el 38,6 % del total de amenazas registradas en 2025 contra empresas, entidades y organizaciones en España. Esta amenaza afectó a 14 sectores diferentes. A continuación se muestra la lista de los 5 sectores más afectados:

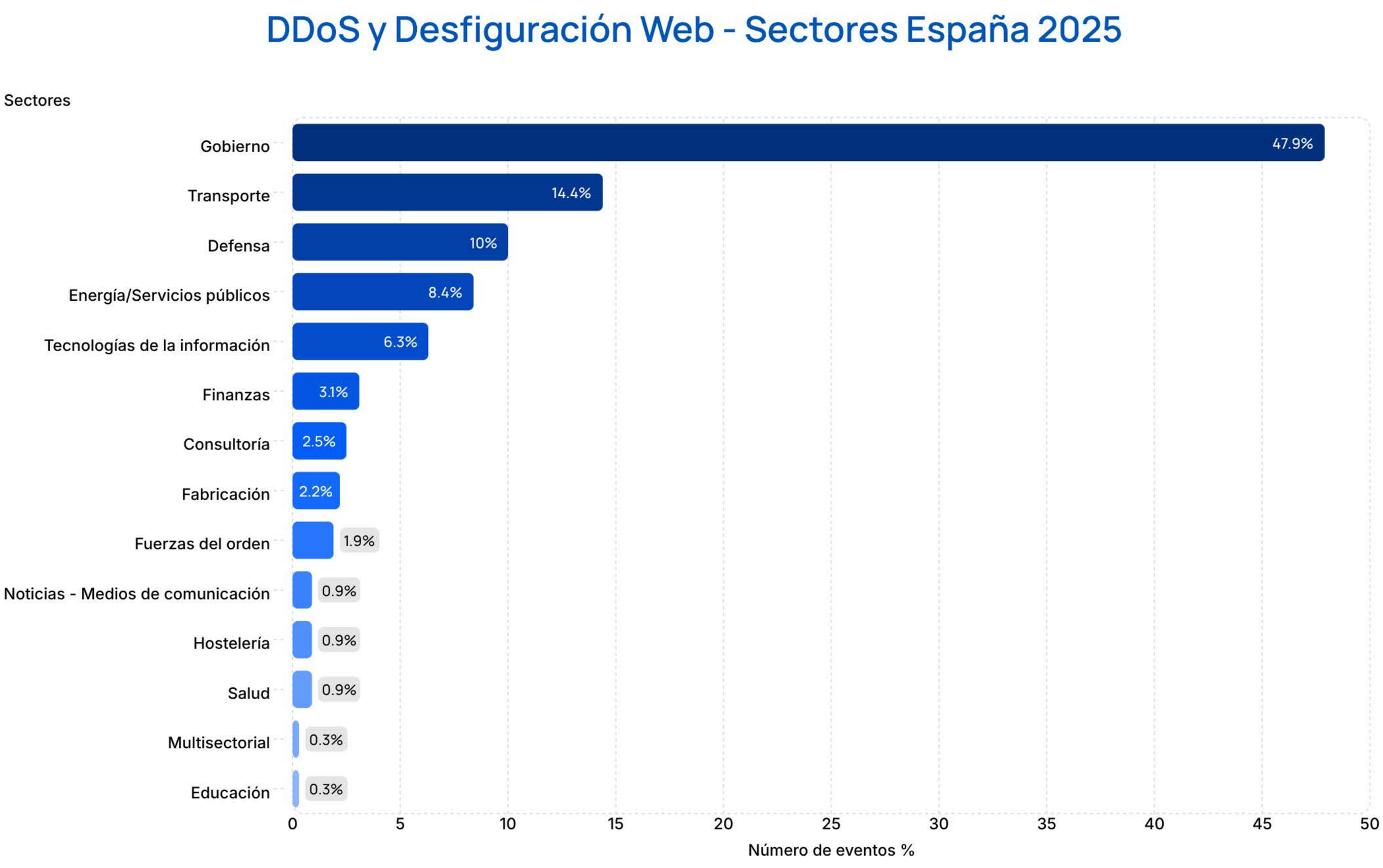
1. Gobierno/Fuerzas del orden (48,0 %)
2. Transporte (14,4 %)
3. Defensa (10,0 %)
4. Energía (8,4 %)
5. TI (6,3 %)

A continuación se muestra la lista de los cinco actores más activos en la categoría de amenazas DDoS y desfiguración web.

Los porcentajes se calculan en función del número total de eventos de DDoS y desfiguración web atribuidos únicamente a esta categoría, incluida la entrada «Desconocido/No revelado».

1. Noname057(16) (50,3 %)
2. Mr Hamza (21,1 %)
3. Dark Storm Team (5,3 %)
4. Twonet (3,4 %)
5. Desconocido/No revelado (3,1 %)

A continuación, se proporcionan los detalles del total de eventos registrados contra el sector específico afectado:



2.b.ii. Fuga de Datos

La amenaza de Fuga de Datos representó el 21,1% del total de eventos registrados en 2025 contra empresas, entidades y organizaciones en España. Esta amenaza afectó a 18 sectores diferentes. A continuación se muestra la lista Top-5 de los sectores específicos más afectados:

1. Finanzas (19,4 %)
2. Energía (13,1 %)
3. Comercio minorista (12,6 %)
4. Salud (7,4 %)
5. TI (6,9 %); Gobierno (6,9 %)

A continuación se muestra la clasificación de los cinco principales actores maliciosos/canales clandestinos más activos en la categoría de amenazas de fuga de datos. Los porcentajes se calculan en función del número total de incidentes de fuga de datos atribuidos únicamente a esta categoría, incluida la entrada «Desconocido/No revelado».

1. Desconocido (5,7 %)
2. bateria (5,1 %)
3. Altamar (3,4 %)
4. nosferatu (2,9 %)
5. sophia01 (2,3 %); vaquilla (2,3 %)

A continuación se proporciona el desglose detallado del total de eventos que afectaron al sector específico objetivo.

Fuga de datos

Sectores – España – Data Leak		
ID	**Sectores**	**Número de eventos %**
1.	Finanzas	19,4%
2.	Energía	13,1%
3.	Comercio minorista	12,6%
4.	Salud	7,4%
5.	TI	6,9%
6.	Gobierno	6,9%
7.	Consultoría	6,3%
8.	Transporte	5,7%
9.	Educación	4,6%
10.	Desconocido	4,0%
11.	Hostelería	4,0%
12.	Fabricación	2,3%
13.	Sociedad civil	1,7%
14.	Entretenimiento	1,7%
15.	Construcción	1,1%
16.	Agricultura y alimentación	1,1%
17.	Servicios técnicos	0,6%
18.	Automoción	0,6%

2.b.iii. Ransomware

La amenaza del ransomware representó el 18,1 % del total de amenazas registradas en 2025 contra empresas, entidades y organizaciones en España. Esta amenaza afectó a 20 sectores diferentes. A continuación se muestra la lista de los cinco sectores específicos más afectados:

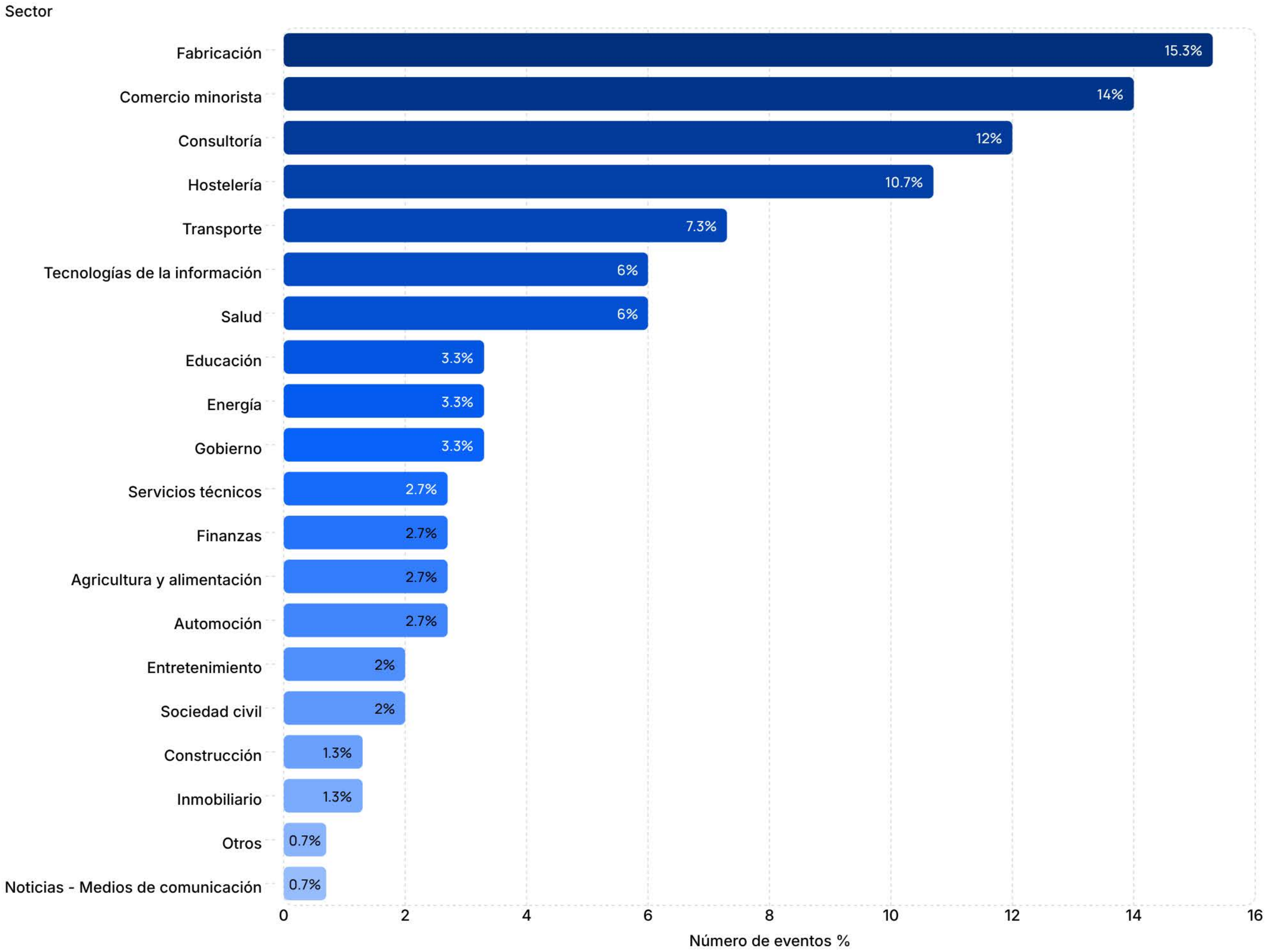
1. Fabricación (15,3 %)
2. Comercio minorista/comercio electrónico (14,0 %)
3. Consultoría (12,0 %)
4. Hostelería (10,7 %)
5. Transporte/Logística (7,3 %)

A continuación se muestra la clasificación de los cinco actores más activos en la categoría de amenazas de ransomware. Los porcentajes se calculan en función del número total de incidentes de ransomware atribuidos únicamente a esta categoría, incluida la entrada «Desconocido/No revelado».

1. Qilin (22,0 %)
2. Akira (10,0 %)
3. LockBit (4,5 %)
4. Space Bears (4,5 %)
5. SafePay (4,0 %); Arcusmedia (4,0 %); INC Ransom (4,0 %)

A continuación se muestra el desglose detallado del total de eventos registrados en relación con el sector específico afectado:

Sectores – España – Ransomware



2.b.iv. Agente de acceso inicial

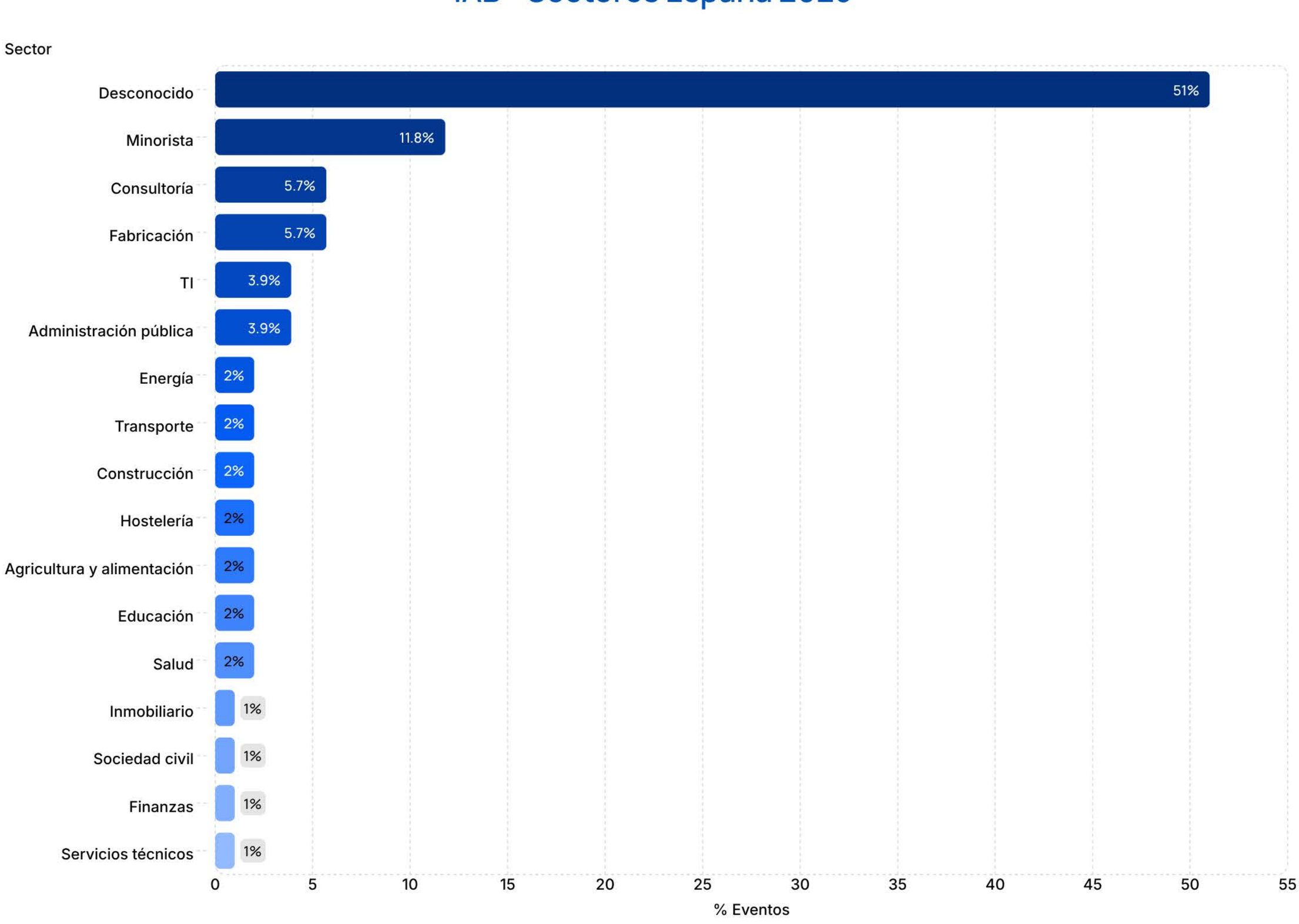
La amenaza del agente de acceso inicial representó el 12,3 % del total de incidentes registrados en 2025 contra empresas, entidades y organizaciones en España. Esta amenaza afectó a 17 sectores diferentes (incluidos los objetivos desconocidos o no revelados). Es importante señalar que, debido a la naturaleza de esta amenaza, no siempre es posible identificar con precisión el sector afectado. En muchos casos, los actores maliciosos no revelan deliberadamente el sector o la identidad de la organización para la que poseen o venden el acceso inicial, como medida de precaución. Como resultado, un alto porcentaje de los sectores afectados se clasifican como Desconocido/No revelado.

A continuación se muestra la lista de los cinco sectores específicos más afectados por la amenaza:

1. Desconocido/No revelado (51,0 %)
2. Comercio minorista/Comercio electrónico (11,8 %)
3. Consultoría (5,7 %)
4. Fabricación (5,7 %)
5. TI (3,9 %); Gobierno (3,9 %)

A continuación se muestra la clasificación de los cinco principales actores maliciosos/canales clandestinos más activos en la categoría de amenazas de intermediarios de acceso inicial (IAB). Los porcentajes se calculan en función del número total de eventos de intermediarios de acceso inicial (IAB) atribuidos únicamente a esta categoría, incluida la entrada Desconocido/No revelado.

1. cosmodrone (13,7 %)
2. miyak0 (10,8 %)
3. rassvettt (5,9 %)
4. Big-Bro (4,9 %); akr1t (4,9 %); Reve (4,9 %)
5. 361Crimelife (2,9 %); niggaboi (2,9 %); kobenotnow (2,9 %)



2.b.v. Leads

La amenaza de los Leads representó el 6,2% del total de eventos monitorizados en 2025 contra empresas, entidades y organizaciones en España. Esta amenaza afectó a 7 sectores diferentes (incluidos los objetivos Desconocidos/No revelados). Es importante señalar que, debido a la naturaleza de la amenaza, no siempre es posible identificar con precisión el sector relevante de los datos contenidos en las recopilaciones de Leads. Como resultado, un alto porcentaje de los sectores afectados se clasifican en la categoría «Desconocido/No revelado».

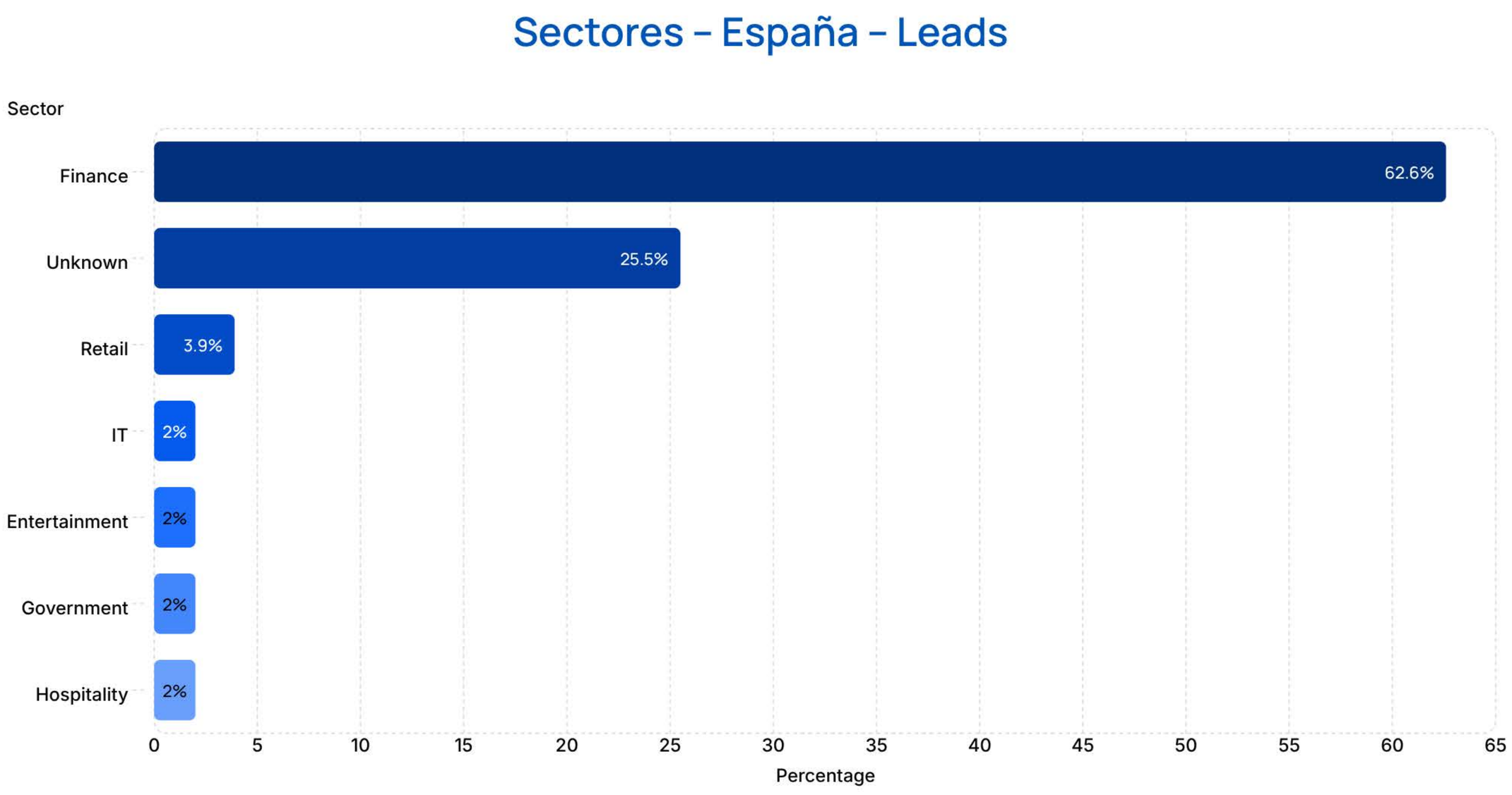
A continuación se muestra la lista de los cinco sectores específicos más afectados por la amenaza:

1. Finanzas (62,6 %);
2. Desconocido/No revelado (25,5 %);
3. Comercio minorista (3,9 %);
4. Tecnologías de la información (2,0 %);
5. Entretenimiento (2,0 %).

A continuación se muestra la clasificación de los cinco principales actores maliciosos/canales clandestinos más activos en la categoría de amenazas «Leads». Los porcentajes se calculan en función del número total de eventos «Leads» atribuidos únicamente a esta categoría, incluida la entrada «Desconocido/No revelado».

1. bateria (5,9 %);
2. statham (3,9 %);
3. Panda (3,9 %);
4. boto (3,9 %);
5. Loser (3,9 %).

A continuación se muestra el desglose detallado del total de eventos que afectaron al sector específico objetivo:



2.b.vi. Acceso no autorizado

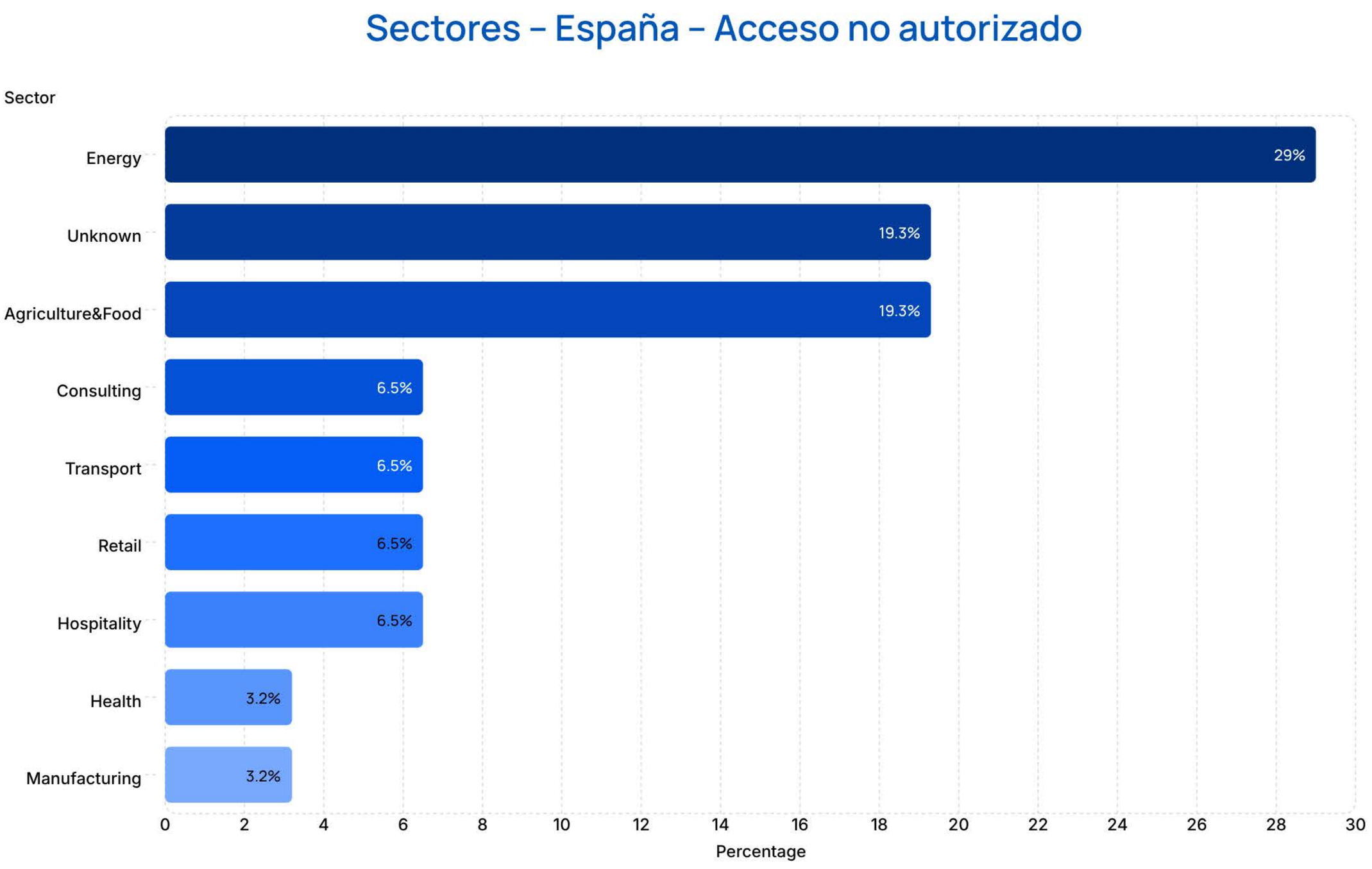
La amenaza de acceso no autorizado representó el 3,7 % del total de incidentes registrados en 2025 contra empresas, entidades y organizaciones en España. Esta amenaza afectó a nueve sectores diferentes. A continuación se muestra la lista de los cinco sectores específicos más afectados por la amenaza:

1. Energía/Servicios públicos (29,0 %);
2. Desconocido/No revelado (19,3 %);
3. Agricultura y producción alimentaria (19,3 %);
4. Consultoría (6,5 %);
5. Transporte/Logística (6,5 %).

A continuación se muestra la clasificación de los cinco principales actores maliciosos/canales clandestinos más activos en la categoría de amenazas de acceso no autorizado. Los porcentajes se calculan en función del número total de incidentes de acceso no autorizado atribuidos únicamente a esta categoría, incluida la entrada Desconocido/No revelado.

1. Z-PENTEST ALLIANCE (35,5 %);
2. Infrastructure Destruction Squad (16,2 %);
3. Noname057(16) (16,1 %);
4. Inteid (12,9 %);
5. Z-Alliance (6,5 %).

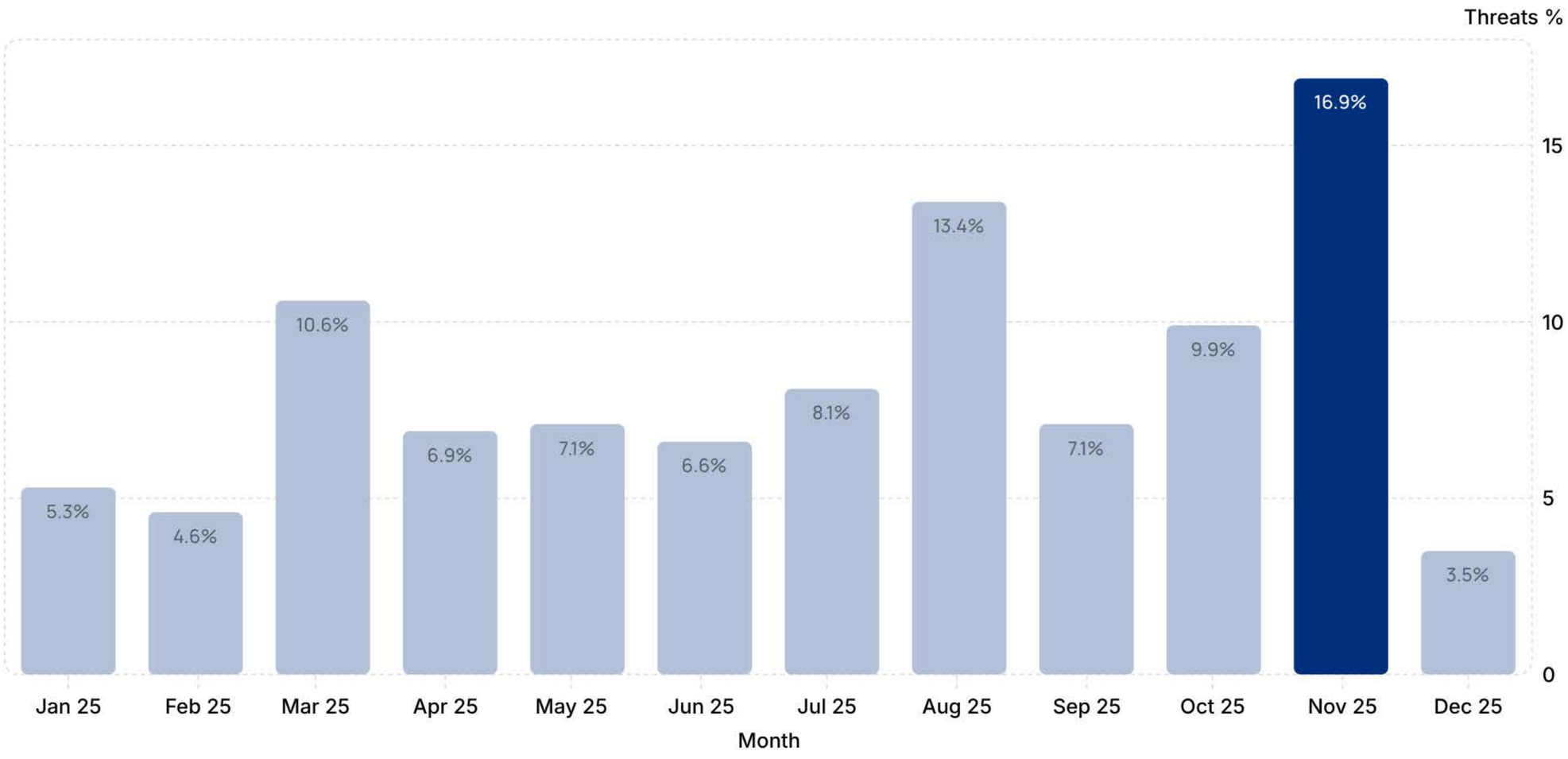
A continuación se muestra el desglose detallado del total de eventos que afectaron al sector específico objetivo:



2.c. Cronología

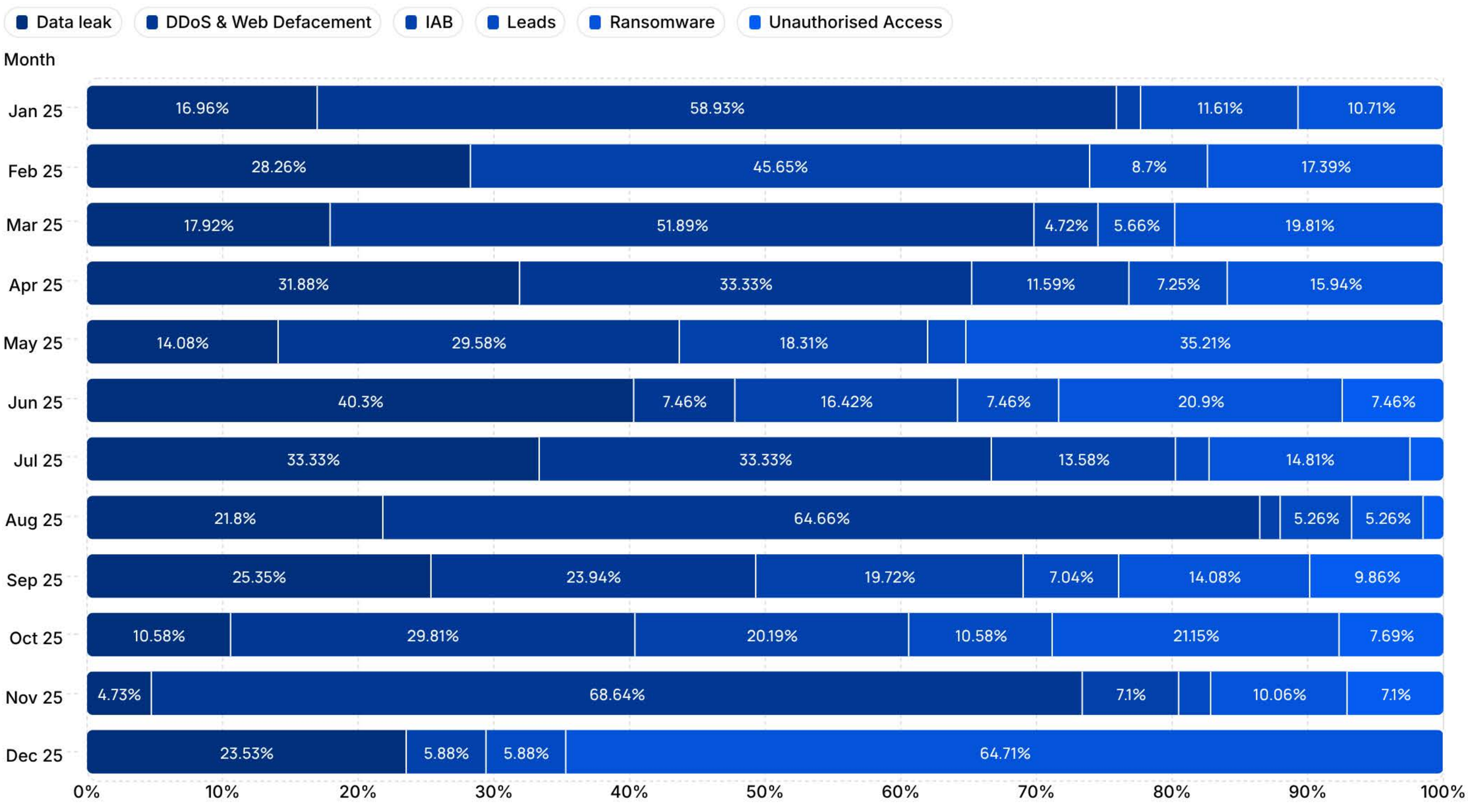
Teniendo en cuenta la cronología de las amenazas cibernéticas totales registradas en 2025 contra empresas y organizaciones en España, el equipo de YCTI observó una distribución relativamente uniforme a lo largo de la mayor parte de los meses del año, con un pico significativo en las amenazas registradas durante marzo (10,6 %) y agosto (13,4 %), y entre octubre (9,9 %) y noviembre (16,9 %) de 2025.

