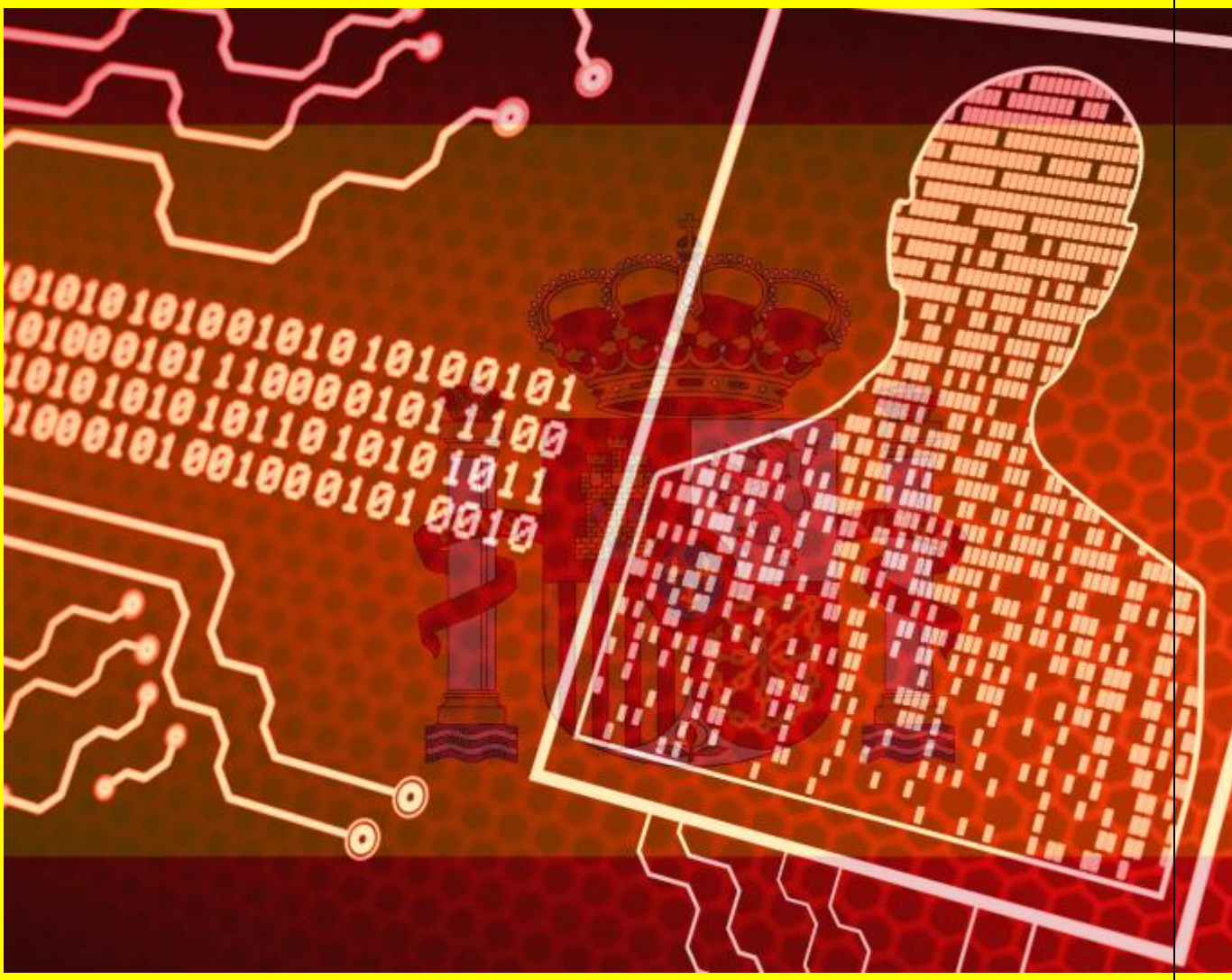
Ciberataques rusos contra España: una ofensiva silenciosa con fines estratégicos