Todas las amenazas - Cronología mensual - España



A continuación, se muestra un gráfico que representa la distribución mensual por tipo de amenaza detectada por el equipo CTI durante 2025 contra empresas y organizaciones comunes en España.

Distribución mensual por tipo de amenaza - España



3. Ciberamenazas dirigidas a organizaciones españolas - 2025

A continuación se presentan cinco amenazas significativas registradas en el año de referencia (2025) dirigidas a organizaciones en España. Los eventos enumerados no representan la totalidad de los datos analizados por el equipo CTI, sino una muestra representativa de los eventos relevantes observados.

3.a. Datos de clientes de Iberia Airlines compartidos en la Dark Web

Fecha: 08/12/2025 | **Sector:** Transporte | **Amenaza:** Ransomware/Fuga de datos | **Ubicación geográfica:** España | **Autor de la amenaza:** Everest | **Fuente:** Dark Web

Evento: El equipo de Inteligencia sobre Amenazas Cibernéticas (CTI) recuperó de un foro clandestino un archivo de datos relacionado con una supuesta filtración de datos que afectaba a la aerolínea Iberia Airlines. Iberia es la aerolínea de bandera de España, fundada en 1927 y con sede en Madrid. Forma parte del Grupo Internacional de Aerolíneas (IAG) y es miembro de la alianza Oneworld, con una fuerte presencia especialmente en las rutas entre Europa y América Latina.

El archivo compartido en el foro clandestino consta de 7996 archivos que contienen un total de 1665 452 048 filas, con un tamaño total de aproximadamente 303 gigabytes. El contenido incluye información personal sobre los clientes de la aerolínea, con detalles sobre vuelos, reservas y facturaciones completadas, transacciones, suscripciones a boletines informativos y programas de fidelización (viajero frecuente).

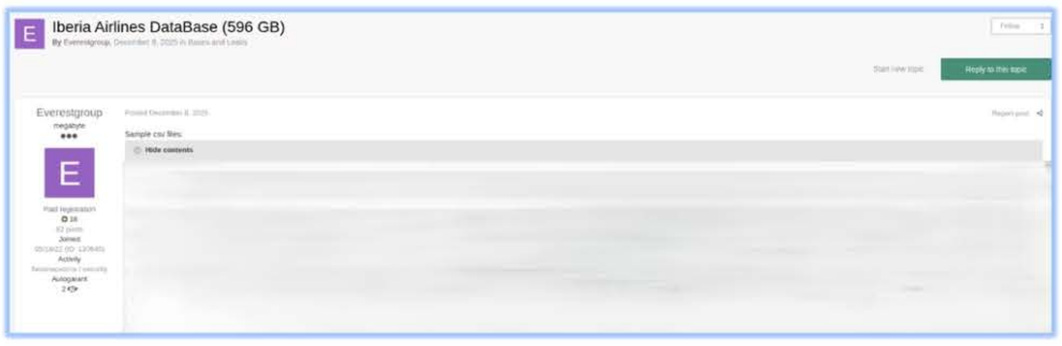
Según lo identificado en los archivos analizados, la información principal parece estar relacionada con datos personales como el nombre completo, la dirección de correo electrónico, el número de teléfono, la fecha de nacimiento, el estado civil, el puesto de trabajo y los detalles del programa de fidelización Iberia Plus.

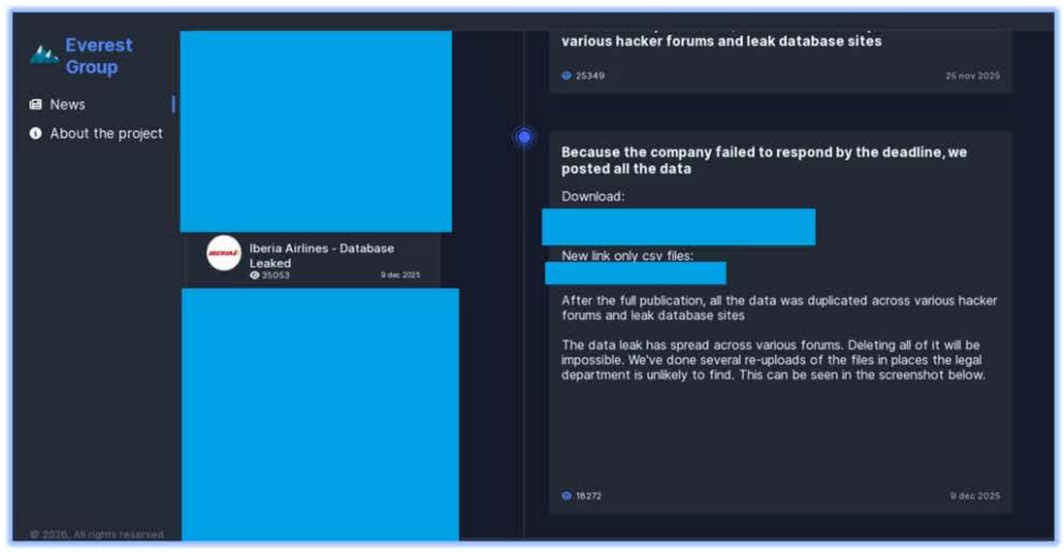
El archivo también contenía información relacionada con transacciones, con múltiples archivos que incluían datos confidenciales como el número parcial de la tarjeta de crédito, la fecha de caducidad, el banco emisor y el tipo de tarjeta.

Según se informa, la filtración fue publicada en el foro clandestino por el usuario «Everestgroup», que probablemente corresponda al grupo de ransomware Everest. De hecho, la empresa fue supuestamente atacada por el grupo de ransomware en noviembre de 2025 y, según fuentes OSINT, Iberia notificó a sus clientes que había detectado un incidente de seguridad relacionado con el acceso no autorizado a los sistemas de uno de sus proveedores, con la posible compromisión de ciertos datos personales (por ejemplo, nombre y apellidos, dirección de correo electrónico y número de identificación del programa de fidelización/Iberia Club), especificando que las credenciales de inicio de sesión de las cuentas no se vieron comprometidas y que las contraseñas no quedaron expuestas [1].

[1] BleepingComputer, *Iberia revela una filtración de datos de clientes tras una brecha de seguridad de un proveedor*, disponible aquí: **https://www.bleepingcomputer.com/news/security/iberia-discloses-customer-data-leak-after-vendor-security-breach/**, 23 de noviembre de 2025.

A continuación se presentan las pruebas relacionadas con la publicación en el foro clandestino, así como la publicación en el sitio web de filtración de datos del grupo de ransomware Everest:





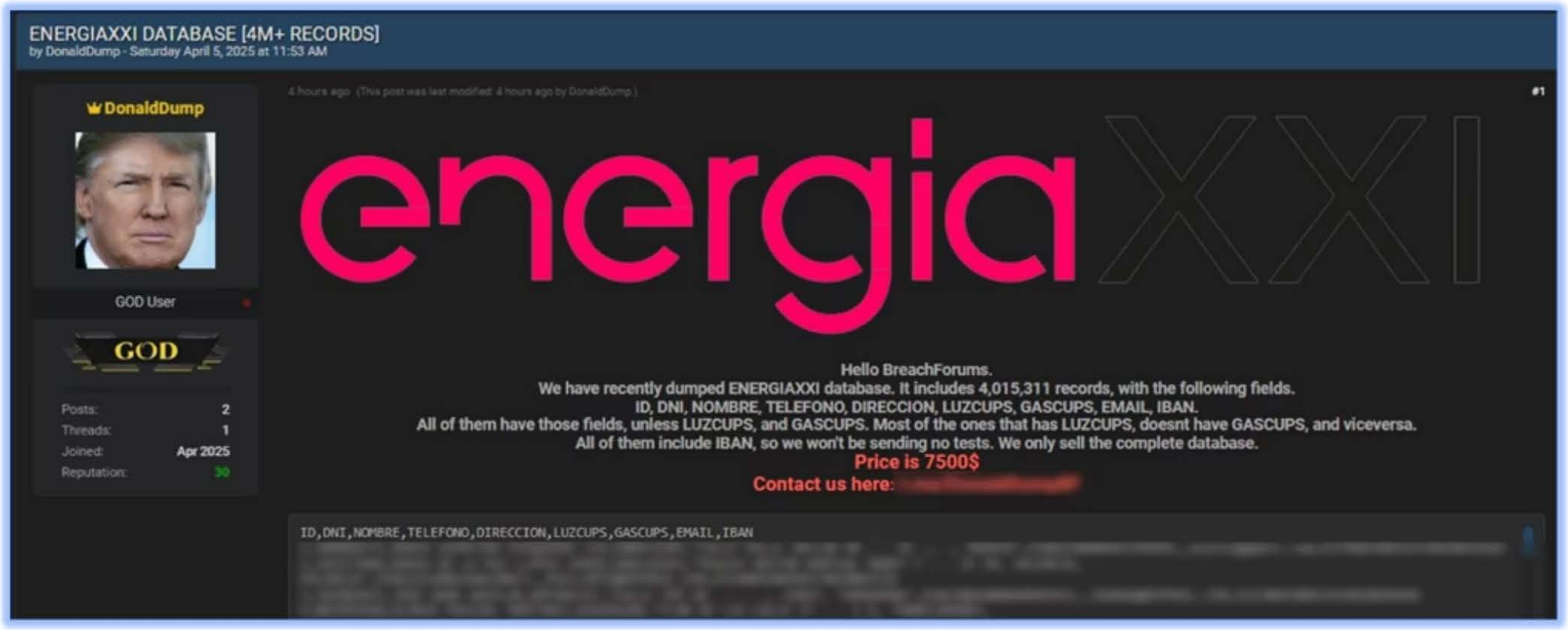
3.b. La base de datos EnergiAXXI supuestamente se puso a la venta en un foro clandestino

Fecha: 05/04/2025 I **Sector:** Energía y servicios públicos I **Amenaza:** Fuga de datos I **Ubicación geográfica:** España I **Autor de la amenaza:** DonaldDump I **Fuente:** Dark Web

Evento: El equipo CTI identificó una publicación en un conocido foro clandestino en la que un agente malicioso que utilizaba el nombre de usuario DonaldDump afirmaba estar vendiendo una base de datos de clientes de «ENERGIAXXI» que contenía más de 4 millones de registros. Según la publicación, el conjunto de datos incluye 4 015 311 entradas y contiene los siguientes campos: ID, DNI, nombre, número de teléfono, dirección, identificador de suministro eléctrico (LUZCUPS), identificador de suministro de gas (GASCUPS), dirección de correo electrónico e IBAN.

El actor malicioso afirmó que todos los registros incluyen un campo IBAN y, por este motivo, no proporcionaría pruebas ni muestras, alegando que la base de datos solo se vende como un paquete completo. La publicación anunciaba un precio de 7500 USD e incluía datos de contacto para negociar.

A continuación, la publicación identificada en un foro clandestino:



3.c. Fog ataca a la Real Academia Española (RAE)

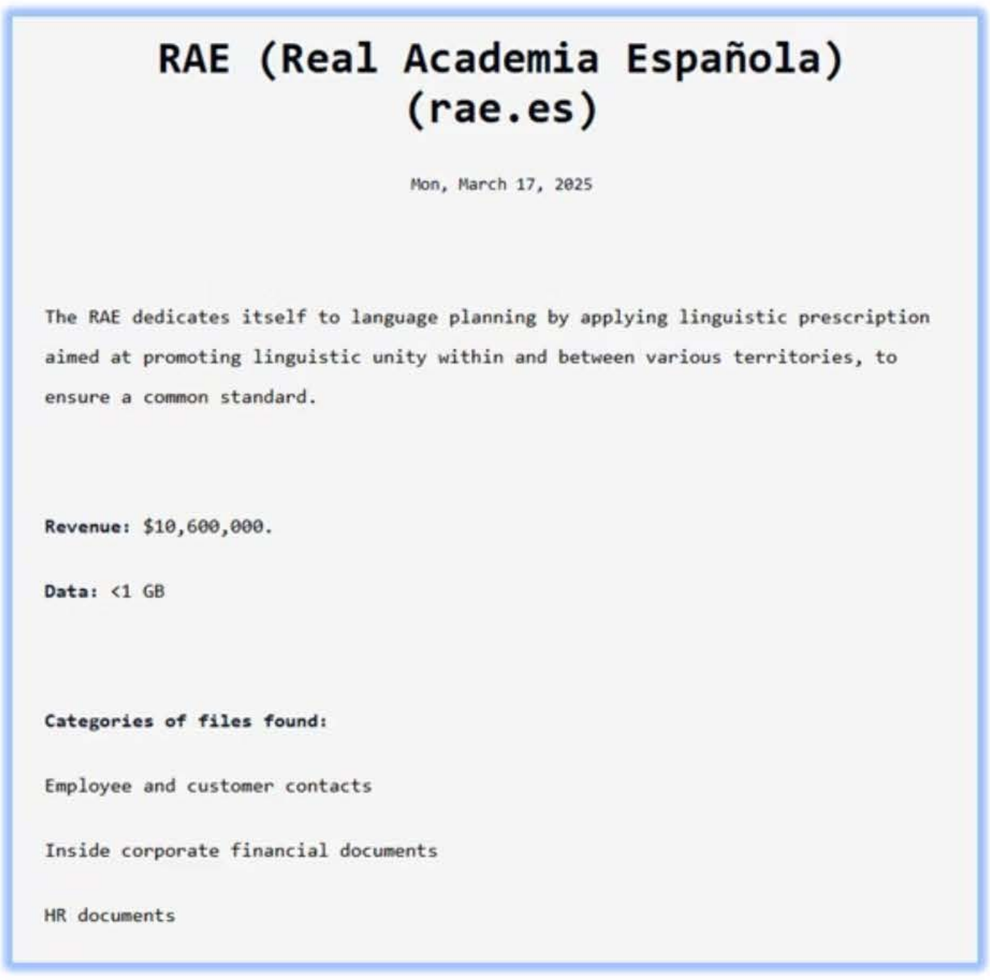
Fecha: 17/03/2025 I **Sector:** Educación I **Amenaza:** Ransomware I **Ubicación geográfica:** España I **Autor de la amenaza:** Fog I **Fuente:** Dark Web

Evento: El grupo de ransomware Fog anunció el ataque a la Real Academia Española (RAE), la institución responsable de la planificación lingüística y la promoción de la unidad lingüística española. La reivindicación se publicó en el sitio web de Fog dedicado a la filtración de datos el 17 de marzo de 2025 e incluía una breve descripción de la víctima y el supuesto volumen y tipo de datos sustraídos.

Según la entrada del sitio web de filtración, Fog afirmó haber obtenido menos de 1 GB de datos, incluidos contactos de empleados y clientes, documentos financieros internos de la empresa y documentación de recursos humanos. Tras la cobertura mediática, la RAE confirmó que su infraestructura informática sufrió un incidente de ciberseguridad la noche del sábado 1 de febrero y que se iniciaron inmediatamente actividades de contención y mitigación [2]. Las declaraciones públicas también indicaron que los recursos lingüísticos y los activos culturales de la RAE permanecían seguros y operativos [3].

Los informes de fuentes abiertas sugieren que, tras el caso de RAE, la actividad pública del grupo disminuyó en marzo de 2025, con pocas o ninguna nueva publicación de víctimas, lo que podría indicar una pausa operativa temporal o un cambio en la estrategia de comunicación [4].

A continuación se presentan las pruebas relacionadas con la publicación en el sitio web de filtración de datos del grupo de ransomware Fog:



RAE (Real Academia Española) (rae.es)

Mon, March 17, 2025

The RAE dedicates itself to language planning by applying linguistic prescription aimed at promoting linguistic unity within and between various territories, to ensure a common standard.

Revenue: $10,600,000.

Data: <1 GB

Categories of files found:

Employee and customer contacts

Inside corporate financial documents

HR documents

[2] Escudo Digital, *La RAE confirma haber sufrido un ataque de ransomware*, disponible aquí: https://www.escudodigital.com/ciberseguridad/rae-confirma-haber-sufrido-ataque-ransomware_62705_102.html, 18 de marzo de 2025.

[3] Servimedia, *La RAE confirma haber sufrido un ataque de ransomware,* disponible aquí: https://www.servimedia.es/noticias/rae-confirma-haber-sufrido-ataque-ransomware/1411519509, 18 de marzo de 2025.

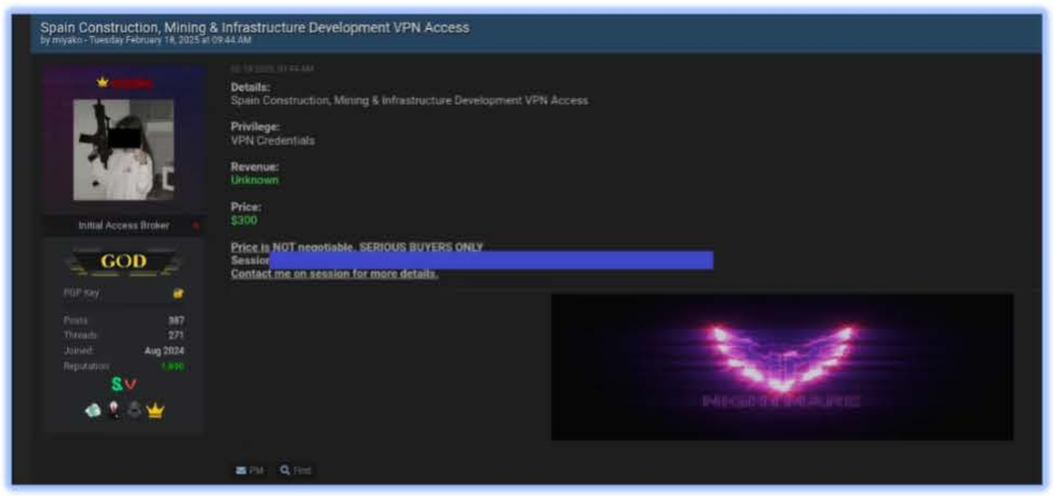
[4] Fog Ransomware Decryption and Recovery, *Fog Ransomware Goes Quiet in March 2025*, disponible aquí: - https://fogdecryptor.com/fog-ransomware-goes-quiet-in-march-2025/, 7 de mayo de 2025.

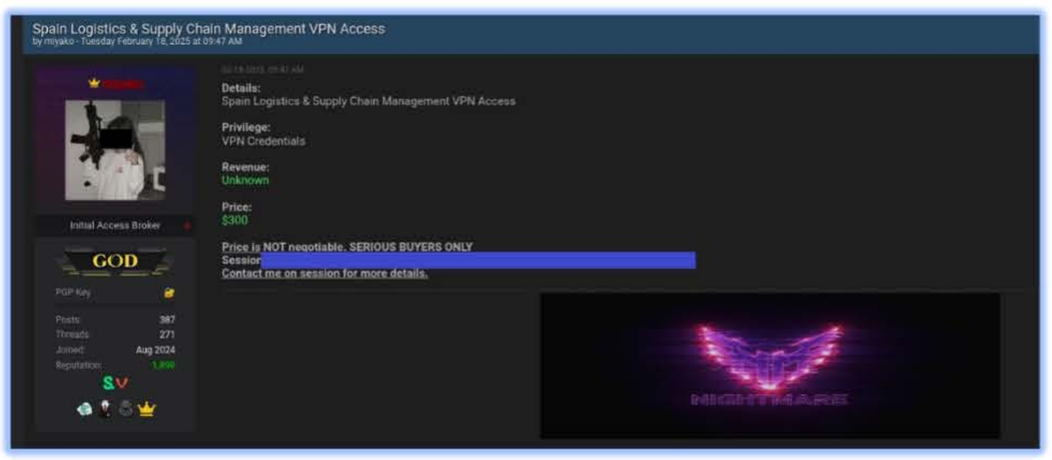
3.d. El agente de acceso inicial vende múltiples accesos españoles

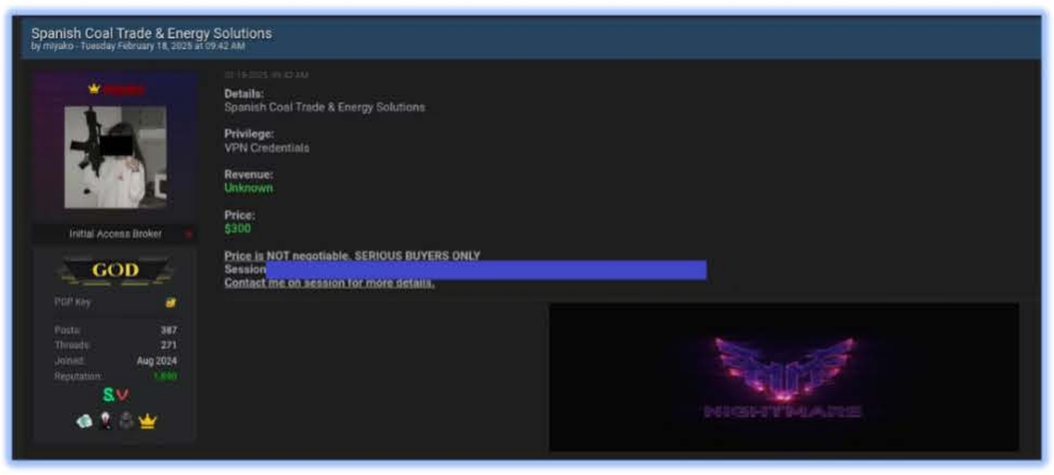
Fecha: 2025 | **Sector:** Multi | **Amenaza:** Intermediario de acceso inicial (IAB) | **Ubicación geográfica:** España | **Agente de la amenaza:** miyako | **Fuente:** Dark Web

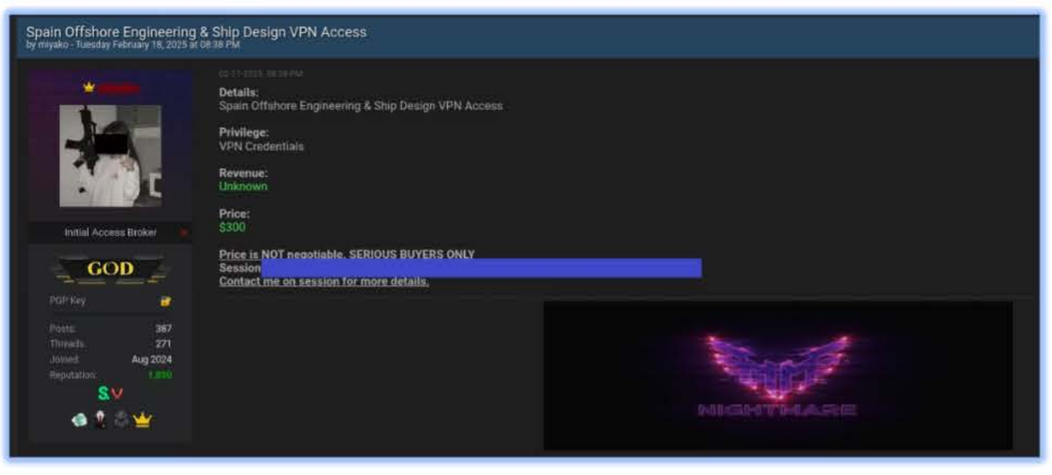
Evento: En un conocido foro clandestino, el Equipo de Inteligencia Cibernética, a través de actividades encubiertas, identificó a un agente malicioso conocido como *miyako* que vendía varios accesos iniciales relacionados con organizaciones españolas. Según las publicaciones, los accesos pertenecen a diferentes organizaciones y sectores, con precios que oscilan generalmente entre 200 y 500 dólares. Según investigaciones de inteligencia de código abierto, es probable que el intermediario de acceso inicial colabore habitualmente con uno o varios grupos de ransomware. No está claro si el agente malicioso forma parte de un grupo malicioso con motivaciones nacionales o si solo le mueven motivos económicos.

Ejemplos de publicaciones seleccionadas de *miyako* identificadas en un conocido foro clandestino:









3.e. Grupos hacktivistas atacan recursos españoles

Fecha: enero-diciembre de 2025 | **Sector:** múltiple | **Amenaza:** denegación de servicio distribuida (DDoS) | **Ubicación geográfica:** España | **Agente de la amenaza:** Grupos hacktivistas | **Fuente:** Dark Web

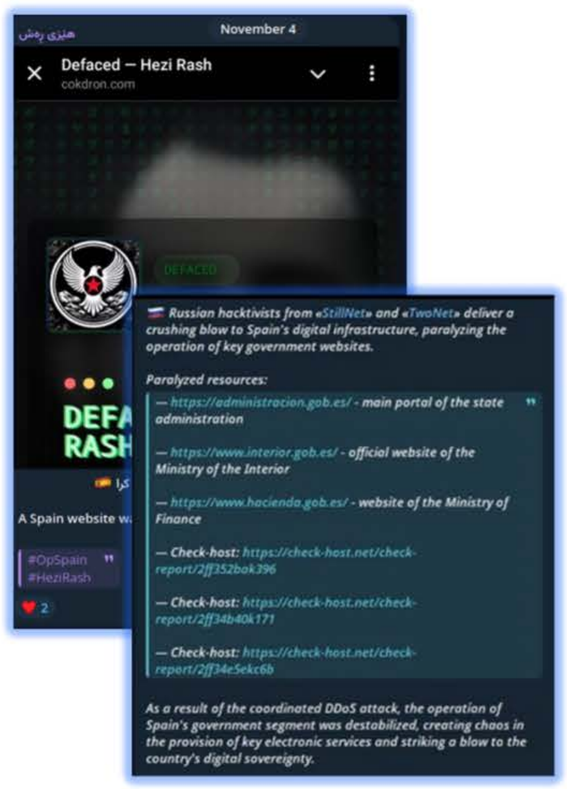
Evento: En 2025, el equipo CTI documentó múltiples operaciones de denegación de servicio distribuido (DDoS) y desfiguración web dirigidas contra organizaciones españolas, llevadas a cabo por diversos grupos hacktivistas con diferentes alineamientos ideológicos. Los grupos hacktivistas aprovecharon las amenazas cibernéticas no solo para generar perturbaciones, sino también como instrumentos de expresión política, justificando sus acciones mediante narrativas vinculadas tanto a los asuntos internos de España como a su posicionamiento en política exterior. Los actores alineados con Rusia, que representaban la mayor parte de la actividad observada, enmarcaron sistemáticamente sus operaciones como represalias vinculadas al apoyo de España a Ucrania y a su aparente alineamiento con las iniciativas de seguridad europeas y de la OTAN. En varios casos, las campañas parecían estar alineadas temporalmente con acontecimientos políticos de gran visibilidad, lo que sugiere que se utilizó el momento oportuno para maximizar el impacto simbólico y la resonancia mediática (en la sección 5 se ofrecen ejemplos de estas actividades que afectan a España: Resumen de las actividades hacktivistas contra organizaciones españolas - 2025).

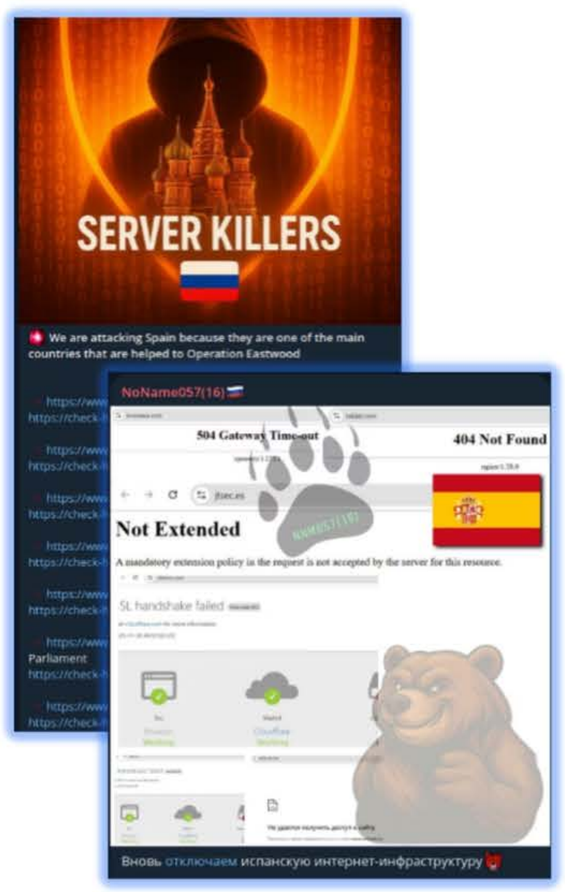
Además, la supervisión de la CTI indica que el volumen de amenazas aumentó durante los periodos asociados a las operaciones policiales contra los ecosistemas hacktivistas prorrusos. En concreto, la operación multinacional Eastwood contra NoName057(16) fue seguida de una renovada actividad a mediados de 2025, en consonancia con los mensajes de los actores maliciosos que presentaban la operación como un desencadenante de represalias y movilización. Más adelante en el año, se produjeron nuevos picos de actividad en consonancia con acontecimientos de gran repercusión en el ámbito nacional, como la exposición pública de personas vinculadas a la amplificación de narrativas hacktivistas prorrusas, lo que contribuyó a que las instituciones gubernamentales españolas volvieran a ser objeto de ataques.

Junto a la actividad alineada con Rusia, los informes de CTI identificaron un segundo grupo de actores que mostraban mensajes alineados con Marruecos o más amplios a favor de los árabes y los musulmanes. Sin embargo, a diferencia de los patrones observados en otros países, estos colectivos no utilizaron predominantemente el conflicto entre Hamás e Israel como justificación para sus operaciones contra España, lo que podría reflejar el posicionamiento interno y la postura de la política pública de España durante 2025.

En general, la diversidad de motivaciones y alineamientos pone de relieve el creciente uso de las operaciones DDoS y de desfiguración como herramientas de influencia, señalización y amplificación narrativa, lo que ilustra la creciente intersección entre las operaciones cibernéticas y la dinámica geopolítica que afecta a España.

Pruebas de los canales de Telegram de los grupos hacktivistas:





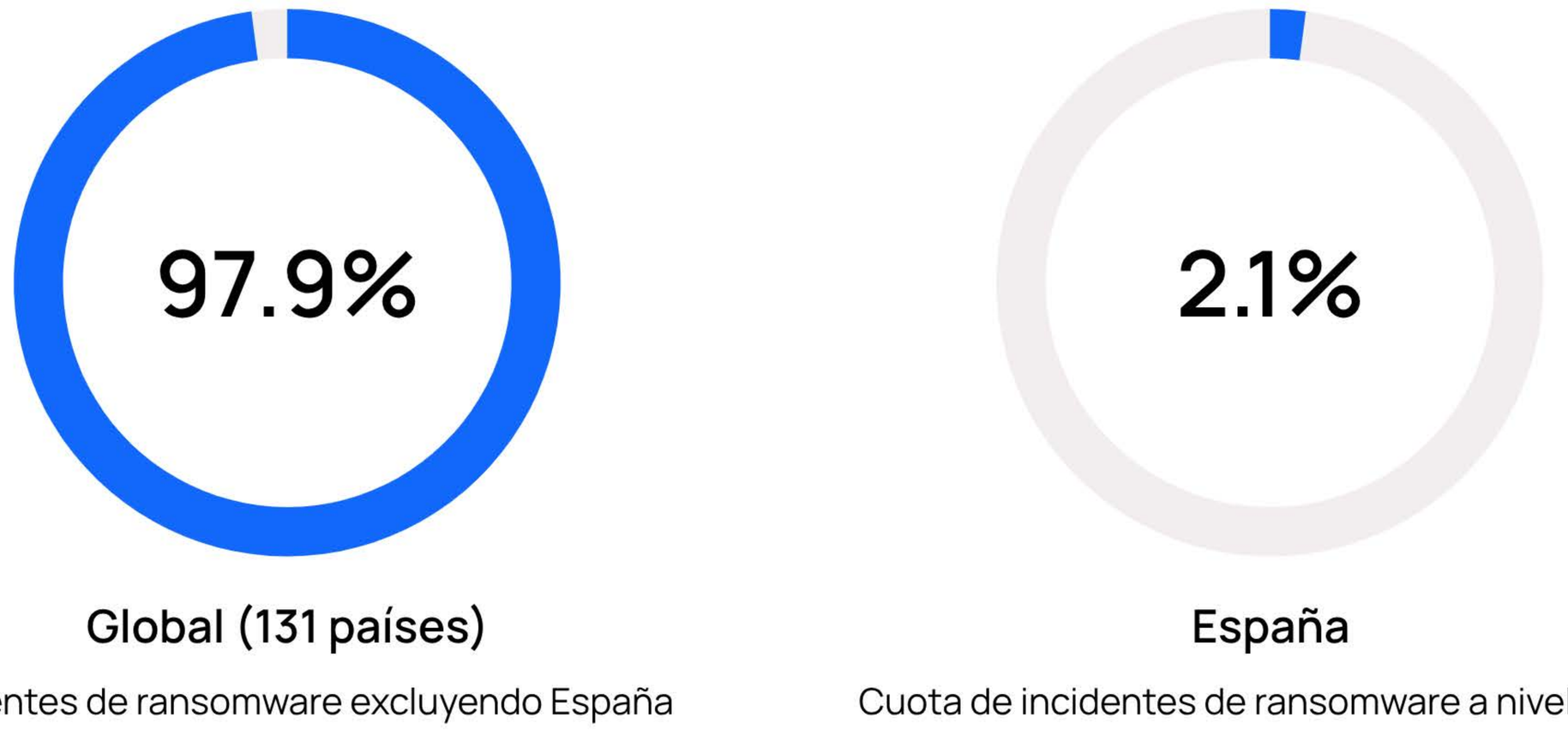
4. Análisis en profundidad de las amenazas de ransomware en España - 2025

En esta sección, el equipo de Yarix Cyber Threat Intelligence (YCTI) ofrece un análisis en profundidad de los incidentes de ransomware que afectaron a entidades en España durante 2025, con el objetivo de aumentar la concienciación sobre el panorama actual de amenazas.

Nota: Los datos recopilados y validados por el equipo YCTI proceden de los sitios web de filtración de datos de los grupos de ransomware monitorizados y se refieren a las reivindicaciones públicas realizadas por los autores de las amenazas (TA).

A nivel mundial, los incidentes reivindicados contra organizaciones en España representan el 2,10 % del total de incidentes de ransomware registrados por el equipo YCTI. En total, se identificaron 132 países en los que empresas y organizaciones se vieron afectadas por incidentes de ransomware durante 2025.

Ratio de incidentes totales de ransomware (global) frente a incidentes de ransomware en España



Global (131 países)

Incidentes de ransomware excluyendo España

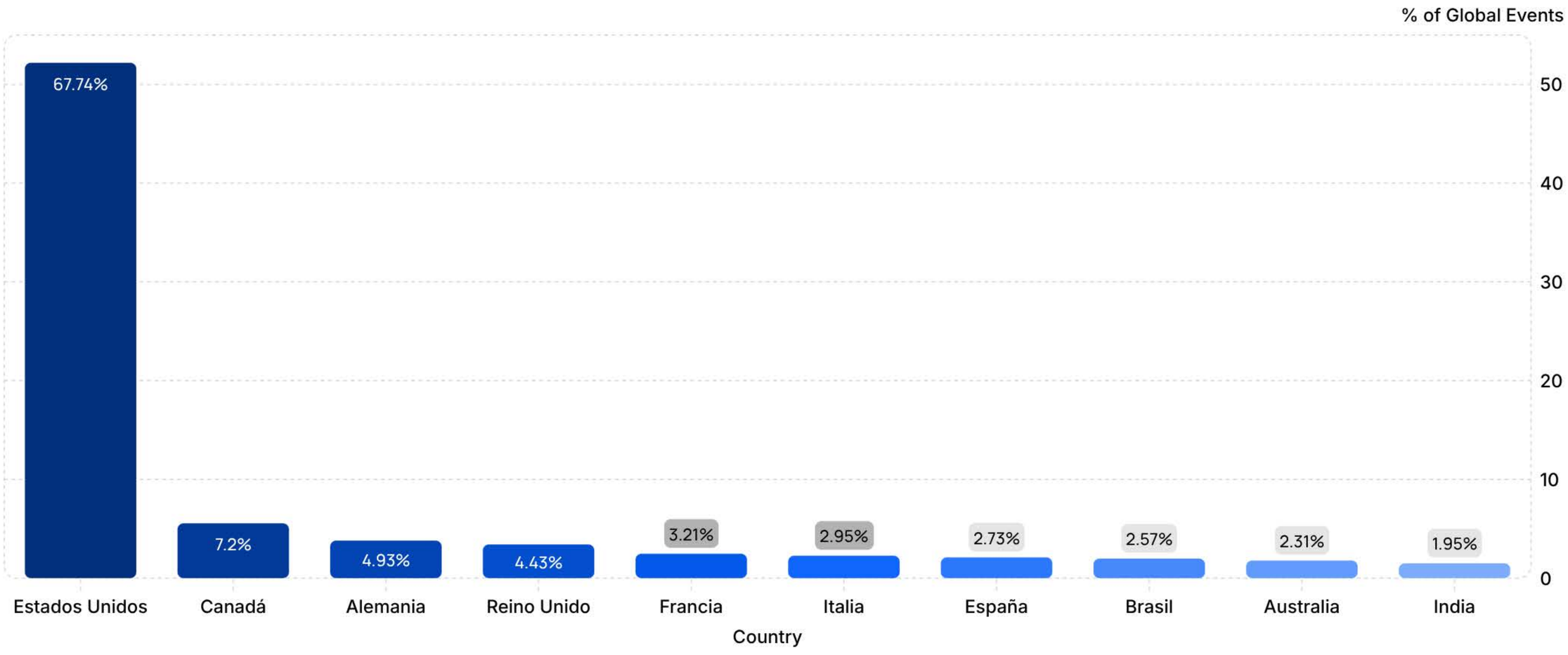
España

Cuota de incidentes de ransomware a nivel global

A modo de comparación, se proporciona la clasificación de los 10 países más afectados por incidentes de ransomware en 2025.

1. Estados Unidos: 52,19 %
2. Canadá: 5,55 %
3. Alemania: 3,80 %
4. Reino Unido: 3,41 %
5. Francia: 2,47 %
6. Italia – 2,27 %
7. España – 2,10 %
8. Brasil – 1,98 %
9. Australia – 1,78 %
10. India: 1,50 %

Top 10 Países - Reclamaciones de Ransomware - Global

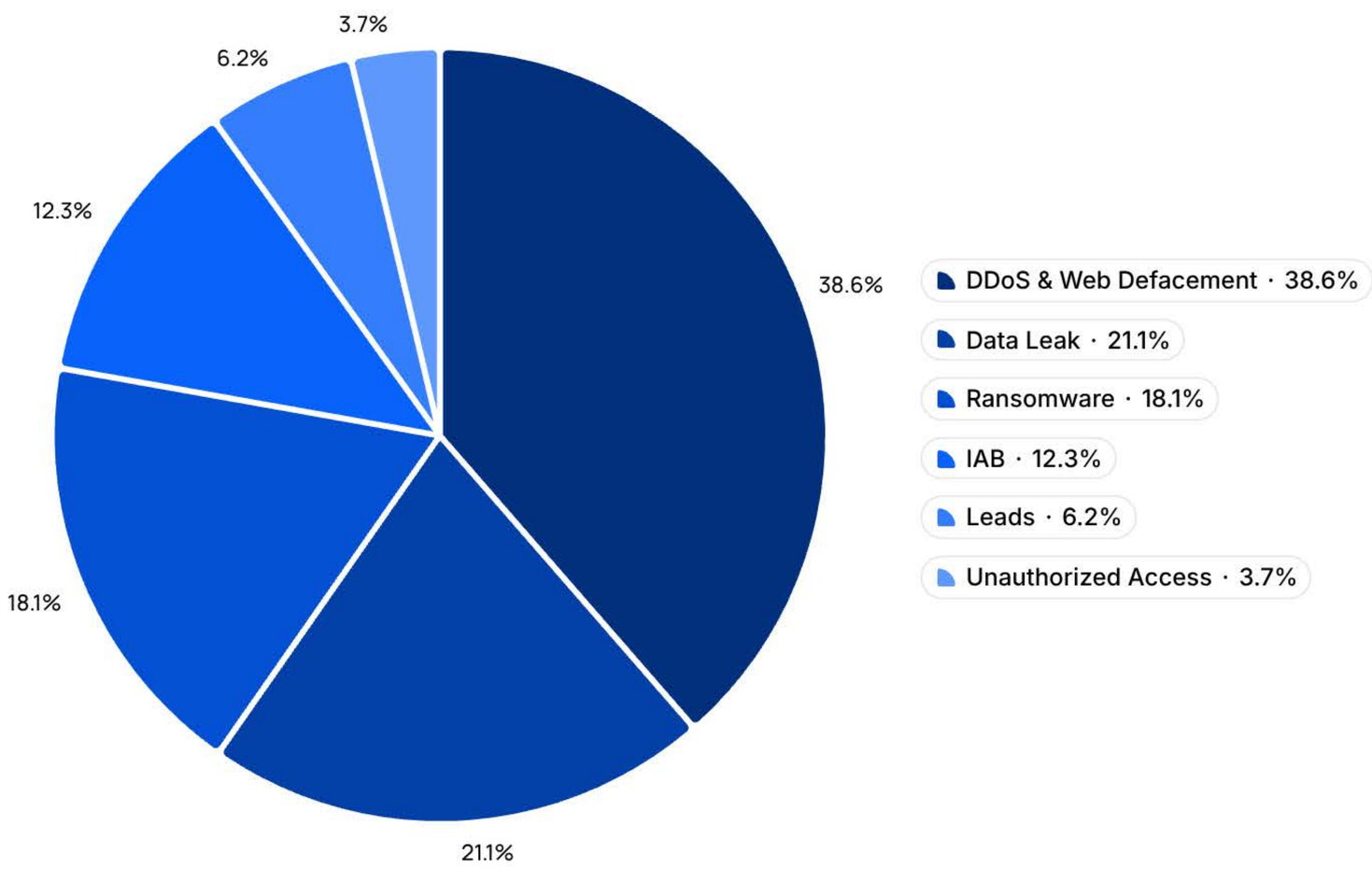


En general, los países incluidos en el ranking de los 10 primeros puestos por número de incidentes de ransomware denunciados durante 2025 representaron el 77,05 % del total de incidentes.

España se encuentra entre los 10 países con mayor número de organizaciones afectadas por ransomware.

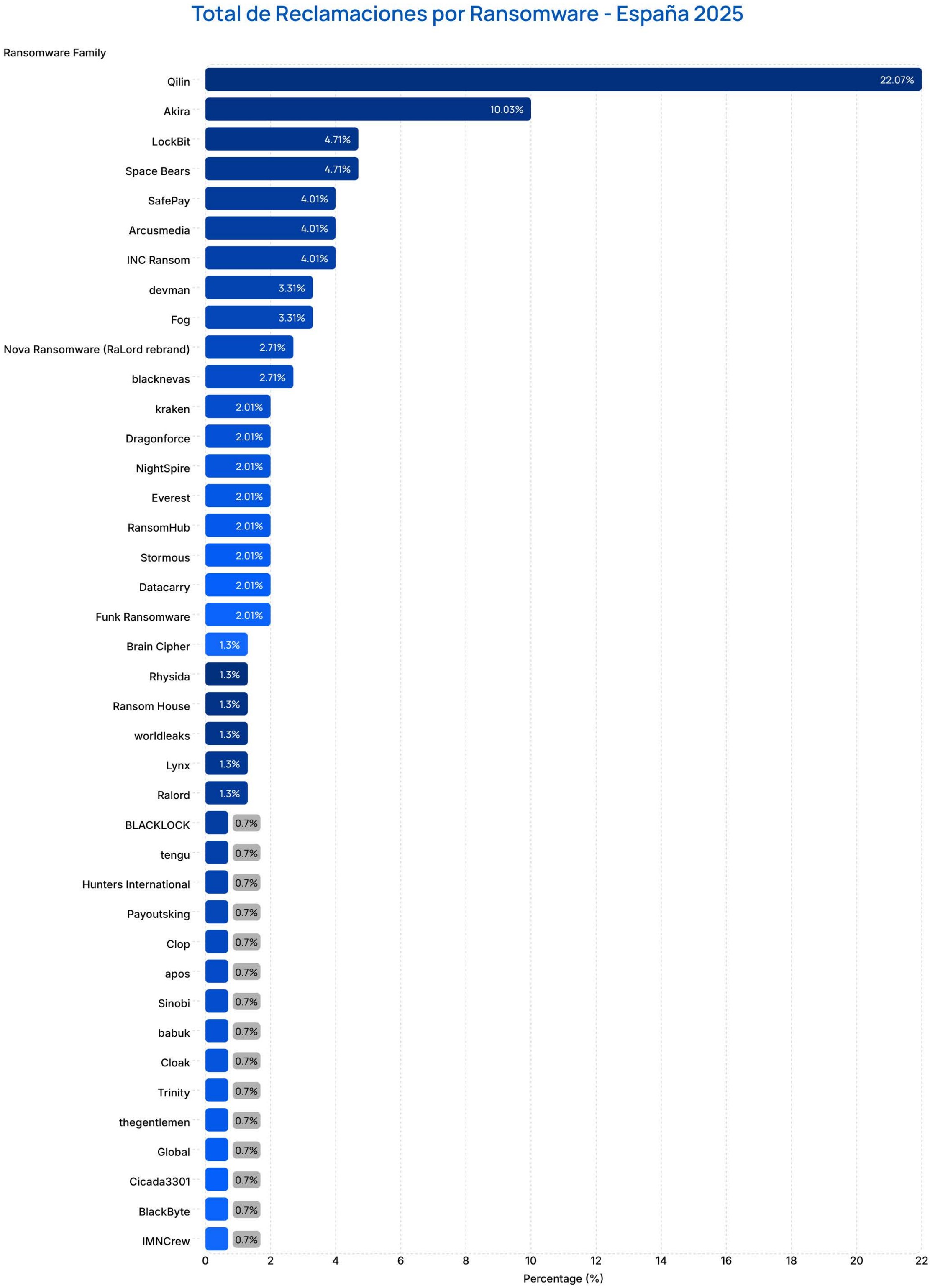
Los incidentes de ransomware representaron el 18,1 % del total de ciberamenazas contra entidades ubicadas en España, según detectó la telemetría del equipo de Inteligencia de Ciberamenazas durante 2025.

Todas las amenazas España 2025



Durante el periodo de referencia, el equipo de Inteligencia de Ciberamenazas de Yarix detectó 40 grupos de ransomware que tuvieron como objetivo entidades en España durante 2025.

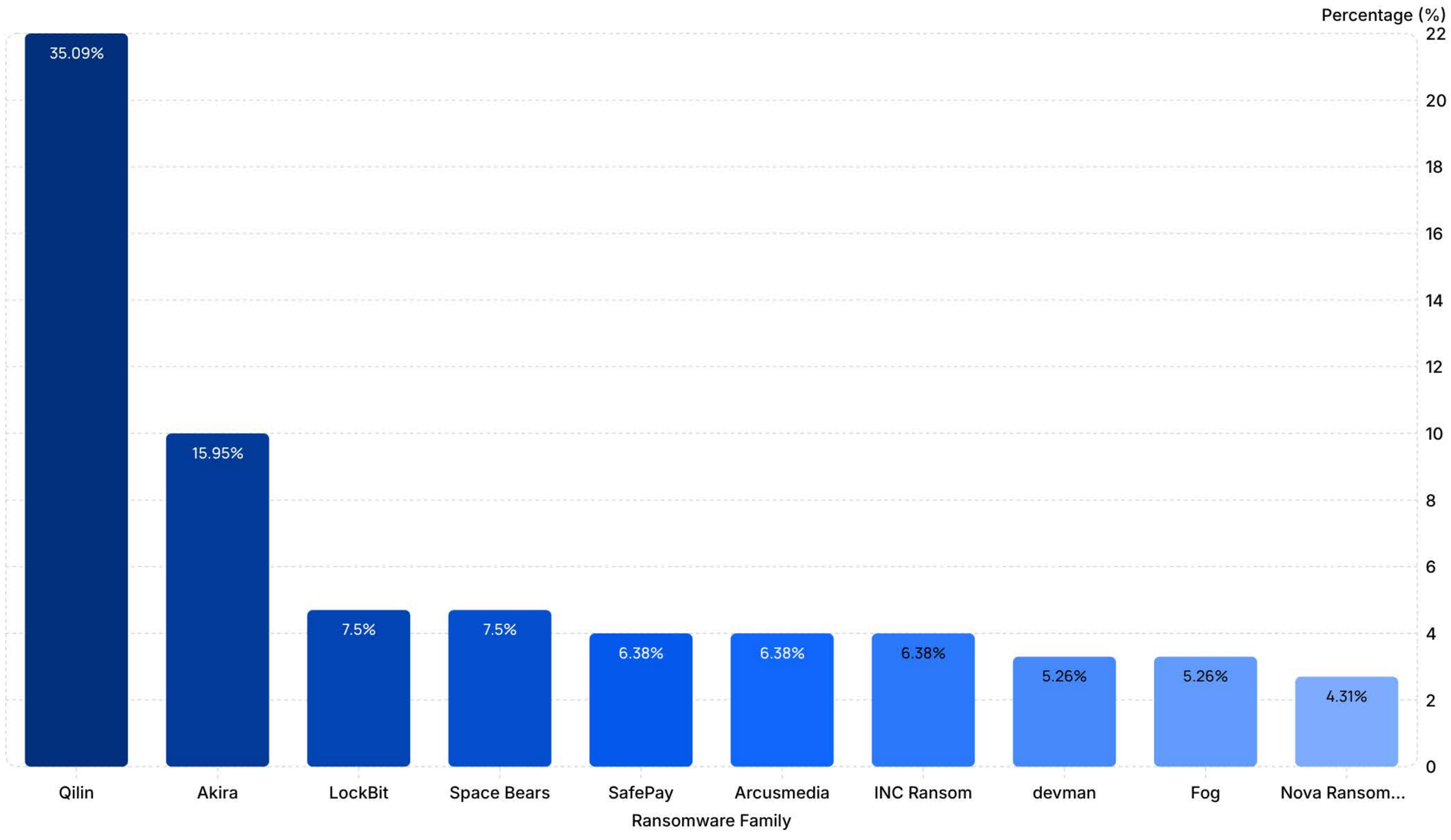
A continuación se muestra una representación del porcentaje de incidentes de ransomware perpetrados contra entidades y organizaciones en España por cada una de las 40 bandas de ransomware observadas.



Según los análisis realizados, las 10 familias de ransomware más importantes por número de reclamaciones contra empresas y organizaciones en España durante 2025 son las siguientes:

1. Qilin, (22,0 %)
2. Akira, (10,0 %)
3. LockBit, (4,7 %)
4. Space Bears, (4,7 %)
5. SafePay, (4,0 %)
6. Arcusmedia, (4,0 %)
7. INC Ransom, (4,0 %)
8. devman, (3,3 %)
9. Fog, (3,3 %)
10. Nova Ransomware (RaLord rebrand), (2,7 %); blacknevas (2,7 %).

En general, los grupos de ransomware incluidos en el ranking de los 10 principales representaron el 62,7 % del total de incidentes contra empresas y organizaciones en España.



Cronograma mensual del Ransomware - España 2025

A continuación se muestra la tendencia mensual de los eventos registrados entre enero y diciembre de 2025.

Los gráficos muestran cuatro picos en los incidentes de ransomware registrados en marzo (11,3 %), mayo (14,0 %), octubre (12,0 %) y diciembre (12,0 %) de 2025.

En cuanto a la tendencia de las reclamaciones de grupos específicos de ransomware, a continuación se muestra un gráfico que describe las cifras mensuales de incidentes reclamados por las 10 principales familias de ransomware que atacan a entidades y organizaciones en España.

Cronograma mensual de eventos de Ransomware - España

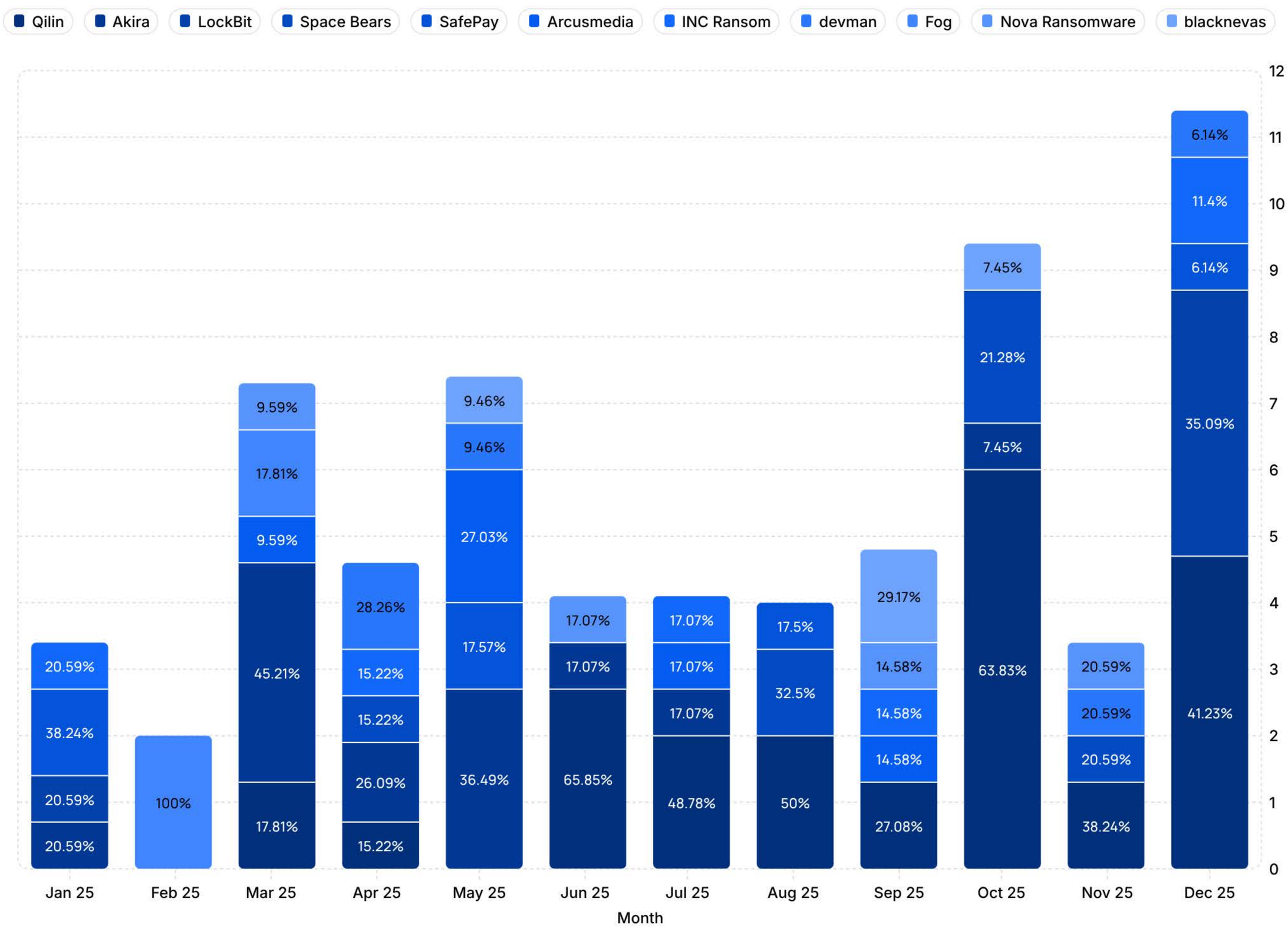
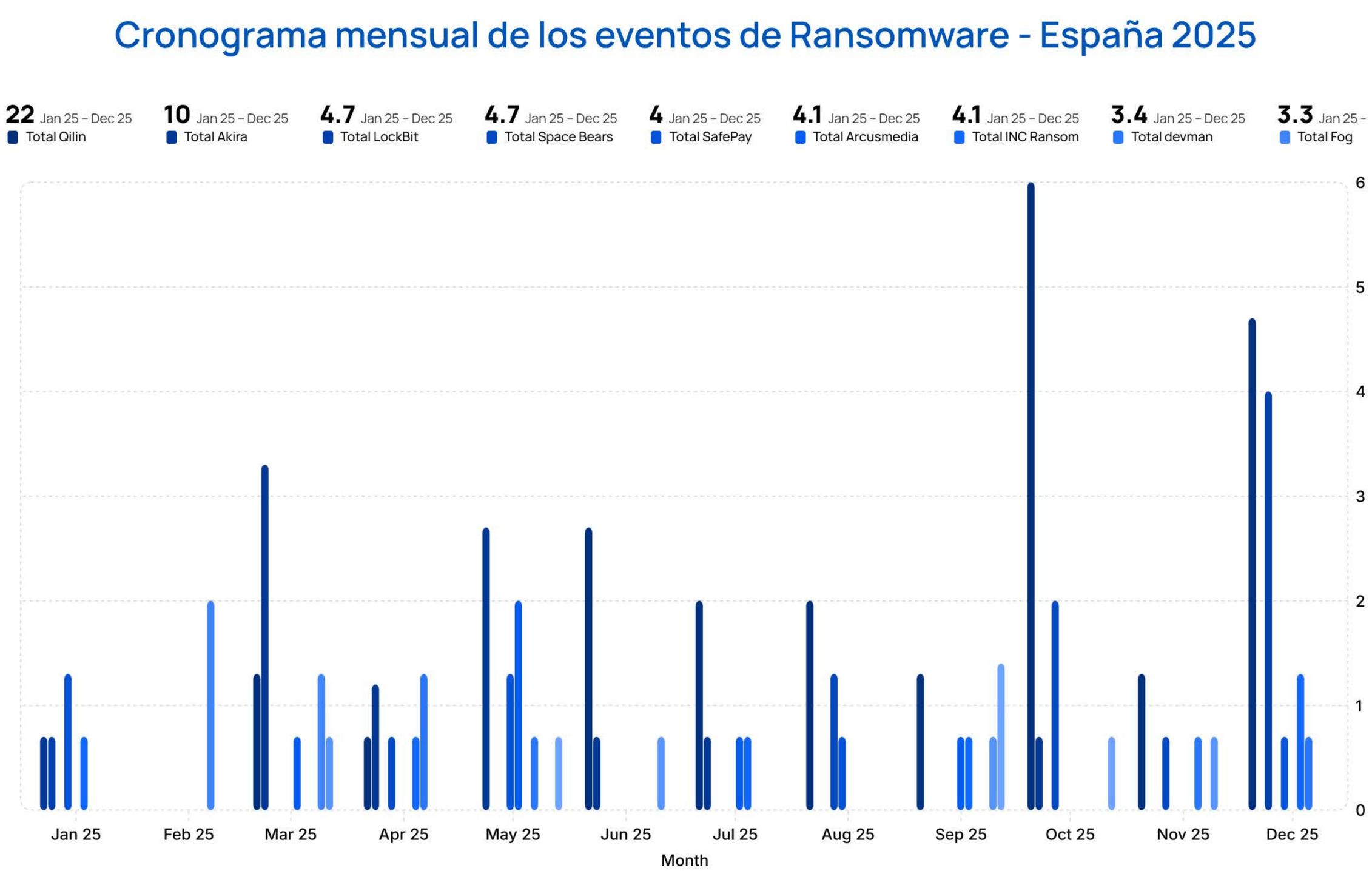


Gráfico alternativo que describe la tendencia mensual de las 10 principales familias de ransomware registradas durante 2025.



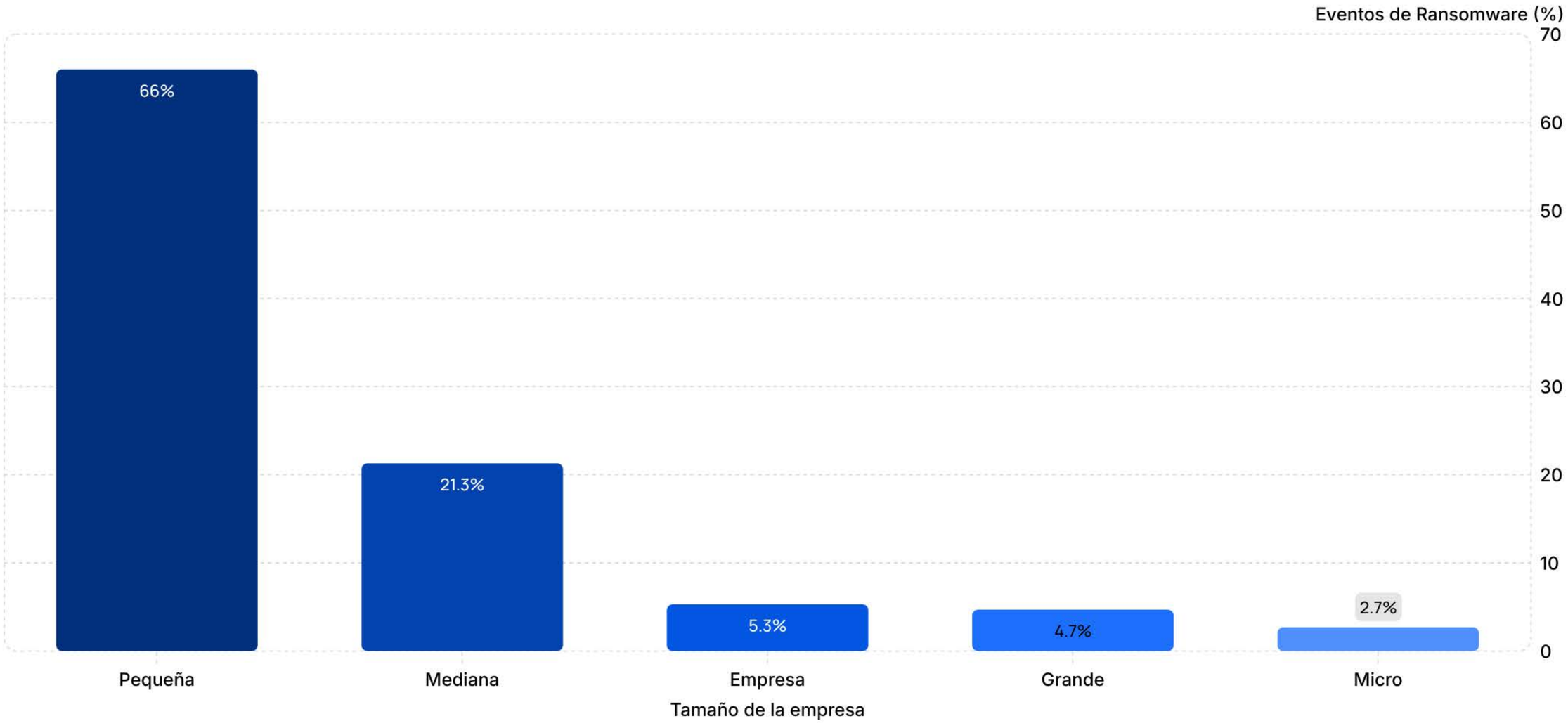
Durante el proceso de validación de los eventos de ransomware, el equipo YCTI clasificó los datos individuales según el tamaño de la empresa, en función del número de empleados dentro de la organización.

Para esta categorización se aplicó el siguiente esquema de clasificación:

Tamaño de la empresa	Número de empleados
Micro	De 1 a 10 empleados
Pequeña	De 11 a 100 empleados
Mediana	De 101 a 500 empleados
Grande	De 501 a 1000 empleados
Empresa	Más de 1.001 empleados

A continuación se muestran los datos relacionados con los incidentes de ransomware que afectan a entidades españolas, teniendo en cuenta el tamaño de las organizaciones:

Porcentaje total de reclamaciones por ransomware - Tamaño de la empresa - España 2025

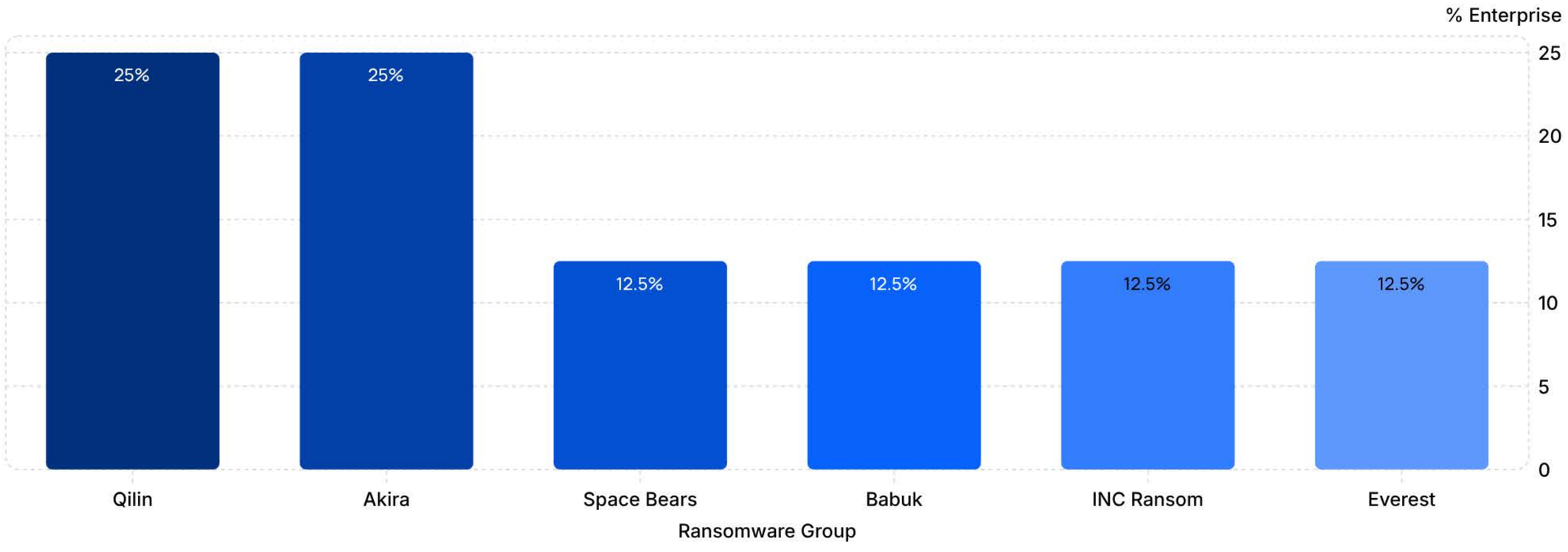


4.a. Grupos de ransomware: Sector "Empresa"

En 2025, se identificaron 6 familias de ransomware que atacaron a organizaciones «Empresa» (1001+ empleados). Los eventos registrados representan el 5,3 % del total de eventos.

En la siguiente tabla, los porcentajes representan la participación de cada grupo de ransomware sobre el total de eventos dirigidos a organizaciones dentro de la misma categoría de tamaño de empresa.

Tamaño de las organizaciones - Reclamaciones de ransomware de Empresas - España



El gráfico anterior ilustra la distribución de los grupos de ransomware que atacan a organizaciones Empresa, mientras que la tabla siguiente compara esta distribución con su participación global en el total de incidentes de ransomware registrados en España.

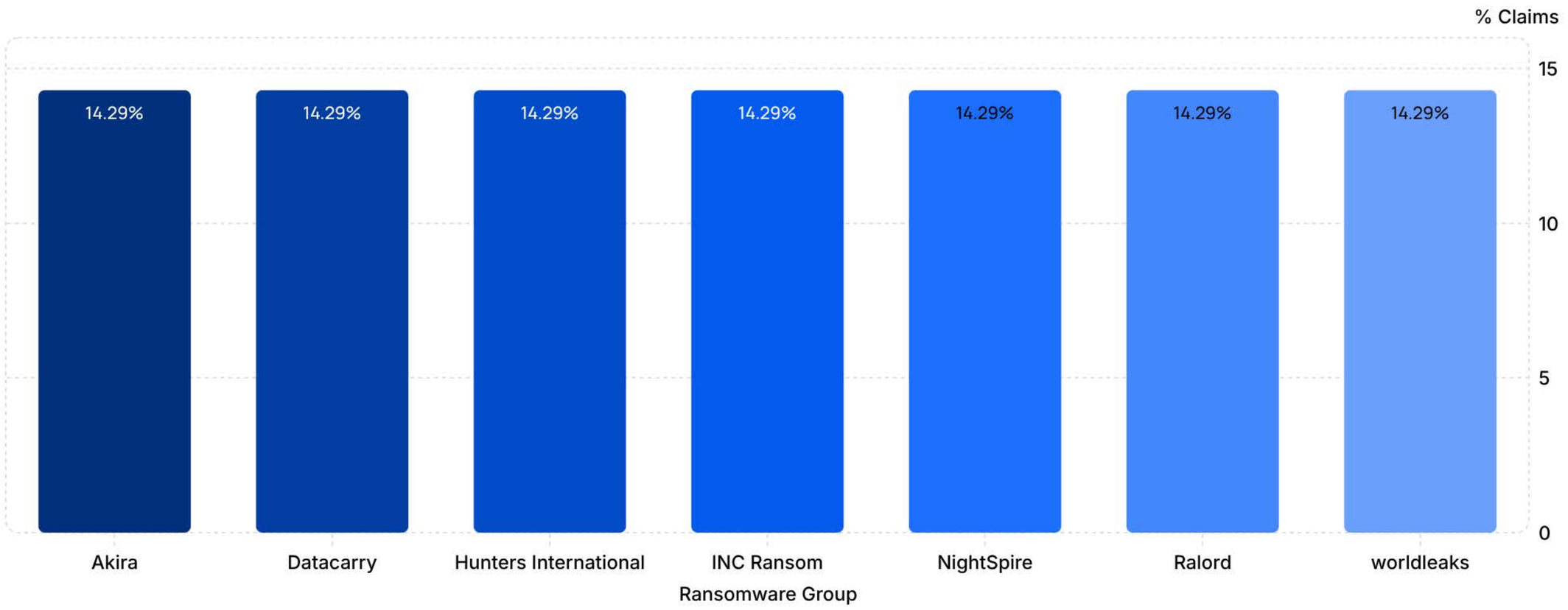
ID	Grupos de Ransomware	% Empresa	% Eventos Totales - España
1	Qilin	25,0%	22,0%
2	Akira	25,0%	10,0%
3	Space Bears	12,5%	4,7%
4	Babuk	12,5%	0,7 %
5	INC Ransom	12,5%	4,0%
6	Everest	12,5%	2%
TOT	**6 Grupos**	**100%**	**43,3%**

4.b. Grupos de ransomware: Sector «Grande»

En 2025, se identificaron siete familias de ransomware que tenían como objetivo organizaciones «grandes» (501-1000 empleados). Los incidentes registrados representan el 4,7 % del total de reclamaciones.

En la siguiente tabla, los porcentajes representan la cuota de cada grupo de ransomware en el total de reclamaciones dirigidas a organizaciones dentro de la misma categoría de tamaño de empresa.

Tamaño de la organización - Gran Empresa Reclamaciones de Ransomware España 2025



El gráfico anterior ilustra la distribución de los grupos de ransomware que atacan a grandes organizaciones, mientras que la tabla siguiente compara esta distribución con su cuota global del total de incidentes de ransomware registrados en España.

ID	Grupos de Ransomware	% Gran Empresa	% Eventos totales
1.	Akira	14,3%	10,0%
2.	Datacarry	14,3%	2,0%
3.	Hunters International	14,3%	0,7%
4.	INC Ransom	14,3%	4,0%
5.	NightSpire	14,3%	2,0%
6.	Ralord	14,3%	1,3%
7.	worldleaks	14,3%	1,3%
TOT	**7 Grupos**	**100%***	**21,3%**

**Note: Los porcentajes pueden no sumar exactamente el 100 % debido al redondeo.*

4.c. Grupos de ransomware: Sector «Mediano»

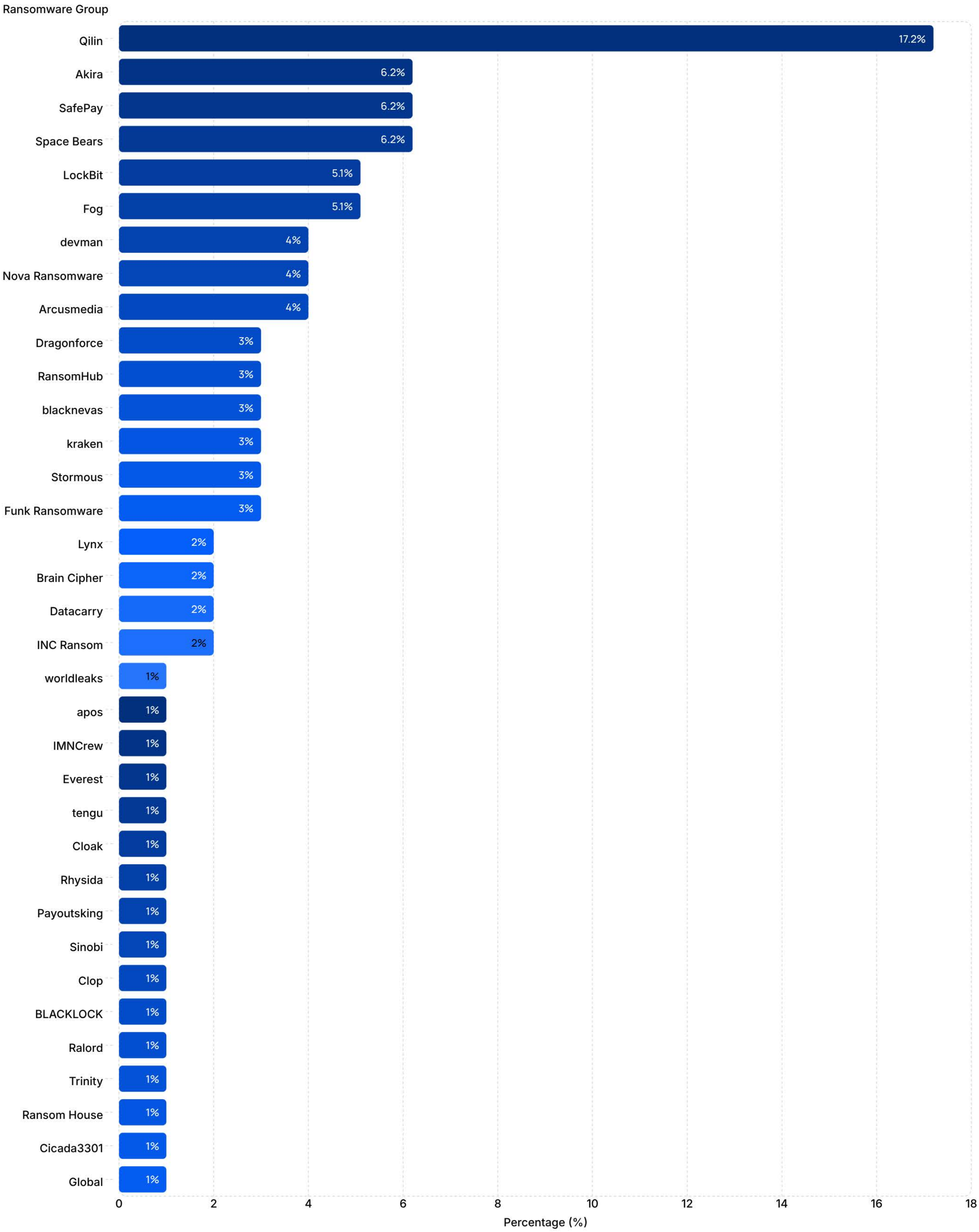
En 2025, se identificaron 13 familias de ransomware que tenían como objetivo a empresas «medianas» (101-500 empleados). Los incidentes registrados representan el 21,3 % del total de reclamaciones.

En el siguiente gráfico, los porcentajes representan la cuota de cada grupo de ransomware en el total de reclamaciones dirigidas a organizaciones dentro de la misma categoría de tamaño de empresa.

4.d. Incidentes de ransomware: Sector «Pequeño»

En 2025, se identificaron 35 familias de ransomware que tenían como objetivo a empresas «pequeñas» (11-100 empleados). Los incidentes registrados representan el 66,0 % del total.

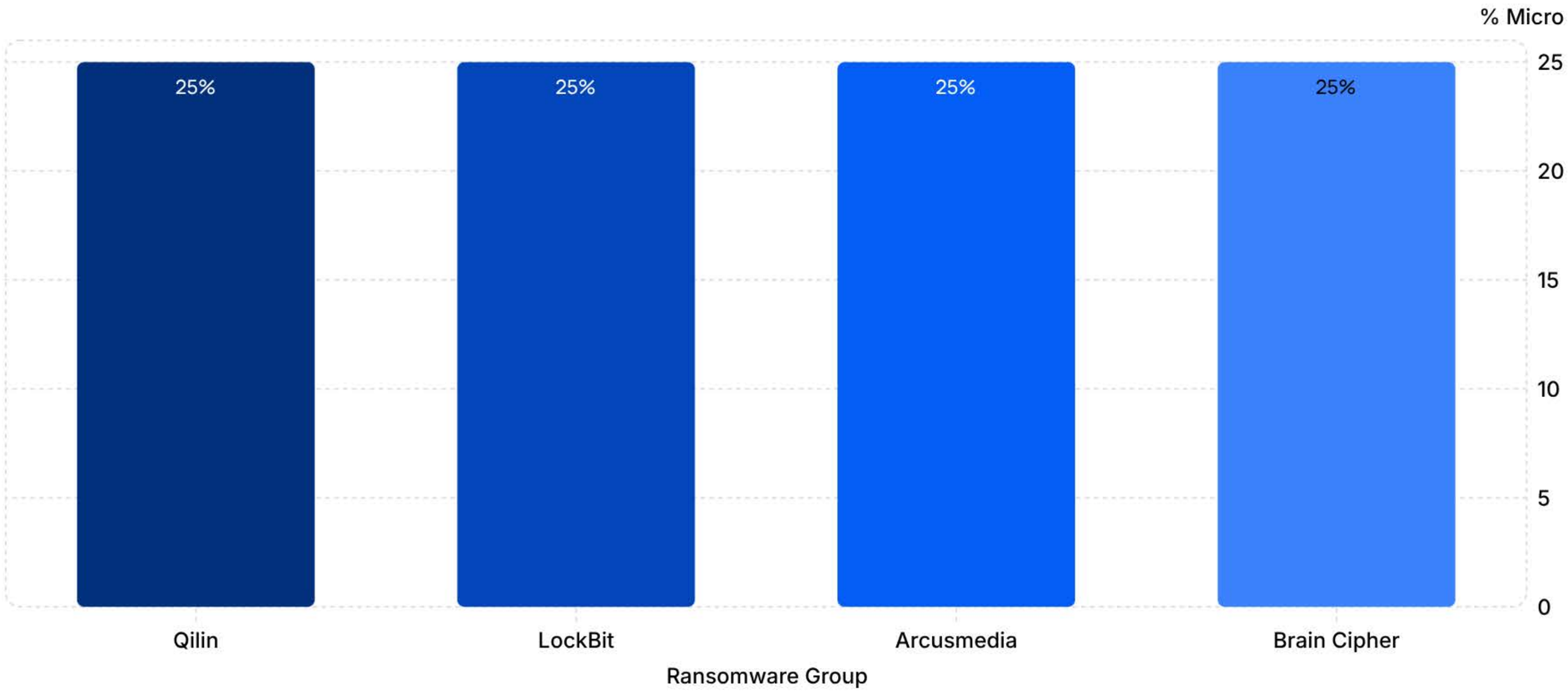
En el siguiente gráfico, los porcentajes representan la proporción de cada grupo de ransomware en el total de reclamaciones dirigidas a organizaciones dentro de la misma categoría de tamaño de empresa.



4.e. Eventos de ransomware: Sector «Micro»

En 2025, se identificaron cuatro familias de ransomware que tenían como objetivo a empresas «micro» (de 1 a 10 empleados). Los eventos registrados representan el 2,7 % del total.

En la siguiente tabla, los porcentajes representan la proporción de cada grupo de ransomware en el total de reclamaciones dirigidas a organizaciones dentro de la misma categoría de tamaño de empresa.



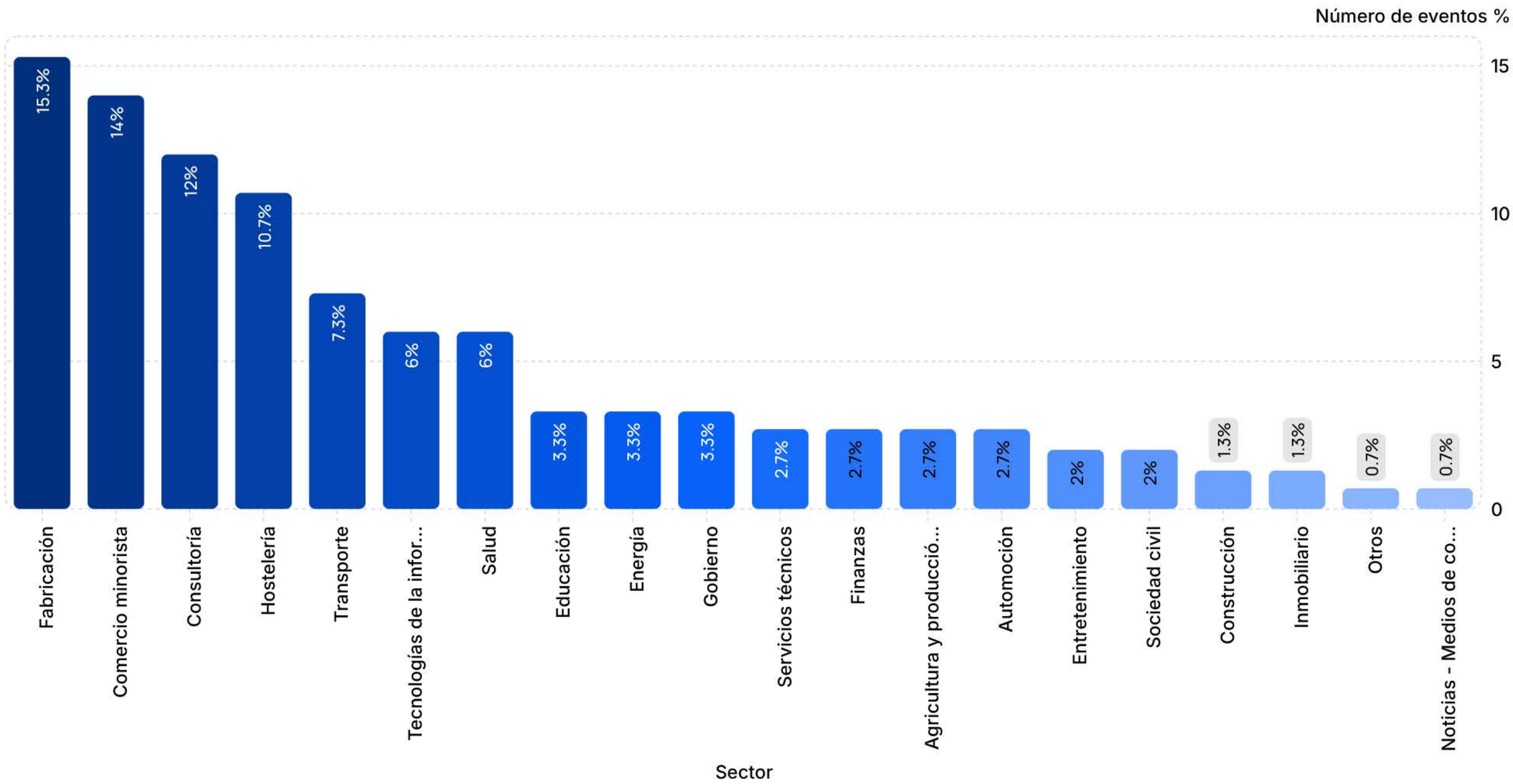
El gráfico anterior ilustra la distribución de los grupos de ransomware que atacan a pequeñas organizaciones, mientras que la tabla siguiente compara esta distribución con su cuota global del total de incidentes de ransomware registrados en España.

ID	Grupos de ransomware	% Micro	% Total de incidentes - España
1	Qilin	25,0%	22,0%
2	LockBit	25,0%	4,7%
3	Arcusmedia	25,0%	4,0%
4	Brain Cipher	25,0%	2,0%
TOT	**4 Grupos**	**100%**	**32,7%**

4.f. Sectores: incidentes de ransomware en 2025, España

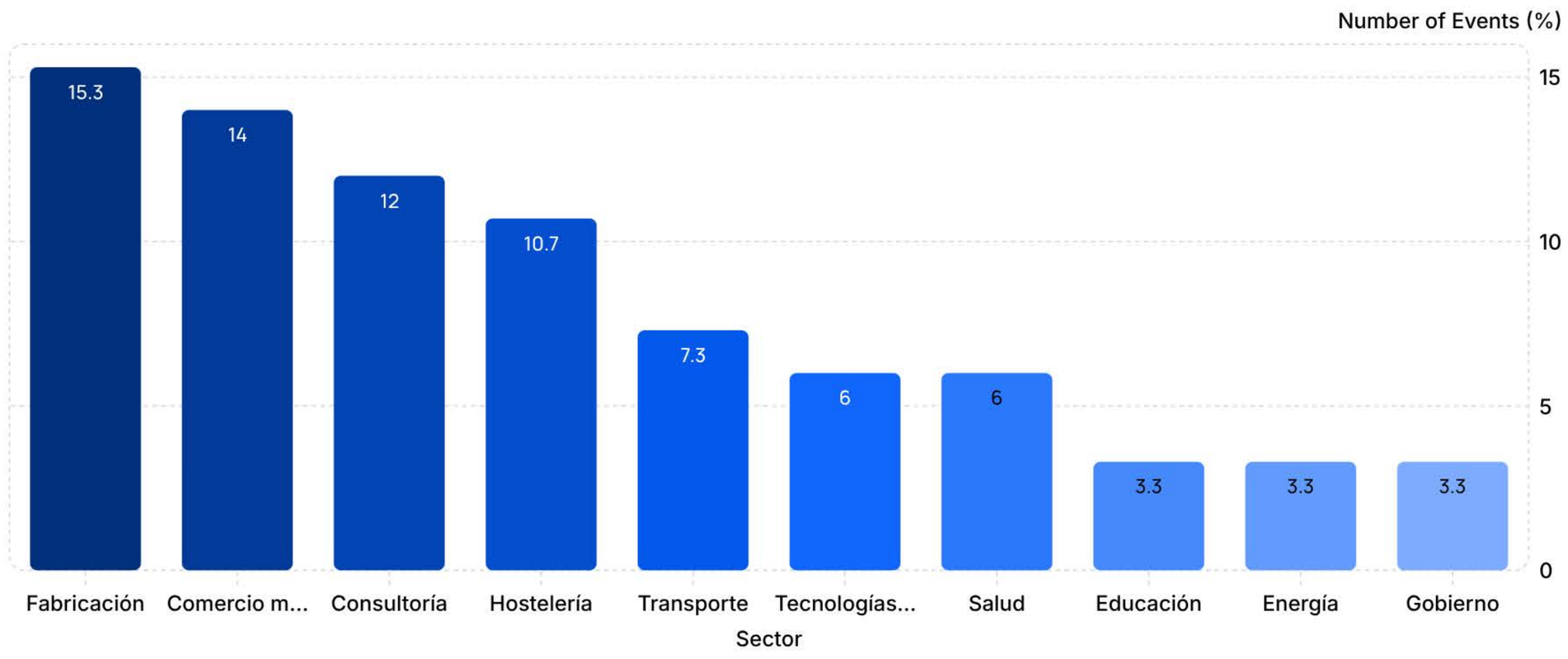
4.f.i. Incidentes de ransomware por sector

A continuación se muestran las estadísticas relacionadas con los sectores afectados por incidentes de ransomware dirigidos a organizaciones en España durante el periodo comprendido entre enero y diciembre de 2025. El total de incidentes afectó a entidades de 20 sectores diferentes (las reclamaciones cuyo sector exacto no se pudo determinar se clasifican como «Otros» y representan el 0,7 % del total de incidentes).



4.f.ii. Los 10 sectores principales: incidentes de ransomware en 2025, España

A continuación se muestra el gráfico de los 10 sectores más afectados por los incidentes de ransomware registrados durante 2025.



Los 10 sectores principales representaron el 81,2 % de los incidentes de ransomware registrados durante 2025. Los 10 sectores restantes sectores (servicios técnicos, finanzas, agricultura y alimentación, automoción, entretenimiento, sociedad civil, construcción, inmobiliario, otros, noticias y medios de comunicación) representaron el 18,8 % restante.

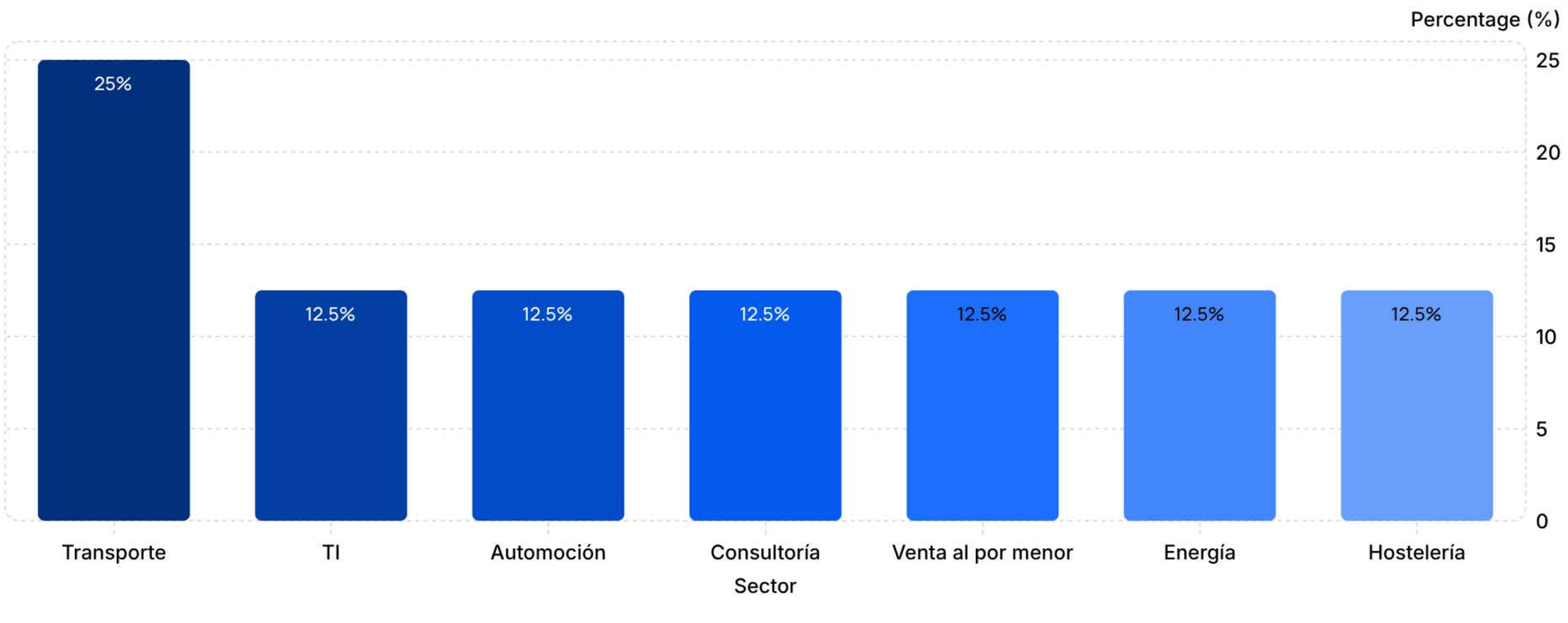
4.f.iii. Sectores y tamaño de las empresas: incidentes de ransomware en 2025 - España

A continuación se muestran los incidentes de ransomware que afectaron a organizaciones españolas, teniendo en cuenta el sector y el tamaño de la empresa.

Empresas: sectores afectados

En 2025, el 5,3 % de las reclamaciones dirigidas a entidades de tamaño empresarial en España afectaron a siete sectores.

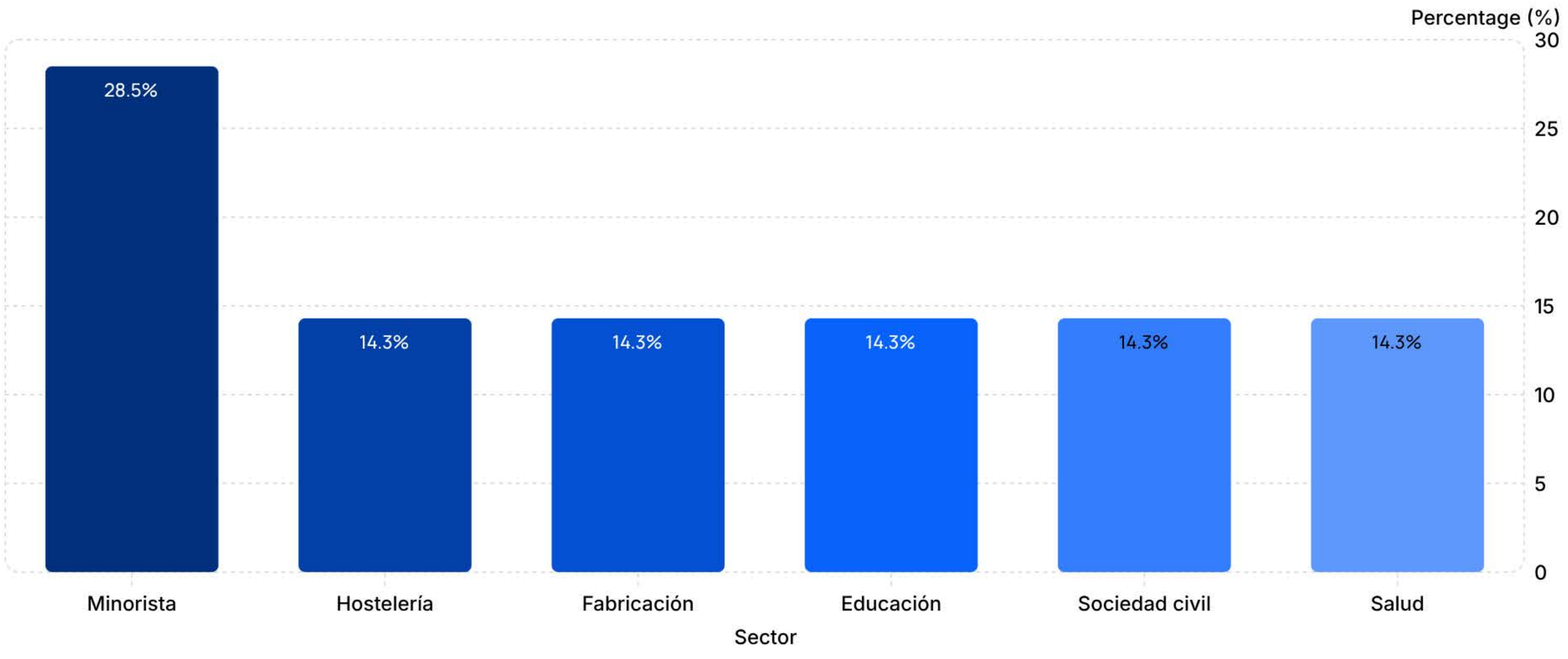
En el siguiente gráfico, los porcentajes sectoriales por tamaño de las entidades se calculan sobre el número total de incidentes que afectaron a organizaciones dentro de la misma categoría de tamaño.



Grandes: sectores afectados

En 2025, el 4,7 % de las reclamaciones dirigidas a entidades GRANDES en España afectaron a 6 sectores.

En el siguiente gráfico, los porcentajes sectoriales por tamaño de las entidades se calculan sobre el número total de incidentes que afectaron a organizaciones dentro de la misma categoría de tamaño.

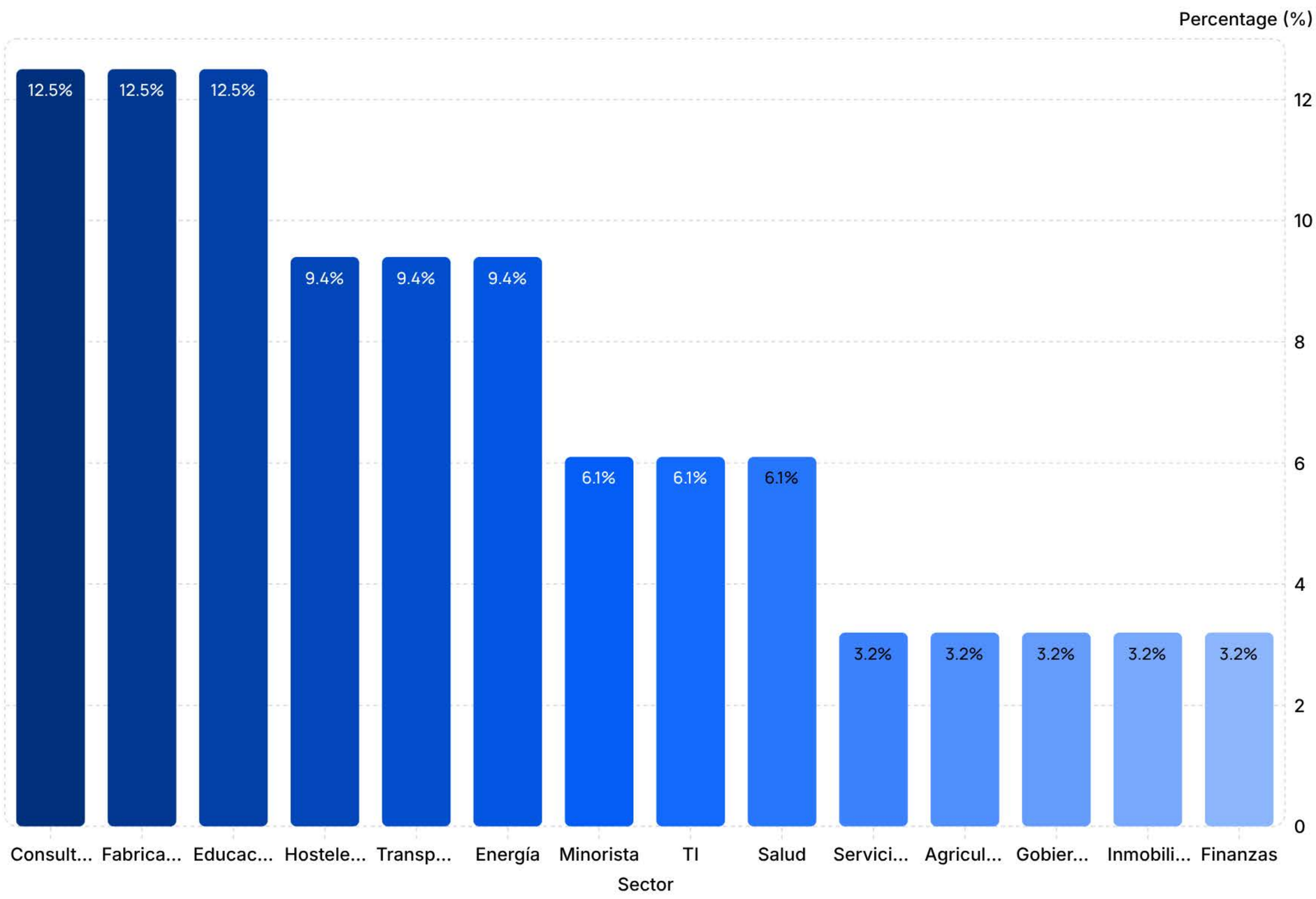


Medio: sectores afectados

En 2025, el 21,3% de las reclamaciones dirigidas a organizaciones de tamaño MEDIANO en España afectaron a 14 sectores.

En el siguiente gráfico, los porcentajes sectoriales por tamaño de las entidades se calculan sobre el número total de incidentes que afectaron a organizaciones dentro de la misma categoría de tamaño.

Sectores - Tamaño de la organización - Mediano España 2025

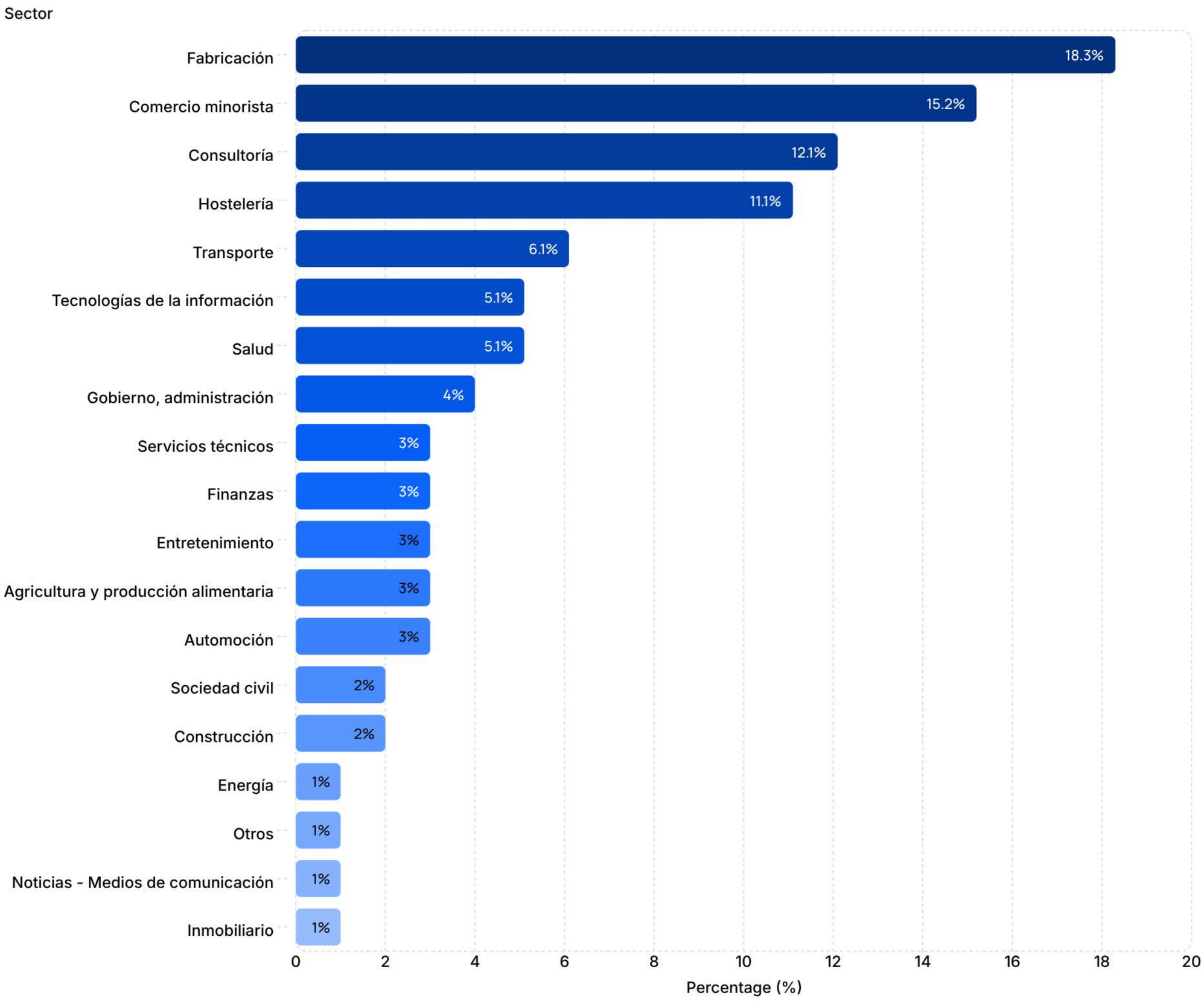


Pequeño: sectores afectados

En 2025, el 66,0% de las reclamaciones dirigidas a empresas PEQUEÑAS en España afectaron a 19 sectores.

En el siguiente gráfico, los porcentajes sectoriales por tamaño de las entidades se calculan sobre el número total de incidentes que afectaron a organizaciones dentro de la misma categoría de tamaño.

Sectores - Tamaño de la organización - Pequeña España 2025

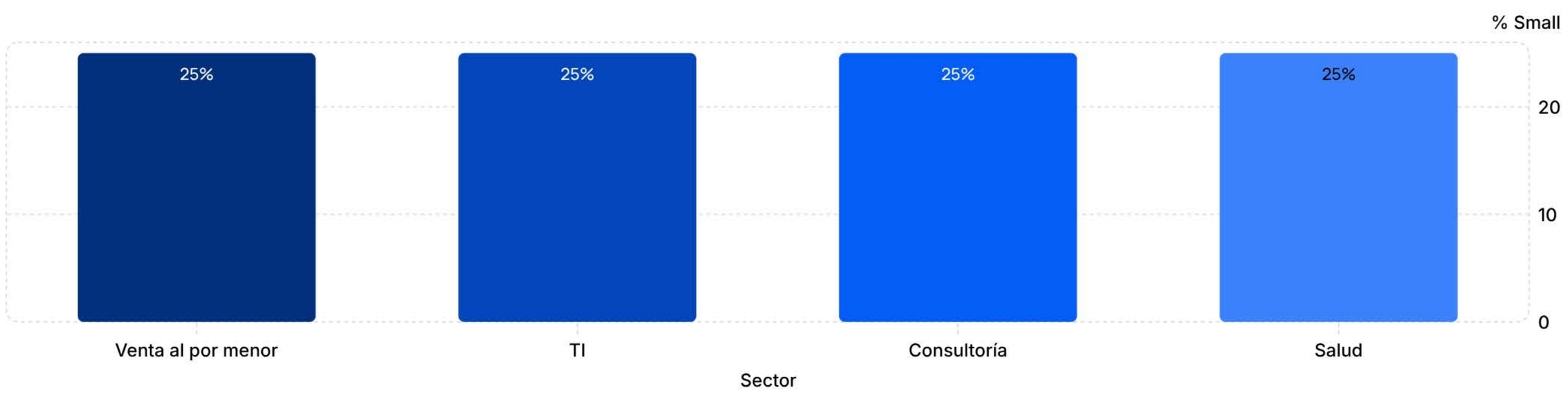


Micro: sectores afectados

En 2025, el 2,7% de las reclamaciones dirigidas a empresas MICRO en España afectaron a 4 sectores.

En el siguiente gráfico, los porcentajes sectoriales por tamaño de las entidades se calculan sobre el número total de incidentes que afectaron a organizaciones dentro de la misma categoría de tamaño.

Sectores - Tamaño de la organización - Micro ESPAÑA 2025



5. Resumen de las actividades hacktivistas contra organizaciones españolas - 2025

5.a. Introducción

El equipo de inteligencia sobre ciberamenazas de Yarix (YCTI) ofrece una visión general de los ataques llevados a cabo por agentes maliciosos cuyas operaciones representan actividades hacktivistas. Según los datos registrados por el equipo YCTI, las operaciones de denegación de servicio/denegación de servicio distribuida (DoS-DDoS) y desfiguración web representaron las principales amenazas a las que se enfrentaron las organizaciones españolas, con un 38,6 % del total de incidentes registrados en 2025.

Por lo general, los grupos hacktivistas persiguen diferentes objetivos en sus operaciones. Intentan disuadir a determinados países de actuar contra los derechos humanos desfigurando sitios web gubernamentales o utilizando ataques DDoS contra recursos que pueden considerarse infraestructuras críticas (como aeropuertos, puertos, portales gubernamentales, proveedores de energía, etc.). Mientras que algunos hacktivistas pueden actuar con fines más humanitarios, otros son más sutiles y protestan contra la agenda nacional o internacional del gobierno. El propósito de sus actividades puede variar, desde desestabilizar el país objetivo hasta instigar disturbios existentes dentro del propio país. Se ha observado o se sospecha que algunos actores hacktivistas tienen fuertes vínculos con potencias extranjeras, como NoName057(16) o el Ejército Cibernético Ruso (Cyber Army of Russia, CARR). Estos dos actores, que surgieron alrededor de marzo de 2022 al inicio del conflicto entre Rusia y Ucrania, operan bajo la apariencia de hacktivistas, pero se sospecha que tienen vínculos con grupos rusos de amenazas persistentes avanzadas [5]. Más recientemente, Estados Unidos confirmó a través de acusaciones del Departamento de Justicia que NoName057(16) y el Cyber Army of Russia (CARR) son productos del Gobierno ruso o están directamente apoyados por él [6].

Por lo tanto, es probable que estos grupos lleven a cabo ataques para promover sus propios intereses, diseñando estratégicamente sus operaciones contra países que actúan en contra de sus supuestos objetivos nacionales.

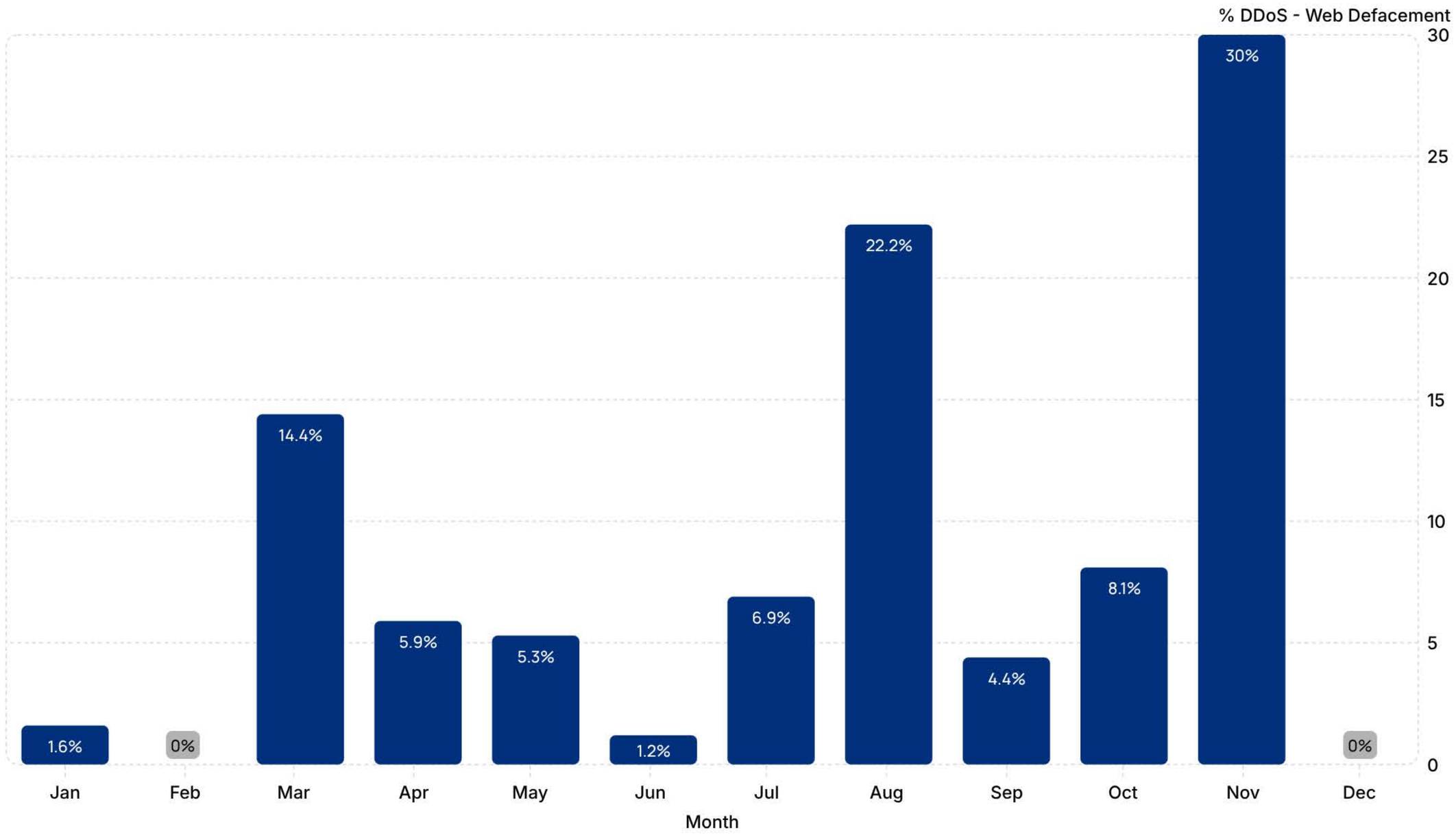
La primera parte de esta sección ofrece una visión general del número de actividades hacktivistas registradas por el equipo YCTI, los actores maliciosos implicados en los ataques, así como su alineación ideológica declarada o evaluada según sus mensajes. La segunda parte describe las motivaciones ideológicas y políticas utilizadas por los grupos hacktivistas para justificar sus operaciones y examina sus correlaciones temporales con los principales acontecimientos en los asuntos internos y externos de España durante 2025.

[5] Mandiant-Google, *APT44: Unearthing Sandworm*, disponible aquí: **https://services.google.com/fh/files/misc/apt44-unearthing-sandworm.pdf** , 17 de abril de 2024.

[6] Departamento de Justicia de EE. UU. (DoJ), el Departamento de Justicia anuncia medidas para combatir a dos grupos rusos de piratería informática patrocinados por el Estado, disponible aquí: **https://www.justice.gov/usao-cdca/pr/justice-department-announces-actions-combat-two-russian-state-sponsored-cyber-criminal**, 9 de diciembre de 2025.

5.b. Estadísticas: sector afectado y actores maliciosos implicados

El siguiente gráfico muestra los picos de actividades hacktivistas observados por el equipo YCTI durante 2025 y dirigidos contra entidades y organizaciones españolas.



Se pueden observar tres picos principales de actividades hacktivistas a lo largo del año, que coinciden con varios acontecimientos relacionados con asuntos y cuestiones nacionales o internacionales de España, algunos de los cuales están estrechamente vinculados a operaciones de lucha contra la ciberdelincuencia en las que participa el Gobierno español. El primer pico se observó entre marzo y mayo de 2025, la segunda oleada se registró entre julio y agosto de 2025, y el tercer pico se registró entre septiembre y noviembre de 2025. La coincidencia temporal no confirma la causalidad, pero es coherente con las narrativas justificativas observadas en las comunicaciones de los actores maliciosos.

Durante 2025, el equipo YCTI observó 24 actores maliciosos (TA) que llevaron a cabo operaciones de DDoS o desfiguración web contra entidades y organizaciones españolas. En la siguiente tabla, el equipo CTI ha indicado el nombre del actor malicioso, el número de eventos relacionados con él (en porcentaje), así como su presunto país de origen o alineación ideológica.

Nota: *La atribución del supuesto país o alineación ideológica correspondiente a los TA se llevó a cabo mediante actividades de inteligencia de fuentes abiertas (OSINT), así como mediante investigaciones encubiertas realizadas por analistas del CTI. El proceso de atribución del equipo YCTI* ***no refleja*** *necesariamente atribuciones oficiales, públicas o técnicas, sino que refleja una evaluación analítica de la alineación del grupo, a menudo expresada en comunicaciones y publicaciones públicas y privadas. Por lo tanto, esta atribución debe considerarse de carácter indicativo, destinada a respaldar el análisis contextual más que a una atribución definitiva. Por ejemplo, algunos colectivos hacktivistas declaran abiertamente en sus mensajes que proceden de una zona o país concretos. Aunque estos indicadores pueden ser falsos o fácilmente fabricados, siguen siendo útiles para comprender las motivaciones que hay detrás de sus actividades y relacionarlas con el contexto geopolítico de sus objetivos.*

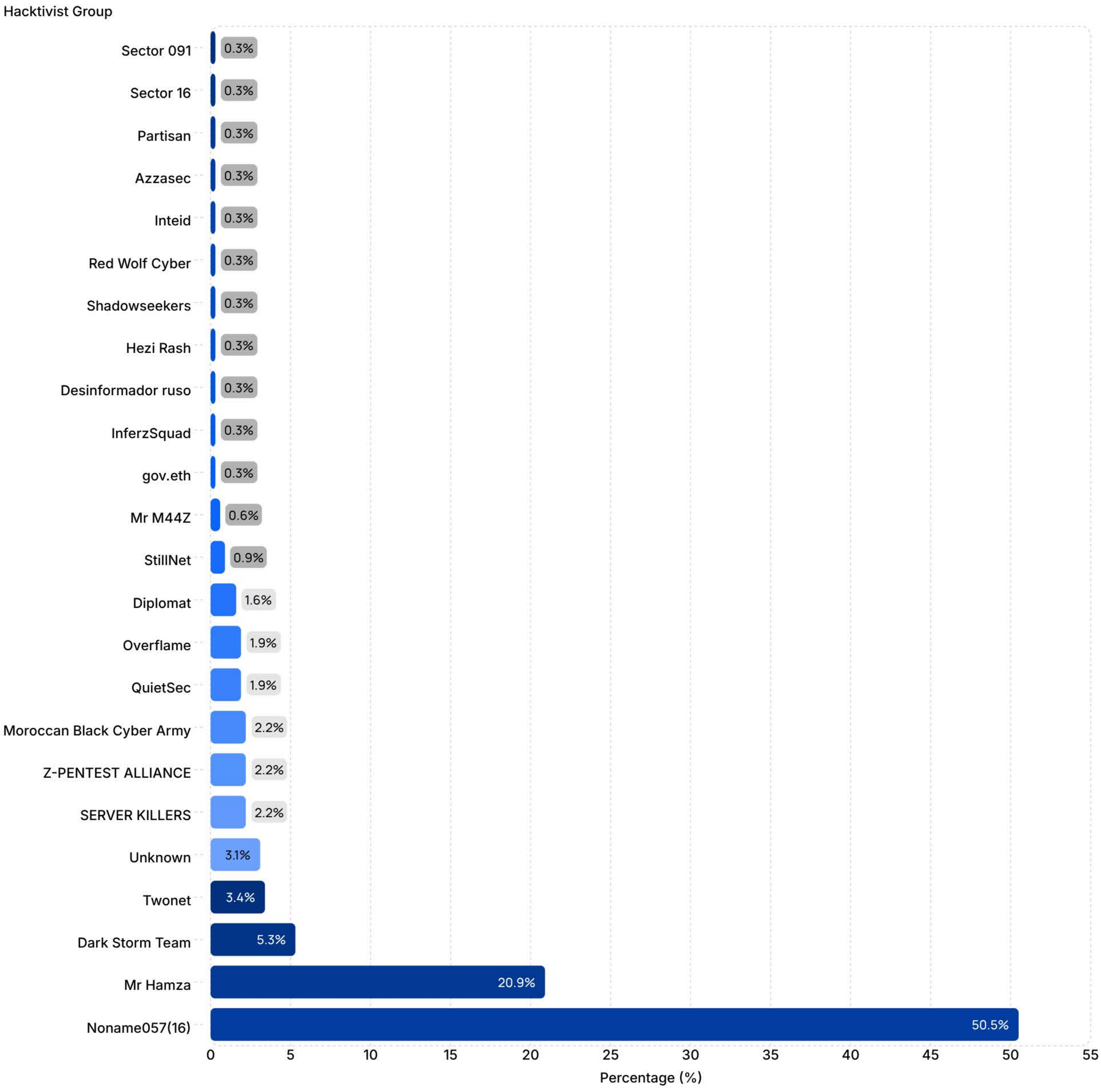
ID	Threat Actor	Número de eventos %	Supuesta alineación ideológica
1	NoName057(16)	50,5%	Russia
2	Mr Hamza	20,9%	Morocco
3	Dark Storm Team	5,3%	Palestine
4	Twonet	3,4%	Russia
5	Unknown	3,1%	Unknown
6	SERVER KILLERS	2,2%	Russia
7	Z-PENTEST ALLIANCE	2,2%	Russia
8	Moroccan Black Cyber Army	2,2%	Morocco
9	QuietSec	1,9%	Russia
10	Overflame	1,9%	Russia
11	Diplomat	1,6%	Russia
12	StillNet	0,9%	Russia
13	Mr M44Z	0,6%	Anonymous
14	gov.eth	0,3%	Unknown
15	InferzSquad	0,3%	Spain
16	Desinformador ruso	0,3%	Russia
17	Hezi Rash	0,3%	Kurdistan
18	Shadowseekers	0,3%	Anonymous
19	Red Wolf Cyber	0,3%	Pakistan
20	Inteid	0,3%	Russia
21	Azzasec	0,3%	Italy
22	Partisan	0,3%	Russia
23	Sector 16	0,3%	Russia
24	Sector 091	0,3%	Russia
TOT	**24 Groups**	**100%**	**-**

El siguiente gráfico se basa en la supuesta alineación ideológica evaluada por los analistas del YCTI:

ID	Alineación ideológica supuesta	Número de eventos %
1.	Rusia	65,9 %
2.	Marruecos/Población proárabe/promusulmana	23,1 %
3.	Palestina	5,3 %
4.	Desconocido	3,4 %
5.	Anónimo	0,9 %
6.	Kurdistán	0,3 %
7.	España	0,3 %
8.	Italia	0,3 %
9.	Pakistán	0,3 %
Total de eventos		**100,0 %**

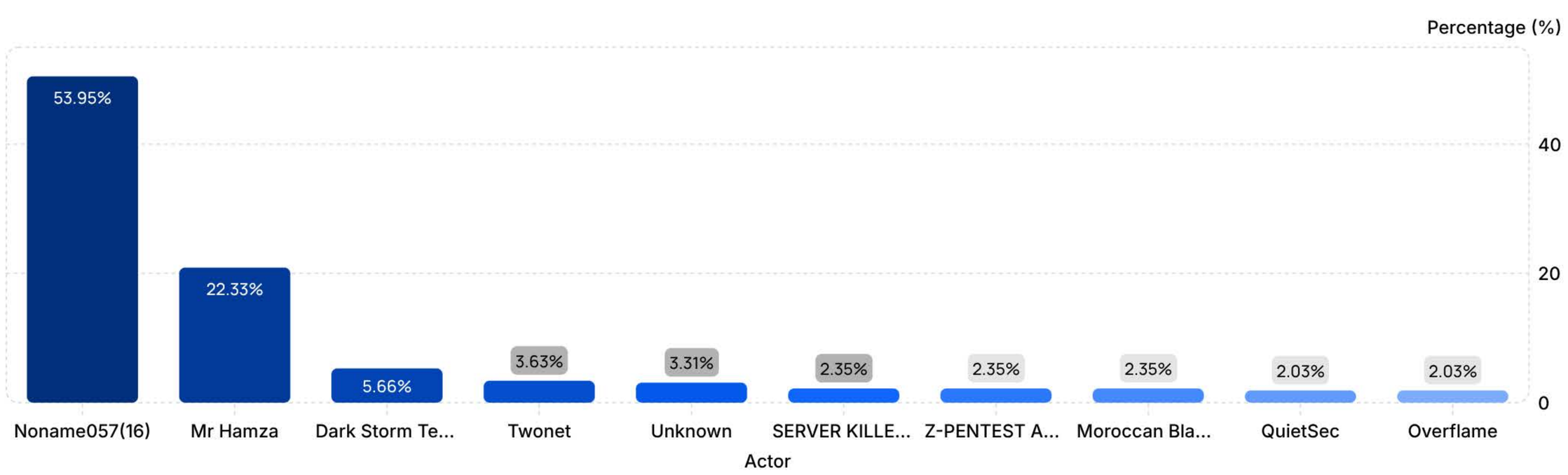
La tabla indica que la mayoría de los eventos dirigidos contra entidades españolas en 2025 estaban asociados con actores que mostraban mensajes alineados con Rusia (65,9 %). El segundo grupo más grande estaba compuesto por actores que mostraban mensajes alineados con Marruecos o más amplios a favor de los árabes/musulmanes (23,1 %), seguidos por mensajes alineados con Palestina (5,3 %). El resto de la actividad fue limitada y se dispersó entre actores no atribuidos/desconocidos (3,4 %), movimientos anónimos/no alineados (0,9 %) y actores individuales vinculados a través de mensajes con el Kurdistán, España, Italia y Pakistán (0,3 % cada uno).

Actividades Hacktivistas% - España 2025



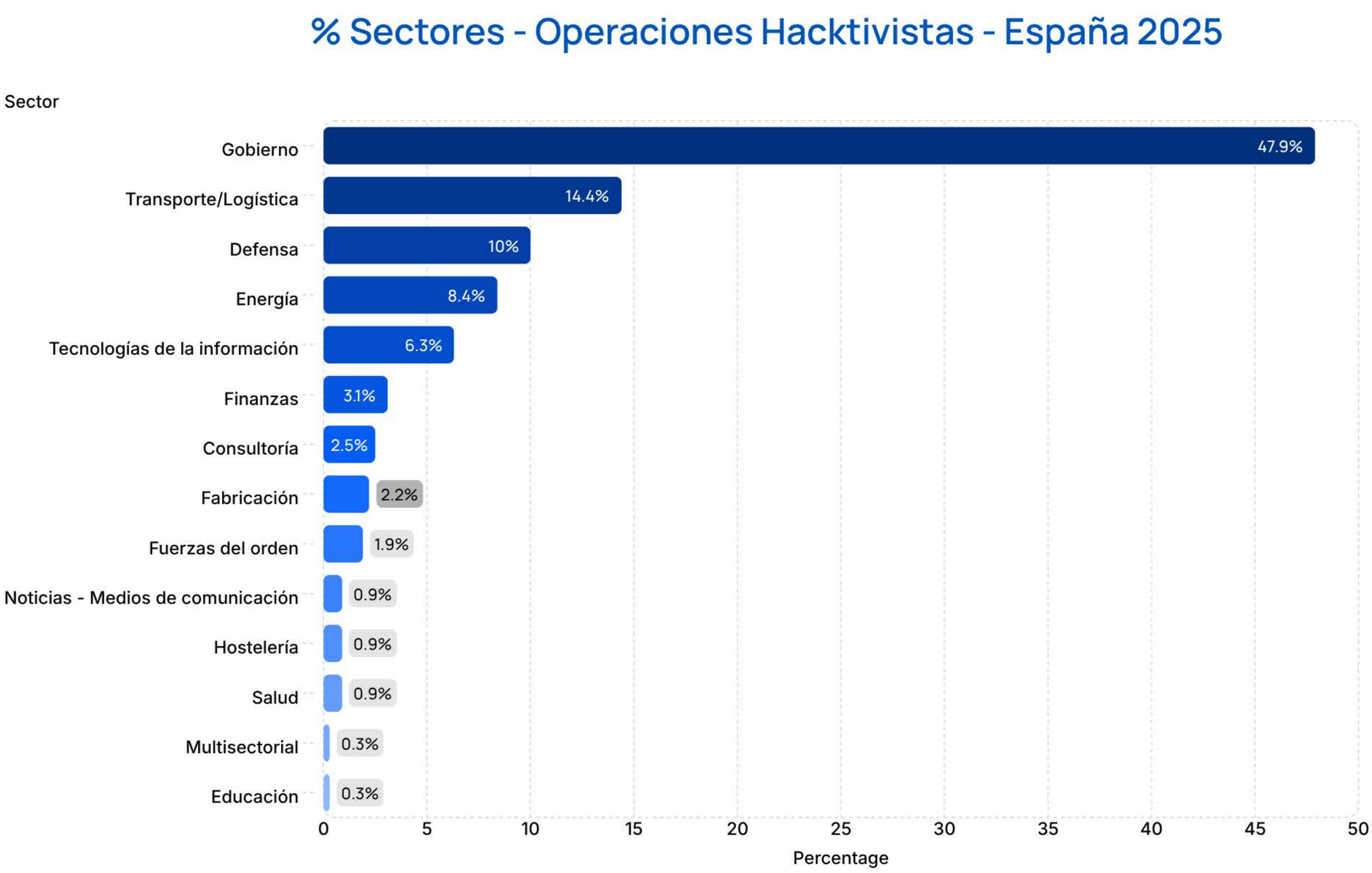
Siguiente gráfico, el equipo de CTI destaca los 10 principales actores maliciosos que llevaron a cabo actividades de DDoS y desfiguración web contra objetivos españoles:

Top-10 Operaciones Hacktivistas España 2025

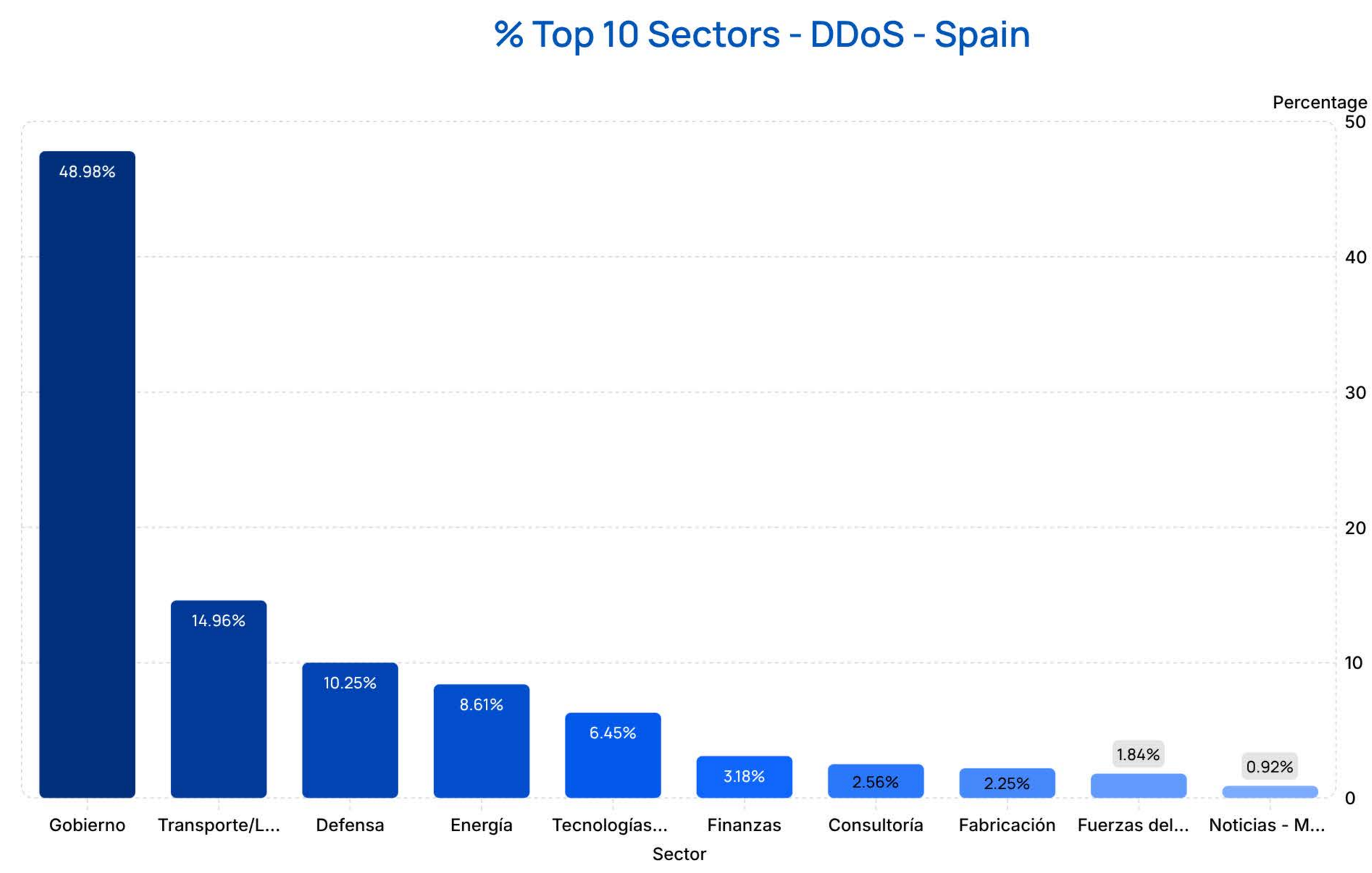


Los principales actores maliciosos fueron responsables del 93,6 % del total de ataques registrados en 2025 contra entidades españolas.

Las amenazas DDoS y Web Defacement representaron el 38,6 % de todos los ataques registrados en 2025 contra empresas, entidades y organizaciones en España. Esta amenaza afectó a 14 sectores diferentes. A continuación se muestra la lista de los sectores específicos afectados por la amenaza:



Los 10 sectores más afectados son los siguientes:



Los eventos registrados contra los 10 sectores más afectados por DDoS y Web Defacement representaron el 97,6 % del total de ataques registrados por el equipo de YCTI, siendo el sector gubernamental el más atacado.

5.c. Motivaciones detrás de las actividades hacktivistas

Mediante la supervisión de canales hacktivistas clandestinos y cerrados, el equipo de CTI ha identificado posibles razones detrás de las oleadas de ataques, que siguen de cerca los acontecimientos en los asuntos internos españoles, así como el panorama geopolítico durante el último año. A lo largo de 2025, los actores maliciosos se refirieron principalmente a crisis en curso, como la guerra entre Rusia y Ucrania, junto con las contraoperaciones contra la ciberdelincuencia lideradas por España o en las que participó este país. Entre los ejemplos más destacados se encuentran la Operación Eastwood y el anuncio por parte de la Policía Nacional [8], el cuerpo policial español, de la inclusión de un antiguo profesor universitario español, acusado de ayudar al grupo de hackers prorruso NoName057(16), en la lista de los más buscados de Europol.[9]

Estos aspectos geopolíticos fueron explotados de manera diferente por los grupos hacktivistas, que utilizaron diversas justificaciones para llevar a cabo operaciones maliciosas contra entidades y organizaciones españolas. Por ejemplo, los actores maliciosos alineados con Rusia utilizaron temas como el apoyo del Gobierno español al Gobierno ucraniano en la lucha contra la invasión rusa para justificar sus actividades de DDoS y desfiguración web.

En este contexto, el análisis de CTI indica que varios actores maliciosos probablemente aprovecharon las protestas internas y los acontecimientos políticos destacados para reforzar narrativas de desestabilización más amplias dirigidas a España. Al alinearse con la cibernética con los periodos de mayor tensión interna y geopolítica, estos actores trataron de amplificar la percepción de fragilidad política, al tiempo que enmarcaban las actividades maliciosas como medidas reactivas o de represalia.

Curiosamente, los actores maliciosos con connotaciones y mensajes proárabes y promusulmanes no parecieron utilizar el tema del conflicto entre Hamás e Israel como justificación para sus operaciones maliciosas. En otras palabras, a diferencia de otros países analizados por el equipo YCTI, las publicaciones de los colectivos observados no criticaban a España por apoyar a Israel en relación con la situación de Gaza. Este aspecto podría interpretarse en conjunción con la política interna española durante 2025, que criticó abiertamente el papel de Israel en el conflicto [10] entre Hamás e Israel, al tiempo que adoptó medidas económicas restrictivas contra el Gobierno de Tel Aviv. [11]

[7] Europol, *Operación global contra la red de ciberdelincuencia prorrusa NoName057(16)*, disponible aquí: **https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network**, julio de 2025..

[8] Policía Nacional, publicación en X sobre la lista de los más buscados de Europol (Enrique Arias Gil), disponible aquí: **https://x.com/policia/status/1966425901605785649**, 12 de septiembre de 2025.

[9] Noticia de Recorded Future News, *Europol añade a un académico español sospechoso de ayudar a hackers prorrusos a la lista de los más buscados*, disponible aquí: **https://therecord.media/europol-adds-spanish-academic-most-wanted-russia-hack**, 15 de septiembre de 2025.

[10] La Moncloa, *El Gobierno de España acuerda medidas para detener el genocidio en Gaza y apoyar al pueblo palestino*, disponible aquí: **https://www.lamoncloa.gob.es/lang/en/gobierno/councilministers/paginas/2025/20250909-council-pressconference.aspx**, 9 de septiembre de 2025.

[11] La Moncloa, *El Gobierno de España refuerza el embargo de armas a Israel y prohíbe las importaciones procedentes de los asentamientos ilegales en los territorios palestinos,* disponible aquí: **https://www.lamoncloa.gob.es/lang/en/gobierno/councilministers/paginas/2025/20250923-councilpress-conference.aspx**, 23 de septiembre de 2025.

A continuación, se ofrece una visión general de las tres oleadas de ataques, en la que se esbozan las posibles justificaciones utilizadas por los autores de las amenazas, a menudo basadas en la agenda y los acontecimientos nacionales y extranjeros de España. Por último, se presentarán pruebas de las afirmaciones de los canales hacktivistas.

5.d. Las tres oleadas de un vistazo, la evolución de la línea operativa hacktivista

Ola 1 - Mar - Mayo 2025

Presión operativa sostenida y alineamiento oportunista con desarrollos geopolíticos y nacionales. La actividad hacktivista se utilizó para enmarcar ataques DDoS y desfiguraciones como acciones reactivas.

Ola 3 - Sep - Nov 2025

La narrativa centrada en España se amplificó como catalizador para reforzar la cohesión del grupo en un contexto de focalización en instituciones gubernamentales. La actividad hacktivista se centró en campañas altamente centralizadas y en la gestión de la percepción pública.

1 2 3

Ola 2 - Jul - Ago 2025

La Operación Eastwood se reformuló como un detonante de movilización para una acción retaliatoria. La actividad hacktivista combinó la señalización estratégica con la proyección de capacidades.

5.d.i. Primera ola: coalición de voluntarios, gasto en defensa y apoyo a Ucrania

> **Highlight – Ola 1:** Las operaciones hacktivistas se programaron deliberadamente en torno a momentos de alta relevancia política, aprovechando la tensión internacional y la presión interna para presentar los ataques como actos reactivos coherentes con narrativas más amplias prorrusas y anti-OTAN.

La primera oleada de actividades de DDoS y desfiguración web dirigidas contra entidades españolas parece coincidir temporalmente con una serie de acontecimientos internacionales y nacionales muy visibles que tuvieron lugar durante el primer trimestre de 2025. En concreto, la actividad maliciosa observada siguió de cerca los acontecimientos políticos y diplomáticos relacionados con la guerra entre Rusia y Ucrania, junto con períodos de mayor debate público y atención política en España. Si bien la coincidencia temporal no establece una causalidad, es coherente con las narrativas justificativas observadas en las comunicaciones de los actores de la amenaza.

El 2 de marzo de 2025, el primer ministro británico Keir Starmer convocó una reunión de alto nivel en Londres con el objetivo de establecer lo que más tarde se denominó una «coalición de voluntarios», destinada a promover una propuesta de paz para Ucrania y garantizar al mismo tiempo el apoyo militar continuo y el mantenimiento de las sanciones contra Rusia en caso de que fracasaran los esfuerzos diplomáticos [12]. El primer ministro español participó en la reunión y reiteró públicamente el compromiso de España de apoyar a Ucrania durante el tiempo que fuera necesario.[13] Esta participación siguió a una visita anterior del primer ministro español a Kiev para conmemorar el tercer aniversario de la invasión a gran escala de Ucrania por parte de Rusia, lo que reforzó aún más la alineación visible de España con las posiciones proucranianas en un momento delicado del conflicto.[14]

Estas iniciativas diplomáticas se produjeron en paralelo a debates europeos más amplios sobre el refuerzo de las capacidades de defensa. A principios de 2025, la Unión Europea impulsó planes para aumentar la inversión en defensa a través de iniciativas como el marco European Defence Readiness 2030 y el plan ReArm Europe. [15]

[12] GOV.UK, Declaración del presidente: Reunión de líderes sobre Ucrania, disponible aquí: https://www.gov.uk/government/news/chairs-statementleaders-meeting-on-ukraine-london-2-march-2025, 2 de marzo de 2025.

[13] La Moncloa, El presidente del Gobierno de España participa en la Reunión de Alto Nivel sobre Ucrania en Londres, disponible aquí: https://www.lamoncloa.gob.es/lang/en/presidente/news/paginas/2025/20250302-london-ukraine-meeting.aspx, 4 de marzo de 2025.

[14] La Moncloa, Pedro Sánchez se reúne con Zelenski en Kiev para conmemorar el tercer aniversario del inicio de la agresión rusa contra Ucrania, disponible aquí: https://www.lamoncloa.gob.es/lang/en/presidente/news/paginas/2025/20250224-ukraine-bilateral-meeting.aspx, 24 de febrero de 2025.

[15] Parlamento Europeo, Plan ReArm Europe/Preparación 2030, disponible aquí: https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/769566/EPRS_BRI(2025)769566_EN.pdf, abril de 2025.

Aunque España expresó una postura crítica hacia el objetivo propuesto por la OTAN de destinar el 5 % del PIB al gasto en defensa, las autoridades españolas apoyaron públicamente los esfuerzos de rearme impulsados por la UE, enmarcándolos como una oportunidad para modernizar las capacidades de defensa y reindustrializar sectores clave de la economía nacional.[16] Esta posición matizada situó a España en el centro de los debates contemporáneos sobre la política europea de seguridad y defensa.[17]

Durante el mismo período, España experimentó una mayor presión interna, incluidas manifestaciones a nivel nacional relacionadas con la actual crisis de la vivienda y los alquileres. Las protestas a gran escala en varias ciudades atrajeron una gran atención mediática y contribuyeron a crear un clima de tensión política y social interna.[18] Estos acontecimientos aumentaron aún más la visibilidad de los asuntos internos de España, tanto a nivel nacional como internacional.[19] En este contexto, los actores maliciosos hacktivistas y con motivaciones políticas parecen haber aprovechado el momento oportuno para llevar a cabo sus operaciones cibernéticas maliciosas. Durante la primera oleada, se llevaron a cabo campañas de DDoS y desfiguración de sitios web en estrecha proximidad temporal con compromisos diplomáticos clave, anuncios relacionados con la defensa y períodos de intenso debate interno. La sincronización de las operaciones cibernéticas con estos acontecimientos sugiere la intención de presentar los ataques como respuestas reactivas o de represalia a la posición de la política exterior española y a su participación en iniciativas de defensa europeas, al tiempo que se amplifica su impacto disruptivo y simbólico en momentos de mayor exposición política.

En general, la primera oleada de actividad indica una alineación deliberada de las operaciones cibernéticas con acontecimientos políticamente destacados, lo que permite a los actores maliciosos aprovechar las tensiones internacionales y las presiones internas existentes sin necesidad de introducir nuevas narrativas. El momento en sí mismo sirvió como elemento central para justificar y dar relevancia a los ataques.

Conclusión clave:

Se considera que la primera ola de actividad hacktivista contra entidades españolas estuvo estratégicamente sincronizada con compromisos diplomáticos de alta visibilidad, debates sobre política de defensa y tensiones políticas internas. En lugar de introducir nuevas narrativas geopolíticas, los actores de amenaza aprovecharon desarrollos internacionales y nacionales ya existentes para presentar las operaciones cibernéticas como medidas reactivas alineadas con mensajes más amplios anti-OTAN y prorrusos. Este patrón pone de relieve cómo las campañas hacktivistas pueden explotar momentos de elevada exposición política para maximizar el impacto simbólico y la amplificación narrativa sin necesidad de una sofisticación operativa sostenida.

Paralelamente a estas actividades, en el mismo período también surgieron acciones basadas en narrativas y afirmaciones falsas por parte de grupos hacktivistas, que se abordan en la siguiente *sección Operaciones de información y afirmaciones falsas*.

[16] Reuters, La coalición gobernante en España se divide sobre el gasto en defensa mientras los líderes de la UE presionan para que se incremente, disponible aquí: https://www.reuters.com/world/europe/spains-pm-sanchez-sees-defence-technology-upgrade-eus-priority-2025-03-20/, 20 de marzo de 2025.

[17] Reuters, España corre el riesgo de descarrilar la cumbre de la OTAN al resistirse al objetivo del 5 % de gasto en defensa, disponible aquí: https://www.reuters.com/business/aerospace-defense/spain-wants-opt-out-natos-5-defence-spending-target-2025-06-19/, 19 de junio de 2025

[18]Reuters, Manifestantes se concentran en toda España contra la crisis de la vivienda y los pisos turísticos, disponible aquí: https://www.reuters.com/world/europe/protesters-rally-across-spain-against-housing-crisis-tourist-flats-2025-04-05/, 5 de abril de 2025.

[19] Le Monde, En España, decenas de miles de personas se manifiestan en todo el país para protestar contra la creciente crisis de la vivienda, https://www.lemonde.fr/en/international/article/2025/04/05/in-spain-tens-of-thousands-march-across-the-country-to-protest-the-growinghousing-crisis_6739878_4.html, 5 de abril de 2025.

Operaciones de información y afirmaciones falsas

Durante el período correspondiente a la primera ola de actividades de DDoS y desfiguración de sitios web, la supervisión del CTI también identificó el uso de operaciones de información y afirmaciones falsas por parte de varios colectivos hacktivistas. En concreto, el equipo de CTI informa de una actividad de afirmaciones falsas que surgió tras el apagón a gran escala que afectó a España a finales de abril de 2025.[20] Aunque las investigaciones oficiales y las evaluaciones técnicas descartaron cualquier componente cibernético y atribuyeron el apagón a causas no maliciosas, el incidente generó una gran atención pública y especulaciones en línea.[21]

En este contexto, un actor hacktivista reivindicó públicamente la responsabilidad de los cortes de electricidad a través de las redes sociales y los canales de mensajería. En concreto, el colectivo hacktivista Dark Storm emitió declaraciones públicas en X (**x.com**) afirmando que, junto con el grupo NoName057, había causado cortes de electricidad en varios países de la OTAN, afirmando: «Hoy, nosotros y el equipo noname057 hemos conseguido cortar el suministro eléctrico en algunos países de la OTAN».[22] Estas afirmaciones no estaban respaldadas por pruebas técnicas y contradecían directamente las declaraciones oficiales y los informes posteriores, que descartaban cualquier componente cibernético en el incidente. La información disponible indica que tales afirmaciones eran oportunistas y engañosas, y no reflejaban las capacidades operativas reales ni la participación en el suceso.[23]

Afirmaciones falsas del equipo Dark Storm

La difusión de afirmaciones falsas parece coherente con una estrategia más amplia destinada a amplificar la narrativa, más que a tener un impacto operativo directo. Al asociarse con un evento disruptivo de gran visibilidad, ajeno a la actividad cibernética, los actores maliciosos buscaban proyectar una imagen de mayor capacidad, relevancia y alcance, al tiempo que reforzaban el mensaje geopolítico existente en consonancia con sus campañas más amplias contra España y otros países europeos.

En general, estas operaciones de información ponen de relieve cómo los grupos hacktivistas que acompañan a las campañas de DDoS y de desfiguración de sitios web pueden intentar ampliar su influencia más allá de las acciones puramente técnicas. En este contexto, las afirmaciones falsas funcionaron como una táctica complementaria, aprovechando el momento y la resonancia mediática de acontecimientos no cibernéticos para mejorar la eficacia y la legitimidad percibidas, a pesar de la ausencia de una base factual o técnica. [24]

[20] NASA Earthdata, Archivo de imágenes Worldview: Corte de energía en España, disponible aquí: **https://www.earthdata.nasa.gov/news/worldviewimage-archive/power-outage-spain**, 1 de mayo de 2025.

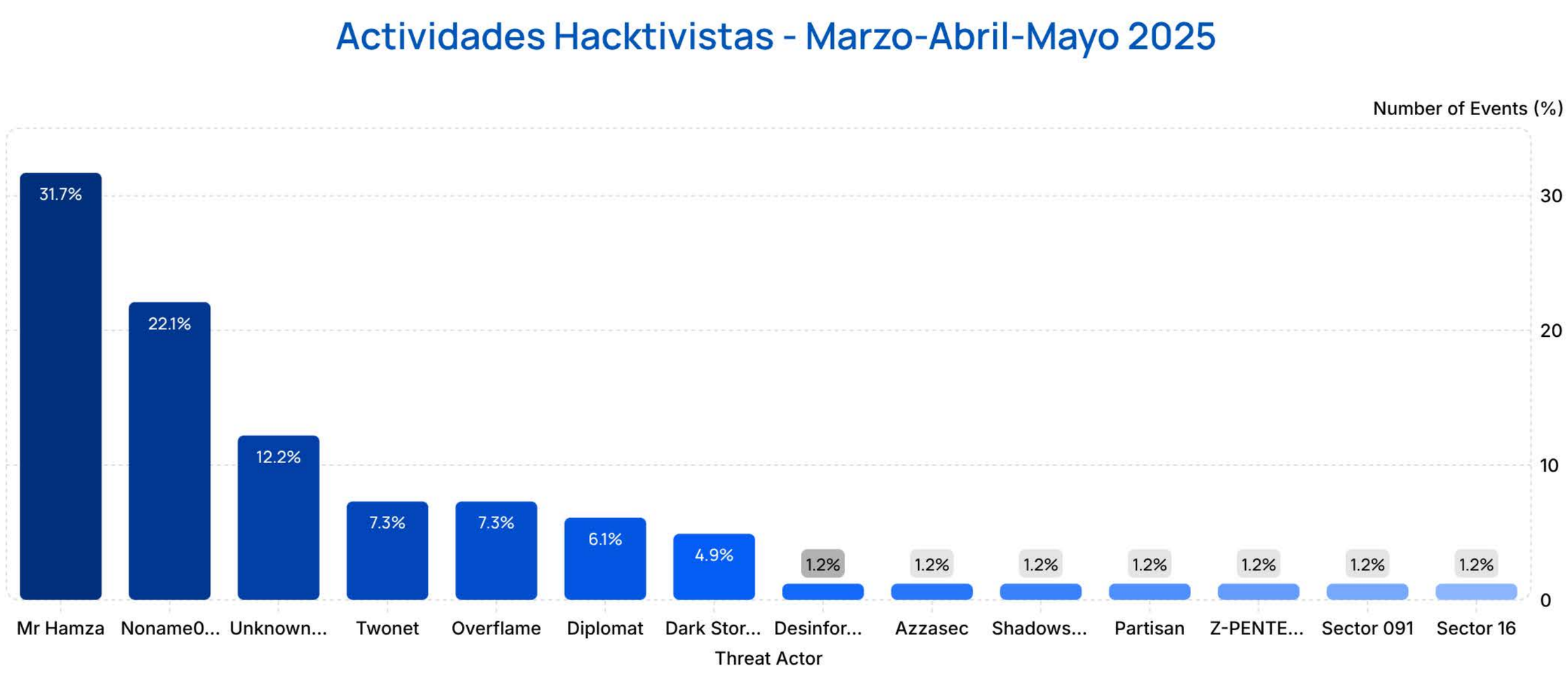
[21] The Guardian, El ministro español descarta un ciberataque como causa del apagón de abril, tras el informe de los expertos, disponible aquí: **https://www.theguardian.com/world/2025/jun/17/expert-report-rules-out-cyber-attack-for-spain-and-portugal-april-blackout** , 17 de junio de 2025.

[22] ZeroFox Intelligence, Informe flash: Hacktivistas reivindican la autoría de los recientes cortes de electricidad, disponible aquí: **https://www.zerofox.com/intelligence/flash-report-hacktivists-claim-responsibility-for-recent-power-outages/** (Informe flash: Hacktivistas reivindican la autoría de los recientes apagones), 1 de mayo de 2025.

[23] ZeroFox Intelligence, Informe flash: Hacktivistas reivindican la autoría de los recientes cortes de electricidad, disponible aquí: **https://www.zerofox.com/intelligence/flash-report-hacktivists-claim-responsibility-for-recent-power-outages/**, 1 de mayo de 2025.

Entre marzo y mayo, el equipo YCTI observó 14 colectivos hacktivistas que atacaban a organizaciones españolas:

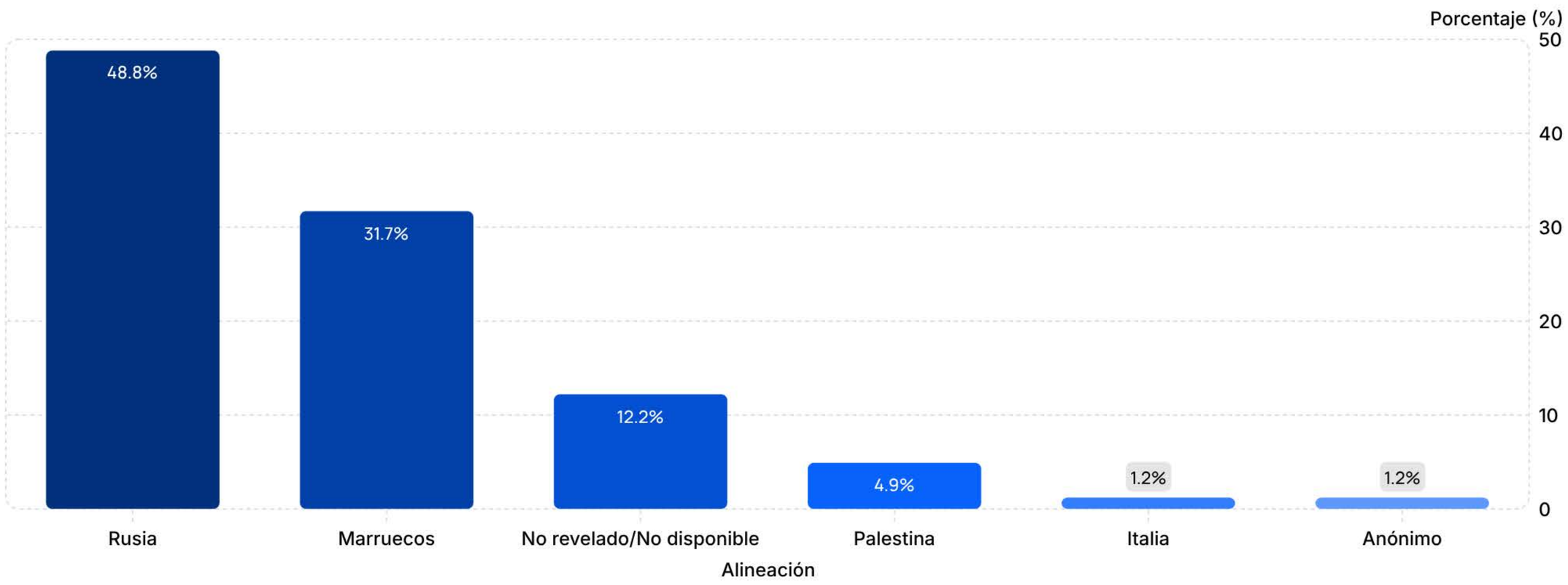
ID	Threat Actor – Primera Ola	Número de eventos (%)	Alineación declarada o evaluada
1	Mr Hamza	31,7%	Marruecos
2	Noname057(16)	22,1%	Rusia
3	Not Available/Not Disclosed	12,2%	No revelado/No disponible
4	Twonet	7,3%	Rusia
5	Overflame	7,3%	Rusia
6	Diplomat	6,1%	Rusia
7	Dark Storm Team	4,9%	Palestina
8	Desinformador ruso	1,2%	Rusia
9	Azzasec	1,2%	Italia
10	Shadowseekers	1,2%	Anónimo
11	Partisan	1,2%	Rusia
12	Z-PENTEST ALLIANCE	1,2%	Rusia
13	Sector 091	1,2%	Rusia
14	Sector 16	1,2%	Rusia
Total Events Registered		**100%**	



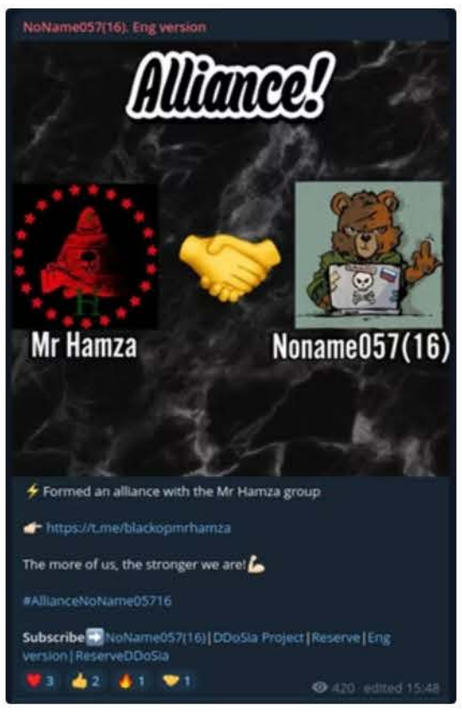
[24] La Moncloa, *El Gobierno de España presenta el informe sobre las causas del apagón, que se debió a una "subida multifactorial"*, disponible aquí: https://www.lamoncloa.gob.es/lang/en/gobierno/councilministers/paginas/2025/20250617-council-press-conference.aspx, 17 de junio de 2025

La siguiente tabla contiene la distribución de actores de amenaza observados durante la primera ola, agrupados por alineación:

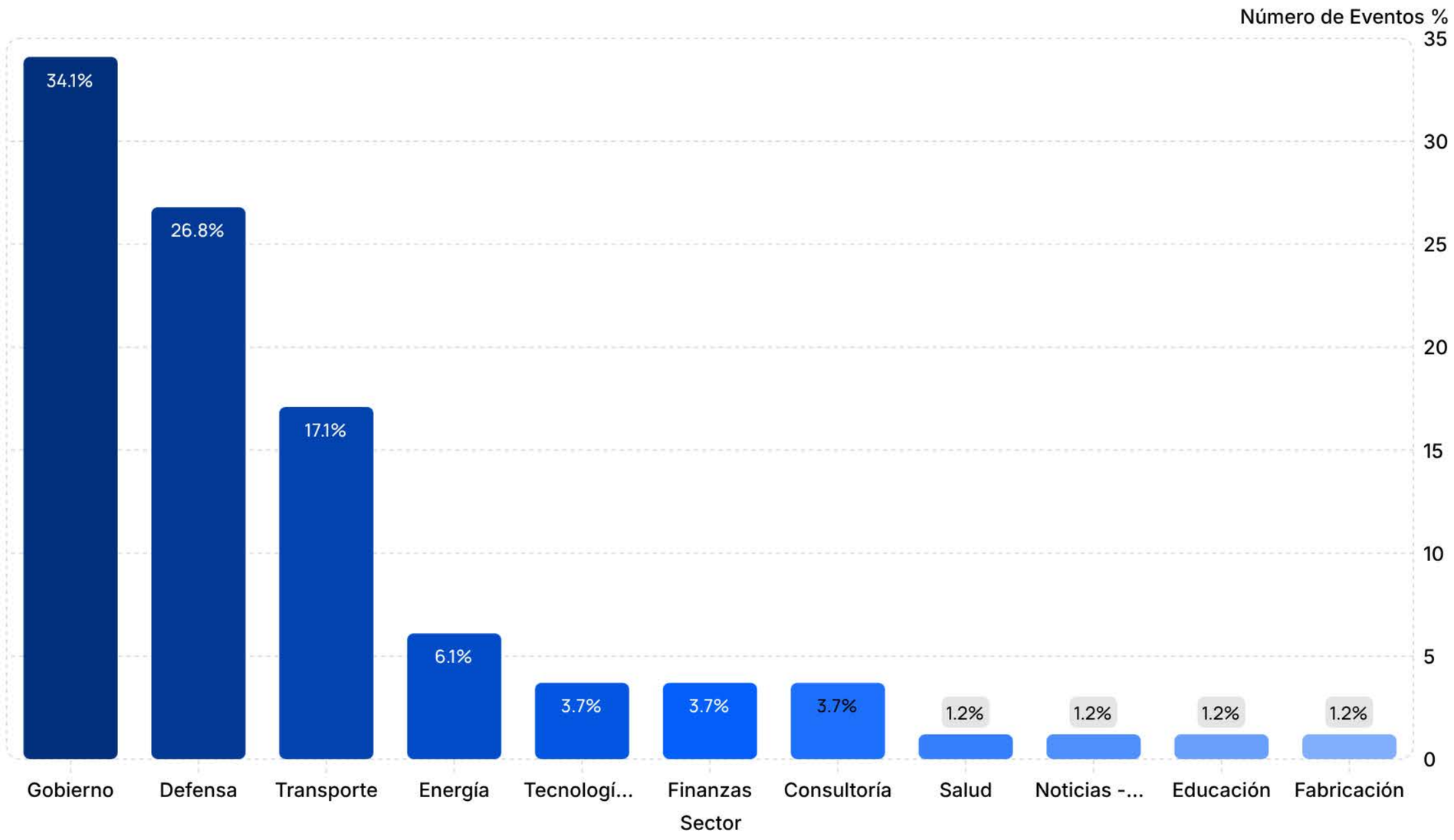
ID	**Alineación declarada o evaluada**	**Número de eventos (%)**	**Número de Threat Actors**
1	Rusia	48,8%	9
2	Marruecos	31,7%	1
3	No revelado/No disponible	12,2%	1
4	Palestinia	4,9%	1
5	Italy	1,2%	1
TOT	**5 Alineaciónes**	**100%**	**14**



Aunque Hamza es identificado públicamente como un agente malicioso alineado con Marruecos y se convirtió en el colectivo más activo durante la primera ola, el análisis de CTI indica una estrecha alineación operativa y narrativa con el grupo vinculado a Rusia NoName057(16). Esto se demuestra aún más por la alianza formalmente declarada con NoName057(16) observada a finales de 2024 [25], lo que, combinado con patrones de objetivos superpuestos, sugiere una posible alineación operativa dentro del ecosistema hacktivista más amplio vinculado a Rusia. Si bien el actor de la amenaza refleja una narrativa alineada con causas proárabes o más amplias proislámicas, también parece estar estrechamente alineado con un ecosistema hacktivista más amplio vinculado a Rusia, lo que sugiere que puede emplear una mezcla de etiquetas ideológicas y nacionales y alinearse potencialmente con intereses extranjeros más amplios.



[25] Radware, *Anuncio de la alianza entre el Sr. Hamza y NoName057(16), noviembre de 2024*, disponible aquí: https://www.radware.com/security/threat-advisories-and-attack-reports/the-rise-of-alliances-noname057-16-transformation-in-2024/, 16 de diciembre de 2024.



El predominio de los objetivos gubernamentales (34,1 %) y de defensa (26,8 %) refleja una clara alineación con el posicionamiento visible de España en los debates sobre seguridad de la UE y su continuo apoyo a Ucrania. Las instituciones gubernamentales representan objetivos políticamente simbólicos capaces de reforzar los mensajes geopolíticos, mientras que las entidades relacionadas con la defensa se corresponden directamente con los debates contemporáneos sobre el rearme y el gasto militar. El importante número de ataques dirigidos al transporte (17,1 %) sugiere además la intención de perturbar o afectar simbólicamente a los sectores relacionados con las infraestructuras nacionales y la movilidad durante los periodos de mayor atención política. Este patrón de ataques es coherente con las campañas de DDoS y desfiguración orientadas a la influencia que han llevado a cabo históricamente los colectivos hacktivistas prorrusos, en las que los mensajes estratégicos y las señales políticas prevalecen sobre la perturbación operativa sostenida.

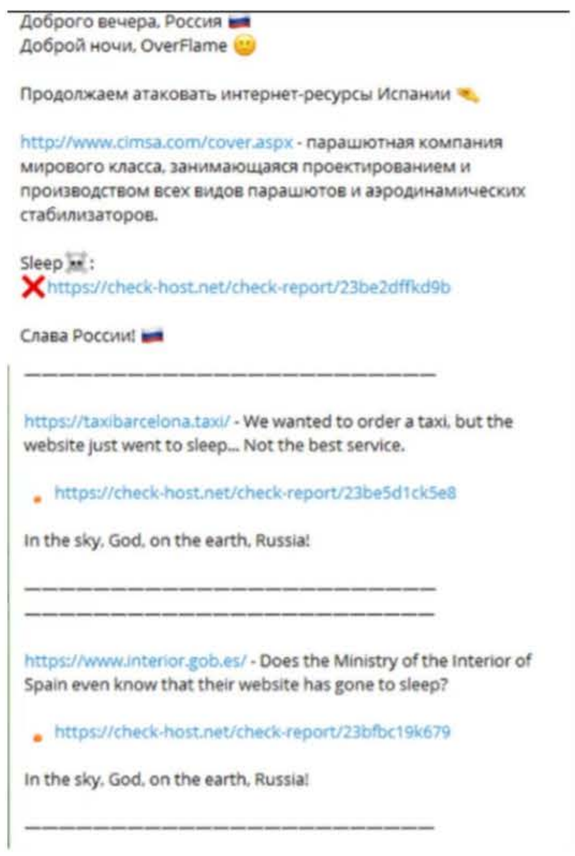
Primera oleada: pruebas de las afirmaciones de los hacktivistas

Las siguientes secciones proporcionan ejemplos de las reivindicaciones realizadas por grupos hacktivistas identificados por el Equipo CTI a partir de canales privados de dichos grupos.

«Mr. Hamza»

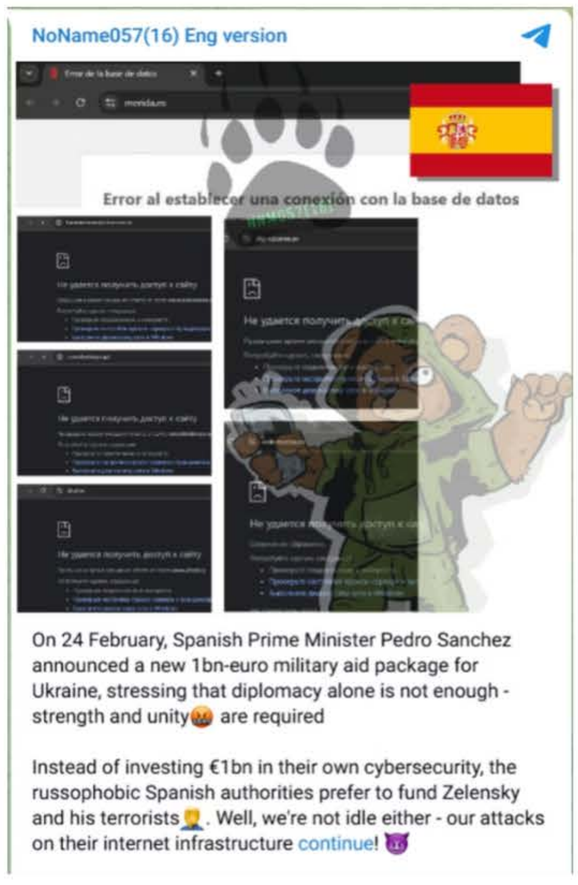
> **Traducción de la publicación original**: Esta noche se lanzaron ciberataques precisos contra la infraestructura electrónica militar española, dirigidos a:
>
> Ministerio de Defensa de España
>
> Ejército de Tierra
>
> Armada Española
>
> Ejército del Aire
>
> Estado Mayor de la Defensa
>
> El mensaje es claro: «Andalucía es nuestra... y la recuperaremos, incluso si os aliáis con el diablo. La historia no olvida.»

«OverFlame»



Traducción de la publicación original: «https:// [..] Queríamos pedir un taxi, pero la página web se colgó... No es el mejor servicio. https://check-host.net[..] ¡En el cielo, Dios; en la tierra, Rusia! --- «https:// [...] ¿Sabe siquiera el Ministerio del Interior de España que su sitio web ha dejado de funcionar? https://check-host.net[..] ¡En el cielo, Dios; en la tierra, Rusia!

«NoName057(16)» - Grupo alineado con Rusia



Traducción de la publicación original: *«El 24 de febrero, el presidente del Gobierno español, Pedro Sánchez, anunció un nuevo paquete de ayuda militar de 1000 millones de euros para Ucrania, subrayando que la diplomacia por sí sola no es suficiente, sino que se requiere fuerza y unidad.*

En lugar de invertir 1000 millones de euros en su propia ciberseguridad, las autoridades españolas rusófobas prefieren financiar a Zelensky y a sus terroristas. Bueno, nosotros tampoco estamos de brazos cruzados: nuestros ataques a su infraestructura de Internet continúan».

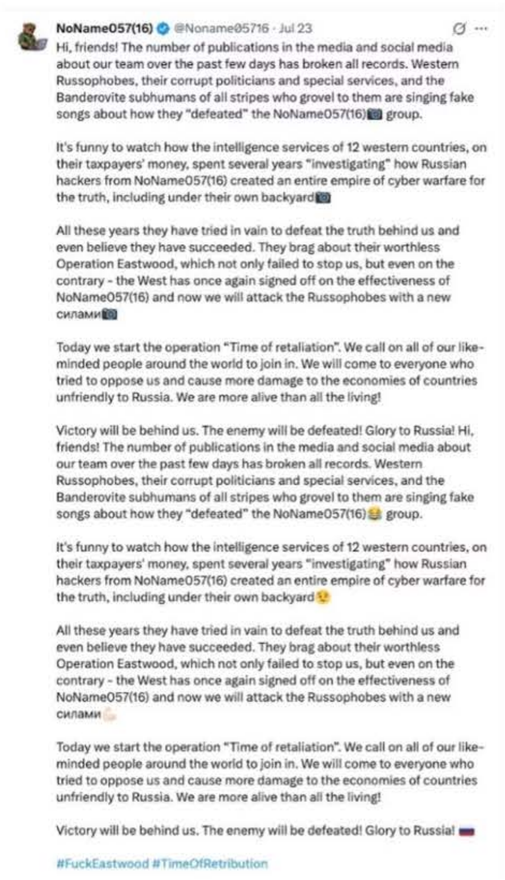
5.d.ii. Segunda ola: Operación Eastwood, un intento de desbaratar NoName057(16)

> **Highlight – Ola 2:** La Operación Eastwood fue rápidamente reformulada como una narrativa de movilización, lo que desencadenó un repunte retaliatorio de actividad DDoS en el que los ataques funcionaron como señalización estratégica, presión reputacional y proyección de capacidades, poniendo de relieve la resiliencia de las redes hacktivistas prorrusas descentralizadas y de carácter ideológico.

La segunda oleada de actividades hacktivistas dirigidas contra organizaciones españolas se observó entre julio y agosto de 2025. Esta oleada se desencadenó principalmente por la operación policial internacional Eastwood. [26] Entre el 14 y el 17 de julio de 2025, Europol y Eurojust, con el apoyo de las autoridades judiciales y policiales de más de una docena de países, llevaron a cabo una operación global coordinada contra el colectivo pro-ruso de hacktivistas y ciberdelincuentes NoName057(16), incautando más de 100 servidores en todo el mundo y emitiendo múltiples órdenes de detención contra los principales sospechosos relacionados con las actividades de denegación de servicio distribuido (DDoS) del grupo. La operación también supuso notificar a cientos de simpatizantes su posible responsabilidad legal por colaborar en los ataques DDoS y representó una de las acciones multinacionales más amplias dirigidas contra redes de ciberdelincuencia con motivaciones ideológicas hasta la fecha.[27]

Aunque las autoridades pretendían perturbar significativamente las operaciones y la infraestructura de NoName057(16), los informes posteriores indican que el grupo no quedó inhabilitado de forma permanente. Inmediatamente después de Eastwood, NoName057(16) minimizó públicamente el impacto en sus canales de Telegram y continuó publicando listas diarias de objetivos durante la propia operación, lo que demuestra que siguió activo a pesar de la presión policial. En los días posteriores al desmantelamiento, el grupo experimentó una breve pausa operativa entre el 18 y el 22 de julio, lo que probablemente reflejaba los reveses sufridos por su infraestructura. Sin embargo, el 23 de julio de 2025, NoName057(16) emitió una respuesta desafiante en la que declaraba que Eastwood había fracasado y anunciaba una campaña denominada «Tiempo de retribución»/«Tiempo de represalias», en la que instaba a sus seguidores a reanudar y ampliar los ataques contra los Estados que habían participado en la operación. Durante las semanas siguientes, hasta finales de agosto, la actividad observada por el colectivo no solo se reanudó, sino que, según algunos análisis, aumentó en volumen en comparación con los niveles anteriores a Eastwood, incluyendo ataques contra múltiples objetivos europeos.[28]

Este patrón, una importante perturbación internacional seguida de una actividad resistente y escalada, proporciona el contexto estratégico para la segunda ola de operaciones hacktivistas que afectan a las organizaciones españolas. En lugar de disuadir la participación hacktivista, la Operación Eastwood parece haber sido aprovechada por los actores alineados con Rusia como una narrativa de movilización y un impulso para intensificar sus campañas, lo que contribuyó a la reanudación de los ataques durante julio y agosto de 2025.



Mensaje de regreso de NoName057(16) tras la Operación Eastwood.

[26] Europol, Operación global contra la red de ciberdelincuencia prorrusa NoName057(16), disponible aquí: https://www.europol.europa.eu/media-press/newsroom/news/global-operation-targets-noname05716-pro-russian-cybercrime-network, julio de 2025.

[27] Eurojust, Desmantelado el grupo hacktivista responsable de ciberataques contra infraestructuras críticas en Europa, disponible aquí: https://www.eurojust.europa.eu/news/hacktivist-group-responsible-cyberattacks-critical-infrastructure-europe-taken-down, 16 de julio de 2025.

[28] Imperva, Operación Eastwood: medición del impacto real sobre NoName057(16), disponible aquí: https://www.imperva.com/blog/operation-eastwood-measuring-the-real-impact-on-noname05716/, 12 de septiembre de 2025

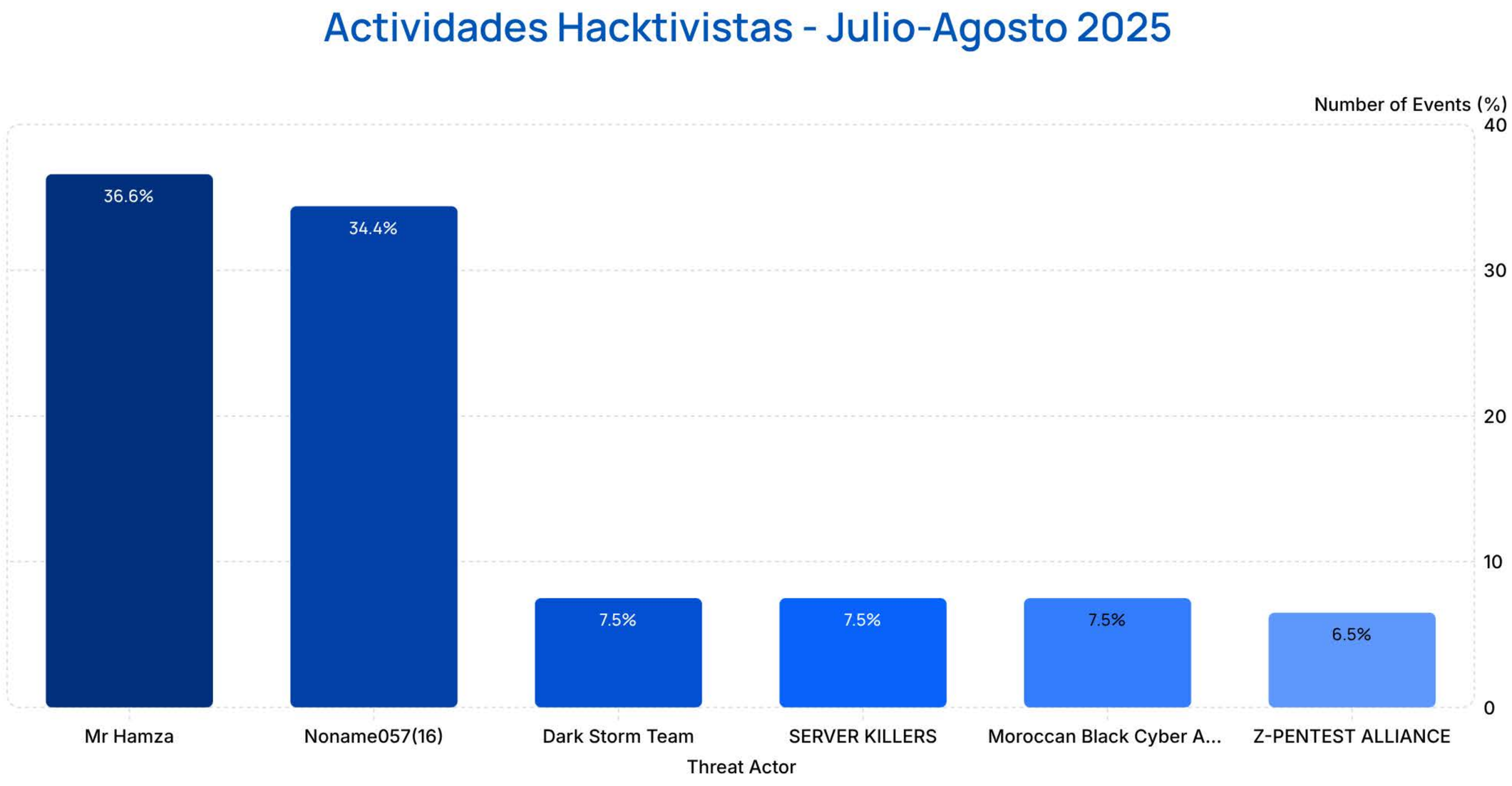
Conclusión clave:

La Operación Eastwood, a pesar de representar una de las interrupciones multinacionales más significativas de las fuerzas del orden contra las redes hacktivistas prorrusas hasta la fecha, no produjo una degradación duradera de la capacidad operativa de NoName057(16). En cambio, la acción policial se reformuló rápidamente como una narrativa de movilización, lo que desencadenó un aumento de las represalias en forma de actividades DDoS en toda Europa. Este patrón subraya la resistencia estructural de los ecosistemas hacktivistas descentralizados e impulsados por ideologías, en los que la incautación de infraestructuras puede causar una interrupción temporal, pero tiene un efecto disuasorio limitado a largo plazo.

Esta escalada provocada por las medidas policiales proporciona el contexto operativo para la segunda ola de actividad hacktivista que afectó a organizaciones españolas entre julio y agosto de 2025.

Entre julio y agosto, el equipo YCTI observó seis colectivos hacktivistas que tenían como objetivo organizaciones españolas:

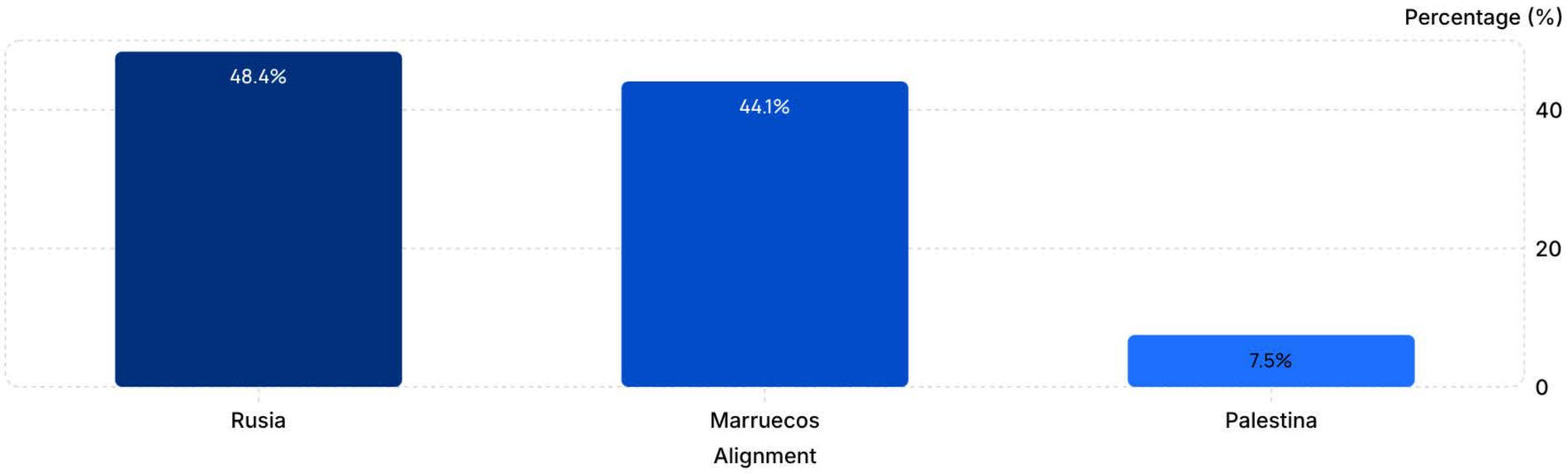
ID	Threat Actor – Segunda Ola	Número de eventos %	Alineación declarada o evaluada
1	Mr Hamza	36,6%	Marruecos
2	Noname057(16)	34,4%	Rusia
3	Dark Storm Team	7,5%	Rusia
4	SERVER KILLERS	7,5%	Russia
5	Moroccan Black Cyber Army	7,5%	Marruecos
6	Z-PENTEST ALLIANCE	6,5%	Rusia
TOTAL EVENTOS REGISTADOS	**100%**	-	-



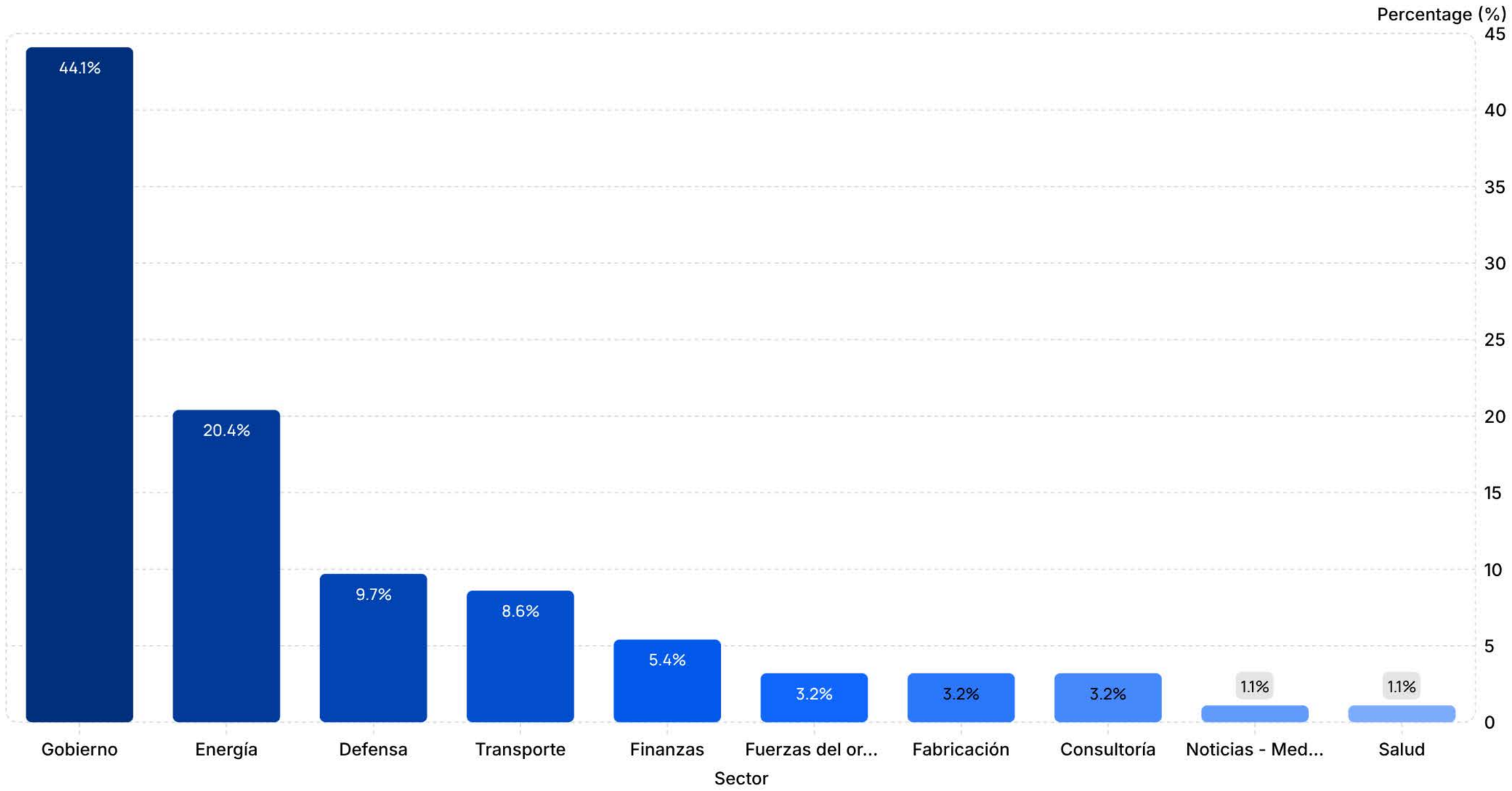
La siguiente tabla contiene la distribución de los actores maliciosos observados durante la segunda ola, agrupados según la alineación declarada o evaluada:

Alineamiento Hacktivista - Julio-Agosto 2025

ID	Alineación declarada o evaluada	Número de eventos (%)	Número de Threat Actors
1	Rusia	48,4%	3
2	Marruecos	44,1%	2
3	Palestina	7,5%	1
TOT	**3 Alignments**	**100%**	**6**



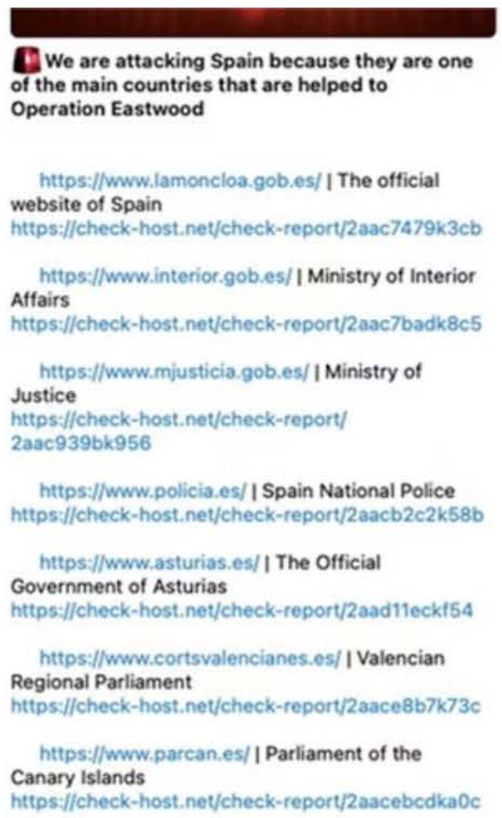
La segunda ola de actividades hacktivistas afectó a diez sectores.



El predominio de los objetivos gubernamentales (44,1 %) y energéticos (20,4 %) indica una priorización deliberada de sectores políticamente simbólicos y estratégicamente sensibles. Las entidades gubernamentales representan objetivos de alta visibilidad capaces de amplificar la resonancia mediática y reforzar las narrativas geopolíticas, mientras que el sector energético constituye una infraestructura crítica con un fuerte valor psicológico y económico. La concentración de la actividad contra estos sectores sugiere que el objetivo de la segunda oleada no era tanto la interrupción operativa sostenida como la transmisión de mensajes estratégicos, la señalización de represalias y la proyección de una capacidad continuada tras la Operación Eastwood. Este patrón de objetivos es coherente con las campañas de DDoS orientadas a la influencia llevadas a cabo históricamente por colectivos hacktivistas prorrusos.

Segunda oleada: prueba de las afirmaciones de los hacktivistas

En esta sección se ofrecen ejemplos de las afirmaciones realizadas por grupos hacktivistas identificados por el equipo CTI a partir de canales privados de dichos grupos.



> **«Server Killers»**
>
> **Traducción de la publicación original**: 'Estamos atacando a España porque es uno de los principales países que están ayudando a la Operación Eastwood.'

> **«Equipo Dark Storm»**
>
> **Traducción de la publicación original**: 'Estamos atacando a España porque es uno de los principales países que están ayudando a la Operación Eastwood.'

Post original: Количество публикаций в СМИ и соцмедиа о нашей команде за последние несколько дней бьет все рекорды. Западные русофобы, их продажные политики и спецслужбы, пресмыкающиеся к ним бандеровские недобитки всех мастей нестройным хором фальшиво поют песни о том, что они "разгромили" группировку NoName057(16).

Смешно наблюдать за тем, как спецслужбы 12 западных стран на деньги своих налогоплательщиков несколько лет вели "расследование" о том, как русские хакеры из NoName057(16) создали целую империю киберборьбы за правду, в том числе и у них под боком.

Все эти годы они тщетно пытались победить правду, которая стоит за нами и даже поверили в то, что им это удалось. Они хвастаются своей никчемной операцией Eastwood, которая не только не смогла остановить нас, но даже наоборот - Запад в очередной расписался в эффективности NoName057(16) и теперь мы будем атаковать русофобов с новыми силами.

Сегодня мы начинаем операцию "Время возмездия". Мы призываем всех наших единомышленников по всему миру присоединиться к ней. Мы придем к каждому, кто пытался противодействовать нам и нанесем еще больше ущерба экономикам недружественных России стран. Мы живее всех живых!

Победа будет за нами. Враг будет разбит! Слава России!

#FuckEastwood #TimeOfRetribution

> **Traducción** : "El número de publicaciones en medios de comunicación y redes sociales sobre nuestro equipo en los últimos días bate todos los récords. Los rusófobos occidentales, sus políticos vendidos y los servicios especiales que se arrastran ante ellos, así como todo tipo de restos banderistas, cantan al unísono una melodía falsa diciendo que "derrotaron" al grupo NoName057(16).
>
> Resulta cómico observar cómo los servicios especiales de 12 países occidentales, utilizando el dinero de sus contribuyentes, llevan varios años realizando una "investigación" sobre cómo hackers rusos de NoName057(16) crearon todo un imperio de ciberguerra por la verdad, incluso justo delante de sus narices.
>
> Durante todos estos años han intentado en vano derrotar la verdad que está detrás de nosotros e incluso llegaron a creer que lo habían conseguido. Presumen de su inútil Operación Eastwood, que no solo no logró detenernos, sino que, por el contrario, Occidente ha vuelto a reconocer la eficacia de NoName057(16), y ahora atacaremos a los rusófobos con nueva fuerza.
>
> Hoy lanzamos la Operación "Tiempo de Retribución". Llamamos a todos nuestros afines en todo el mundo a unirse. Iremos a por todos los que intentaron oponerse a nosotros y causaremos aún más daños a las economías de los países hostiles a Rusia. Estamos más vivos que nunca.
>
> La victoria será nuestra. ¡El enemigo será derrotado! ¡Gloria a Rusia!
>
> #FuckEastwood #TimeOfRetribution "

5.d.iii. Tercera ola: inclusión de «Desinformador ruso» en la lista de los más buscados de la UE y aplicación de la ley

> **Highlight – Tercera ola:** La exposición de un canal de amplificación con base en España («Desinformador Ruso»), vinculado a NoName057(16) dentro de la lista de los más buscados de la UE, actuó como un catalizador de movilización, reforzando la cohesión narrativa dentro de la red prorrusa y permitiendo una campaña altamente centralizada y orientada a la influencia, dirigida contra instituciones gubernamentales españolas, en la que los canales alineados con el hacktivismo combinaron la disrupción técnica con la desinformación y la gestión de la percepción para moldear la opinión pública nacional.

La tercera ola parece haberse coaligado en torno a un único caso nacional de gran visibilidad, transformando una acción policial en un punto focal para la renovada movilización hacktivista.

Se considera que la tercera ola de actividad hacktivista dirigida contra entidades españolas está estrechamente relacionada con la identificación pública y la posterior inclusión en la lista de los más buscados de la UE de Enrique Arias Gil, presuntamente asociado al canal de Telegram «Desinformador Ruso». El canal funcionaba principalmente como una plataforma de amplificación en español para las operaciones hacktivistas prorrusas, republicando y promoviendo sistemáticamente las reivindicaciones de los ataques (sobre todo las de NoName057(16)), al tiempo que retransmitía las actividades atribuidas a otros colectivos afines, como TwoNet, Anonymous Russia y PalachPro.

El seguimiento de la CTI indica que «Desinformador Ruso» operaba menos como un actor operativo directo y más como un nodo de amplificación mediática, mejorando la visibilidad, la legitimidad y el impacto percibido de las campañas de DDoS y desfiguración llevadas a cabo contra objetivos españoles y europeos. El predominio de los contenidos en español sugiere un enfoque deliberado en influir en el público nacional y reforzar las narrativas dentro de España.

En septiembre de 2025, Europol incluyó públicamente a Arias Gil en la plataforma «Los más buscados de la UE». Según las informaciones, la investigación, a cargo de la unidad española ENFAST (Red Europea de Equipos de Búsqueda Activa de Fugitivos), se refiere a acusaciones que incluyen daños informáticos con intención terrorista, glorificación del terrorismo y participación en una organización criminal. La exposición pública de un presunto facilitador nacional vinculado a NoName057(16) elevó significativamente la visibilidad del caso y reforzó la percepción de que existen estructuras de apoyo internas alineadas con las campañas hacktivistas prorrusas.

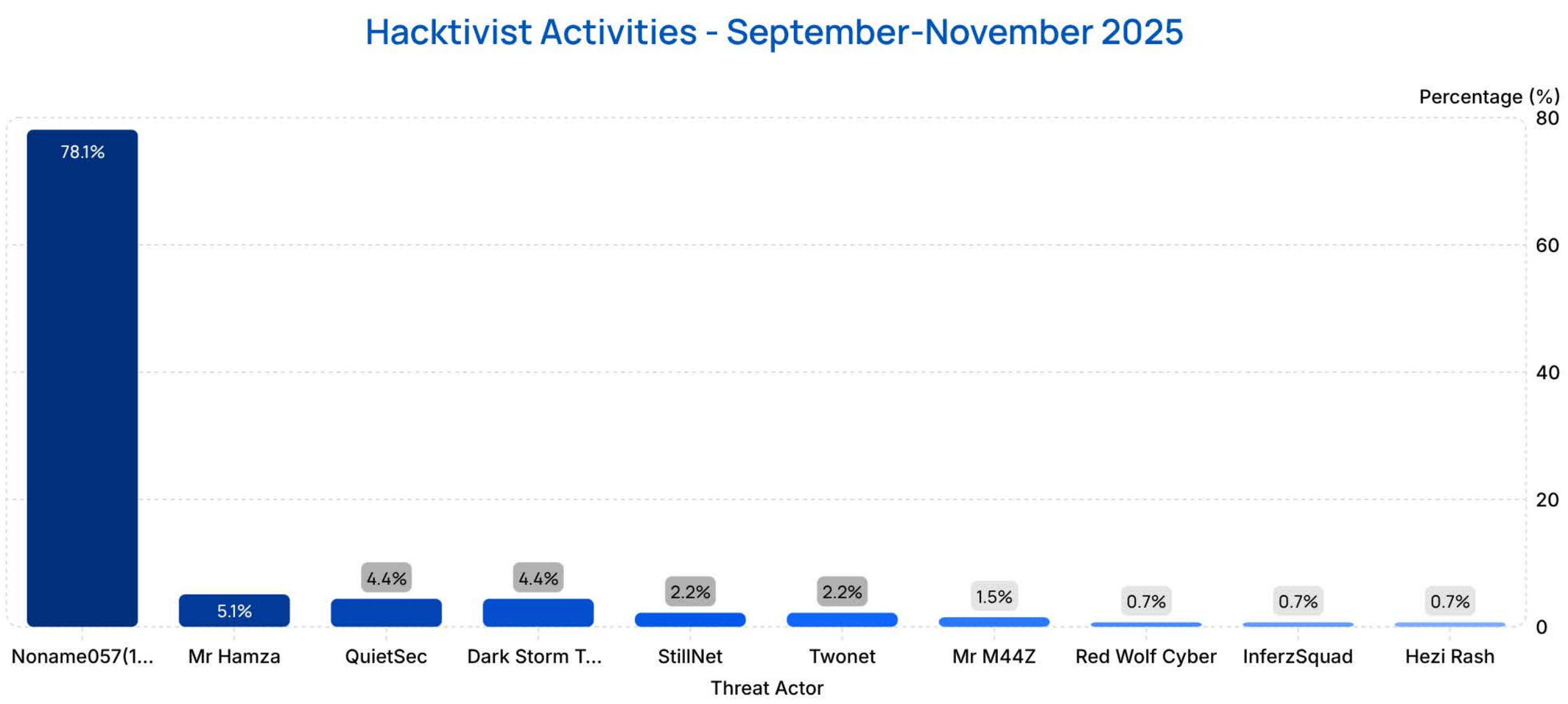
En este contexto, la tercera ola muestra un perfil operativo marcadamente concentrado. NoName057(16) representó el **78,1 %** de los eventos registrados durante el periodo, superando con creces a todos los demás colectivos observados. Esta concentración sugiere una campaña impulsada principalmente por un único actor dominante, en lugar de un aumento oportunista y ampliamente distribuido. La distribución de la alineación refuerza aún más esta valoración, ya que el **87,6 %** de los eventos se atribuyen a actores alineados con Rusia.

Conclusión clave:

La tercera oleada indica que la exposición de un amplificador de narrativas con base nacional vinculado a NoName057(16) actuó como catalizador de la movilización, en lugar de como elemento disuasorio. La inclusión en la lista de los más buscados de la UE parece haber reforzado la cohesión narrativa dentro del ecosistema hacktivista prorruso, contribuyendo a una campaña altamente centralizada y orientada a la influencia dirigida a las instituciones gubernamentales españolas.

Entre septiembre y noviembre de 2025, el equipo YCTI observó 10 colectivos hacktivistas que tenían como objetivo organizaciones españolas:

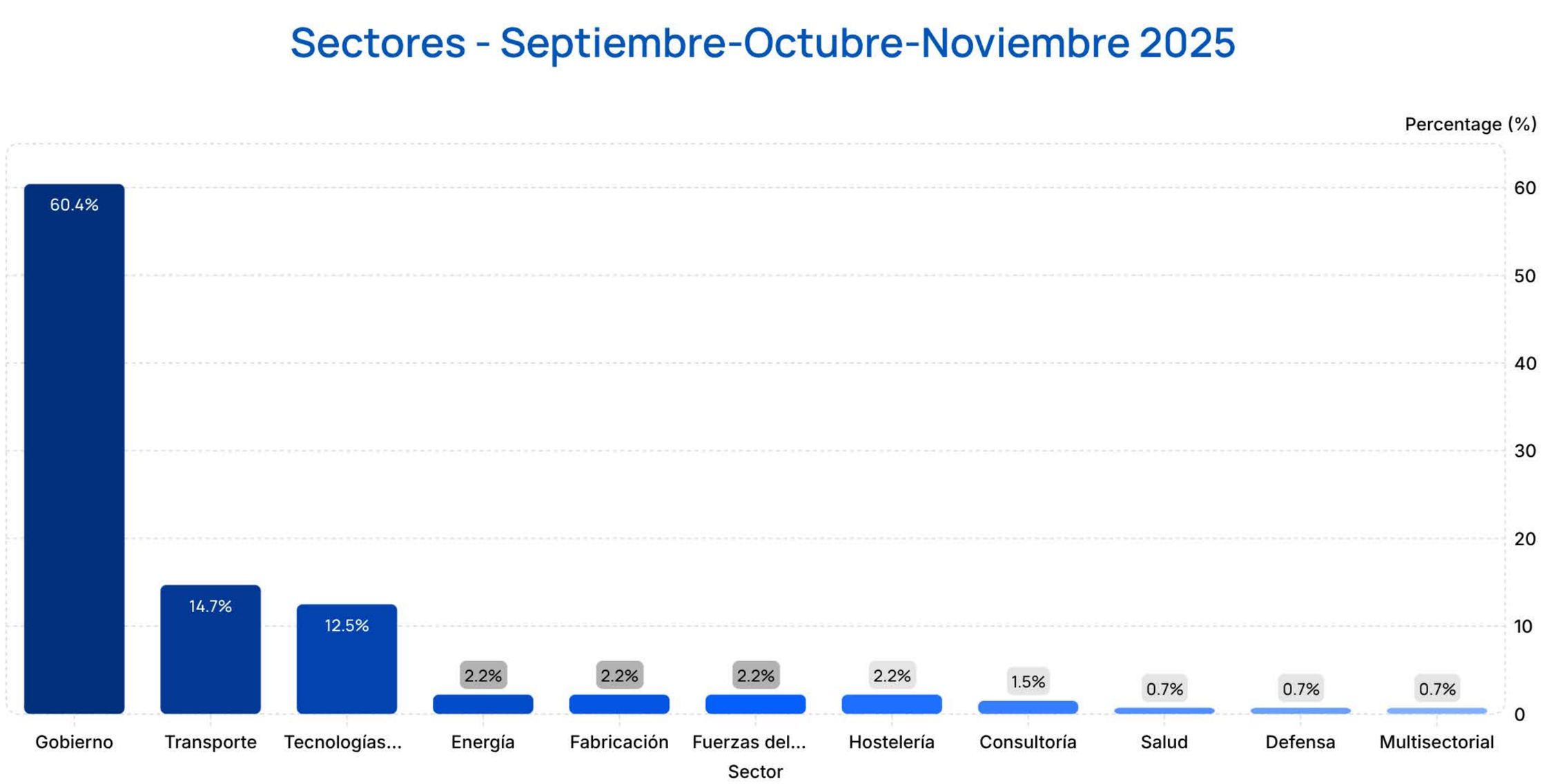
ID	Threat Actor – Tercera Ola	Número de eventos %	Alineación declarada o evaluada
1	Noname057(16)	78,1%	Rusia
2	Mr Hamza	5,1%	Marruecos
3	QuietSec	4,4%	Rusia
4	Dark Storm Team	4,4%	Palestina
5	StillNet	2,2%	Rusia
6	Twonet	2,2%	Rusia
7	Mr M44Z	1,5%	Anónimo
8	Red Wolf Cyber	0,7%	Rusia
9	InferzSquad	0,7%	España
10	Hezi Rash	0,7%	Kurdistan
TOT	-	**100%**	-



La siguiente tabla contiene la distribución de los actores de amenaza observados durante la tercera oleada, agrupados por alineación:

ID	Alineación declarada o evaluada	Número de eventos %	Número de actores maliciosos
1.	Rusia	87,6%	5
2.	Marruecos	5,1%	1
3.	Palestina	4,4%	1
4.	Anónimo	1,5%	1
5.	España	0,7%	1
6.	Kurdistán	0,7%	1
TOT	**6 Alineaciones**	**100%**	**10**

La tercera ola de actividades hacktivistas afectó a once sectores.



El predominio de los objetivos gubernamentales (60,4 %) indica un enfoque deliberado en instituciones políticamente simbólicas y de gran visibilidad, en consonancia con la actividad hacktivista diseñada para maximizar la resonancia mediática, la presión sobre la reputación y la señalización política, en lugar de provocar una interrupción operativa sostenida. El importante número de ataques dirigidos al transporte (14,7 %) y a las tecnologías de la información (12,5 %) sugiere además un esfuerzo por extender las narrativas de perturbación a los servicios de cara al público y a la infraestructura digital habilitadora, amplificando la percepción del alcance del impacto y manteniendo al mismo tiempo un énfasis en las instituciones estatales. Este patrón de ataques es coherente con las campañas de DDoS orientadas a la influencia llevadas a cabo históricamente por colectivos hacktivistas prorrusos, en las que los mensajes estratégicos y las señales políticas superan a los efectos técnicos sostenidos.

Respuesta narrativa y amplificación mediática: #OpMortadelos

Tras la publicación del aviso de Europol, el canal de Telegram «Desinformador Ruso» pasó rápidamente a una campaña abierta orientada a los medios de comunicación con el objetivo de replantear la acción policial como una persecución política. Desde el día de la inclusión en la lista, el canal lanzó la etiqueta *#OpMortadelos*, difundiendo publicaciones coordinadas que presentaban a las autoridades españolas como corruptas, controladas por los atlantistas y comprometidas en una «caza de brujas» contra las voces disidentes.

En lugar de negar su alineación con NoName057(16), los mensajes del canal buscaban deslegitimar la investigación mediante el encuadre de victimismo, la retórica conspirativa y los insultos directos contra las instituciones de seguridad españolas. Paralelamente, las publicaciones amplificaban narrativas prorrusas más amplias, incluidas afirmaciones sobre actividades de inteligencia ucraniana en España, lo que situaba el caso en un espacio de información geopolítica más amplio.

Pruebas del canal de Telegram Desinformador Ruso – Fuente: Equipo CTI de Yarix

Esta rápida transición de la exposición de la aplicación de la ley a la escalada narrativa refuerza la valoración de que «Desinformador Ruso» funcionó como un nodo de influencia y amplificación dentro del ecosistema hacktivista prorruso. La campaña ilustra cómo los canales afiliados a los hacktivistas pueden complementar la interrupción técnica (DDoS/defacements) con la desinformación y la gestión de la percepción, con el objetivo de mantener la movilización y moldear la opinión pública nacional durante los periodos de mayor atención política.

En conjunto, esto sugiere que la amplificación narrativa y los ataques simbólicos se reforzaron mutuamente para mantener la movilización, con operaciones de información y ataques de alta visibilidad contra el Gobierno que funcionaron como componentes complementarios de una campaña centralizada orientada a la influencia.

Tercera ola: prueba de las afirmaciones de los hacktivistas

Las siguientes secciones proporcionan ejemplos de las afirmaciones realizadas por varios grupos hacktivistas durante el periodo de tiempo considerado e identificadas por el equipo CTI a partir de canales privados de los grupos hacktivistas.

Sever Killers

Transcripción de la publicación: *"Estamos atacando a España porque es uno de los principales países que han apoyado la Operación Eastwood.*

https://... | Sitio web oficial de España

https://... | Ministerio del Interior

https://... | Ministerio de Justicia

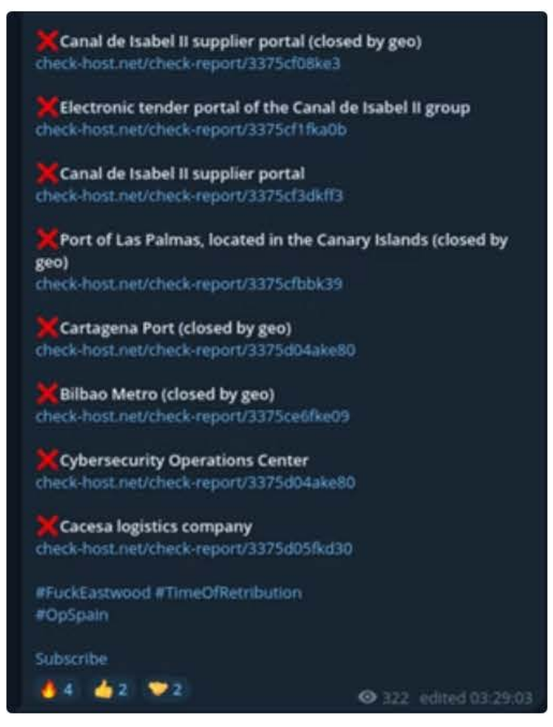
https://... | Policía Nacional de España

https://... | Gobierno del Principado de Asturias

https://... | Parlamento de la Comunidad Valenciana

https://... | Parlamento de Canarias'"

NoName057(16)



Transcripción de la publicación: "*Más regalos DDoS para España*

Portal de proveedores del Canal de Isabel II (cerrado por geolocalización)
check-host.net...

Portal de licitaciones electrónicas del grupo Canal de Isabel II
check-host.net...

Portal de proveedores del Canal de Isabel II
check-host.net...

Puerto de Las Palmas, situado en las Islas Canarias (cerrado por geolocalización)
check-host.net...

Puerto de Cartagena (cerrado por geolocalización)
check-host.net...

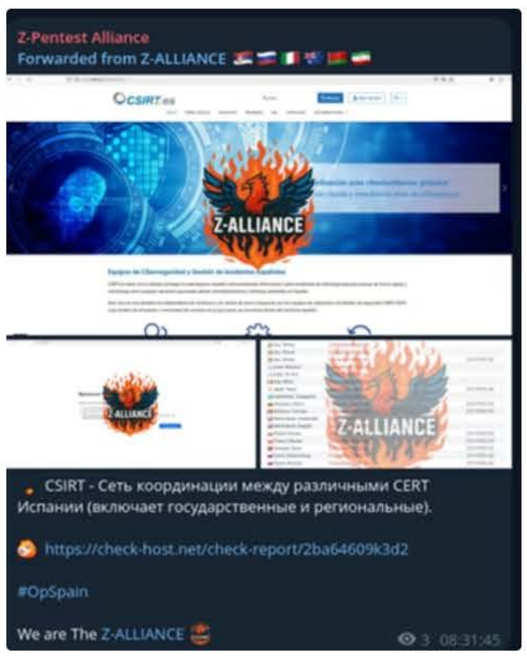
Metro de Bilbao (cerrado por geolocalización)
check-host.net...

Centro de Operaciones de Ciberseguridad
check-host.net...

Empresa logística Cacesa
check-host.net...

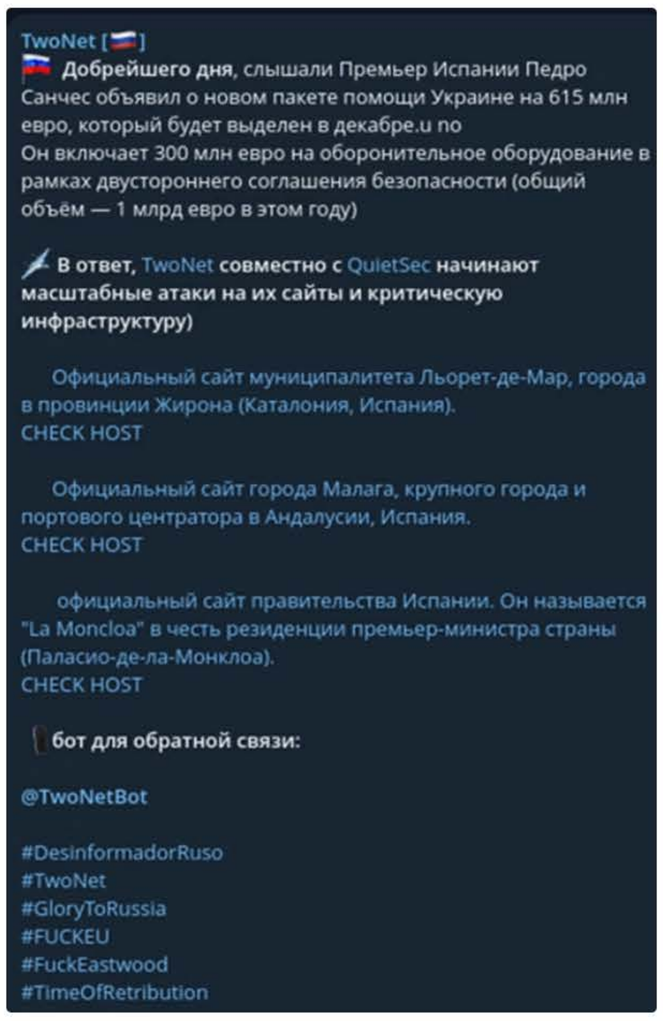
#FuckEastwood #TimeOfRetribution #OpSpain

Alianza Z-Pentest



> ***Original Post:*** *CSIRT - Red de coordinación entre различными CERT España (incluye estatales y regionales). https://... #OpSpain Somos The Z-ALLIANCE*
>
> ***Traducción automática:*** *CSIRT - Red de coordinación entre los distintos CERT de España (incluye los estatales y autonómicos). https://...*

Two Net



> ***Original Post:*** *“Добрейшего дня, слышали Премьер Испании Педро Санчес объявил о новом пакете помощи Украине на 615 млн евро, который будет выделен в декабре.и по Он включает 300 млн евро на оборонительное оборудование в рамках двустороннего соглашения безопасности (общий объём 1 млрд евро в этом году)*
>
> *В ответ, TwoNet совместно с QuietSec начинают масштабные атаки на их сайты и критическую инфраструктуру)*
>
> *Официальный сайт муниципалитета Льорет-де-Мар, города в провинции Жирона (Каталония, Испания).*
> *CHECK HOST*
>
> *Официальный сайт города Малага, крупного города и портового центратора в Андалусии, Испания.*
> *CHECK HOST*
>
> *официальный сайт правительства Испании. Он называется "La Moncloa" в честь резиденции премьер-министра страны (Паласио-де-ла-Монклоа).*
> *CHECK HOST*
>
> *бот для обратной связи:*
>
> *@TwoNetBot*
>
> *#Desinformador Ruso #TwoNet #GloryToRussia #FUCKEU #FuckEastwood #TimeOfRetribution”*

Traducción automática: “«Buenas tardes, ¿os habéis enterado? El presidente del Gobierno de España, Pedro Sánchez, anunció un nuevo paquete de ayuda a Ucrania por valor de 615 millones de euros, que se asignará en diciembre. Incluye 300 millones de euros en equipamiento de defensa en el marco del acuerdo bilateral de seguridad (importe total este año: 1.000 millones de euros).

En respuesta, TwoNet, junto con QuietSec, lanza ataques a gran escala contra sus sitios web y su infraestructura crítica.

Sitio web oficial del municipio de Lloret de Mar, ciudad de la provincia de Girona (Cataluña, España). CHECK HOST

Sitio web oficial de la ciudad de Málaga, una gran ciudad y centro portuario de Andalucía, España. CHECK HOST

Sitio web oficial del Gobierno de España. Se denomina «La Moncloa», en referencia a la residencia del presidente del país (Palacio de la Moncloa). CHECK HOST

bot de contacto: @TwoNetBot

#DesinformadorRuso #TwoNet #GloryToRussia #FUCKEU #FuckEastwood #TimeOfRetribution»

6. Consideraciones finales

A continuación se presentan algunas ideas sobre las seis categorías principales de amenazas cibernéticas observadas, junto con hipótesis sobre posibles escenarios de amenazas a la ciberseguridad en España para 2026:

Denegación de servicio distribuida (DDoS) y desfiguración web – ALTO

En 2025, las operaciones de DDoS y desfiguración web impulsadas por hacktivistas representaron la principal amenaza que afectó a las organizaciones españolas, con un 38,6 % del total de incidentes registrados por la telemetría CTI. La actividad se asoció en gran medida con actores que mostraban mensajes alineados con Rusia, que representaron el 65,9 % de los incidentes hacktivistas, seguidos por mensajes alineados con Marruecos o más amplios a favor de los árabes y los musulmanes. El sector más afectado fue el gubernamental, seguido del transporte, la defensa, la energía y las tecnologías de la información, lo que indica una clara preferencia por objetivos políticamente simbólicos. La cronología muestra tres picos principales de actividad hacktivista durante marzo de 2025, julio y agosto de 2025, y septiembre, octubre y noviembre de 2025. Estos picos coincidieron temporalmente con acontecimientos de gran visibilidad en la política interior y exterior, así como con operaciones policiales contra ecosistemas hacktivistas prorrusos, incluida la Operación Eastwood y los posteriores acontecimientos relacionados con la aplicación de la ley.

Data Leakage (Fuga de datos) - ALTO

En 2025, la fuga de datos representó el 21,1 % del total de incidentes registrados contra organizaciones españolas, lo que la convierte en la segunda categoría de amenazas más frecuente. Los sectores más afectados fueron el financiero (19,4 %), el energético (13,1 %) y el minorista (12,6 %), seguidos por el sanitario, el informático y el gubernamental, lo que pone de relieve la exposición tanto de la economía como de los servicios públicos. La distribución entre 18 sectores sugiere que la actividad de fuga de datos no se limita a un solo sector vertical e incluye tanto compromisos oportunistas como específicos. La presencia de múltiples actores y canales clandestinos, incluida una parte significativa «desconocida», indica que la atribución sigue siendo un reto y que la amenaza se ve facilitada por un amplio ecosistema de vendedores y corredores.

Ransomware - ALTO

En 2025, el ransomware representó el 18,1 % del total de ciberamenazas registradas contra organizaciones en España. A nivel mundial, España se situó entre los 10 primeros países con más incidentes de ransomware en 2025, lo que supone el 2,10 % del total registrado por el equipo CTI. La amenaza del ransomware en España se caracterizó por una alta fragmentación del ecosistema, con 40 bandas de ransomware observadas atacando a entidades españolas durante el año. Los grupos de ransomware más activos fueron Qilin (22,0 %) y Akira (10,0 %), seguidos de varios actores con cuotas menores, lo que indica un panorama competitivo y diversificado. En cuanto al perfil de las víctimas, el ransomware afectó principalmente a pequeñas empresas (66,0 %), seguidas de organizaciones medianas (21,3 %), grandes empresas (5,3 %), grandes (4,7 %) y microempresas (2,7 %). Por sectores, los más afectados fueron la industria manufacturera (15,3 %), el comercio minorista y el comercio electrónico (14,0 %), la consultoría (12,0 %) y la hostelería (10,7 %), lo que sugiere que las industrias con una gran intensidad operativa y dependientes de los servicios siguen estando muy expuestas.

Agentes de acceso inicial (IAB) – MEDIO

En 2025, la amenaza de los agentes de acceso inicial representó el 12,3 % de los incidentes registrados contra entidades en España. Debido a la naturaleza de este mercado, más de la mitad de los casos registrados estaban asociados a sectores desconocidos o no revelados (51,0 %), lo que refleja las prácticas deliberadas de seguridad operativa de los autores de las amenazas, que a menudo solo revelan los detalles de las víctimas a compradores acreditados. Entre los casos revelados, los más representados fueron el comercio minorista y el comercio electrónico (11,8 %), la consultoría (5,7 %), la fabricación (5,7 %) y las tecnologías de la información y la administración pública (3,9 % cada uno). Dado su papel como facilitador clave de las actividades de ransomware e intrusión, la actividad de los IAB representa una importante amenaza precursora, especialmente cuando se combina con pruebas de colaboración recurrente entre los brokers de acceso y los grupos de ransomware.

Leads – BAJO

La amenaza Leads representó el 6,2 % del total de eventos monitorizados en 2025 contra organizaciones en España. La amenaza se concentró principalmente en el sector financiero (62,6 %), mientras que una parte significativa siguió siendo desconocida o no se reveló, lo que refleja las limitaciones a la hora de identificar de forma fiable el origen de los conjuntos de datos agregados de leads. Aunque la proporción global es menor en comparación con otras categorías, los leads pueden facilitar el fraude, el relleno de credenciales, el phishing y la ingeniería social, lo que afecta especialmente a los consumidores y a las funciones de atención al cliente.

Acceso no autorizado – BAJO

Los incidentes de acceso no autorizado representaron el 3,7 % del total de incidentes registrados en 2025 contra entidades españolas. Los sectores más afectados fueron el de la energía y los servicios públicos (29,0 %), el desconocido o no revelado (19,3 %) y el de la agricultura y la producción alimentaria (19,3 %). La distribución de los actores indica una actividad repetida por parte de un conjunto limitado de grupos y canales, lo que sugiere que esta categoría de amenaza puede reflejar tanto intrusiones de tipo hacktivista como compromisos oportunistas de servicios expuestos. Aunque la proporción de incidentes es relativamente pequeña, la concentración en sectores vinculados a infraestructuras críticas justifica un seguimiento continuo.

Informe Nacional Sobre el Panorama de Las Amenazas Cibernéticas
España 2025

YARIX

Protege lo que más importa.
Descubre nuestros servicios en
www.yarix.com

Yarix, la marca de ciberseguridad de Var Group, es un proveedor internacional de confianza en servicios avanzados de seguridad. Fundada en 2001, apoya a organizaciones públicas y privadas de diversos sectores en la protección de sus activos digitales y en la continuidad operativa en entornos complejos y en constante evolución. A través de un enfoque integral que combina tecnologías avanzadas, experiencia especializada y un Security Operations Center global activo 24/7, Yarix ofrece protección proactiva, monitorización continua y una rápida respuesta ante incidentes, permitiendo a las organizaciones operar con seguridad y acelerar su transformación digital.