Almudena de la Encarnación Bedoya

19 de marzo de 2025

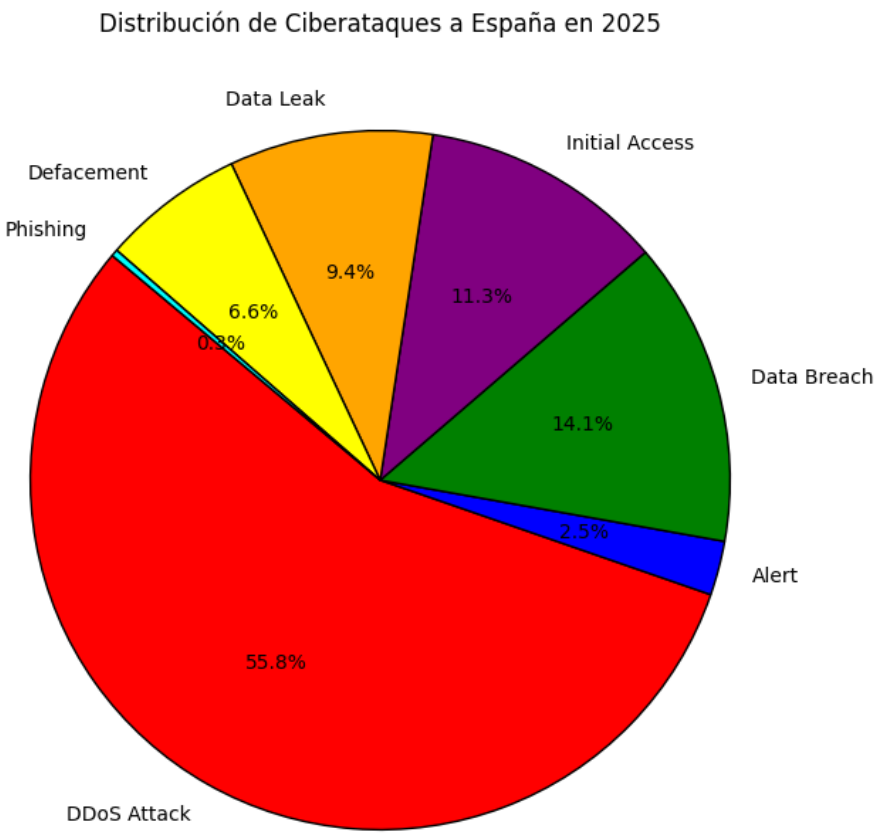
Almudena de la Encarnación Bedoya
Máster Profesional en Analista de Inteligencia de LISA Institute. Analista de Inteligencia especializada en OSINT, ciberinteligencia y detección de fraude.

Experta en la explotación de fuentes abiertas para la investigación y toma de decisiones estratégicas, con experiencia en la detección y análisis de amenazas digitales. Formadora en la creación de departamentos de inteligencia y detección de fraude, y participante en programas de bug bounty. Miembro activo en iniciativas de búsqueda de personas desaparecidas mediante OSINT y en desarrollo de soluciones de ciberseguridad e identidades digitales para la protección ante filtraciones de datos.

España se ha convertido en un objetivo prioritario de ciberataques, con una creciente ofensiva contra infraestructuras críticas y organismos gubernamentales. En este artículo, la alumni del Máster Profesional de Analista de Inteligencia de LISA Institute, Almudena de la Encarnación, analiza como grupos vinculados a Rusia buscan desestabilizar y generar incertidumbre.

Desde que comenzó la invasión rusa a Ucrania en 2022, España ha sido un firme defensor del gobierno ucraniano, brindando apoyo diplomático, humanitario y militar. Esta postura ha puesto al país en la mira de actores hostiles, especialmente de Rusia. Moscú ha utilizado el ciberespacio como un campo de batalla adicional en su guerra híbrida.

En los últimos meses, los ciberataques contra infraestructuras críticas y entidades gubernamentales españolas se han intensificado. Esto revela una estrategia bien organizada para desestabilizar y desviar la atención de la nación ibérica.



En el contexto actual de los conflictos bélicos, el ciberespacio se ha convertido en un campo de guerra fundamental. No es solo un terreno de enfrentamiento entre grandes potencias, sino también un medio para ejecutar acciones invisibles y difíciles de atribuir.

Los ciberataques de actores no estatales, como los grupos de hackers, son frecuentes. Sin embargo, los ataques provenientes de estados nación están adquiriendo una dimensión más compleja. No solo buscan desorganizar sociedades desde dentro, sino también enviar mensajes políticos, influir en decisiones gubernamentales y sembrar discordia en las relaciones internacionales.

➞ Te puede interesar: Las 10 empresas referentes en ciberseguridad en España

En el caso de España, su postura favorable a Ucrania, un aliado clave en la región, la ha convertido en un blanco prioritario de ciberataques. En particular, los ataques rusos forman parte de una estrategia más amplia de desestabilización política y militar a través de medios no convencionales.

Uno de los métodos más comunes que se han utilizado en los ataques rusos contra España es el ataque de denegación de servicio distribuido (DDoS). Aunque estos ataques no suelen comprometer la integridad de la información, generan un impacto significativo. Sobrecargan los servidores de las víctimas con una cantidad masiva de peticiones, provocando la caída temporal de los servicios afectados.

Recientemente, varios ministerios y organismos gubernamentales españoles han sido víctimas de estos ataques. Las entidades que han sufrido las consecuencias de estos ataques incluyen:

- **Ministerio de Cultura y Deporte (mcu.es)**
- **Ministerio de Ciencia e Innovación (ciencia.gob.es)**
- **Ministerio de Asuntos Exteriores (exteriores.gob.es)**
- **Servicio de emergencias 112 (112.es)**
- **Y otros más…**

Si bien estos ataques no comprometen directamente la confidencialidad de los datos, interrumpen la disponibilidad de servicios críticos tanto para los ciudadanos como para la administración pública. Este tipo de ataque tiene un objetivo claro: perturbar las operaciones gubernamentales, crear confusión y debilitar la percepción de fiabilidad del gobierno ante la ciudadanía.

Herramientas y tácticas utilizadas en los ciberataques

Los ciberataques DDoS se han ejecutado utilizando una variedad de herramientas y tácticas. Los atacantes suelen recurrir a redes de bots (botnets), que son grupos de dispositivos infectados controlados remotamente. Estos dispositivos incluyen ordenadores personales, servidores y otros equipos conectados a la red. Sin el conocimiento de sus propietarios, se utilizan para realizar ataques masivos.

➡ Te puede interesar: Guía para las empresas sobre cómo actuar ante un ciberataque

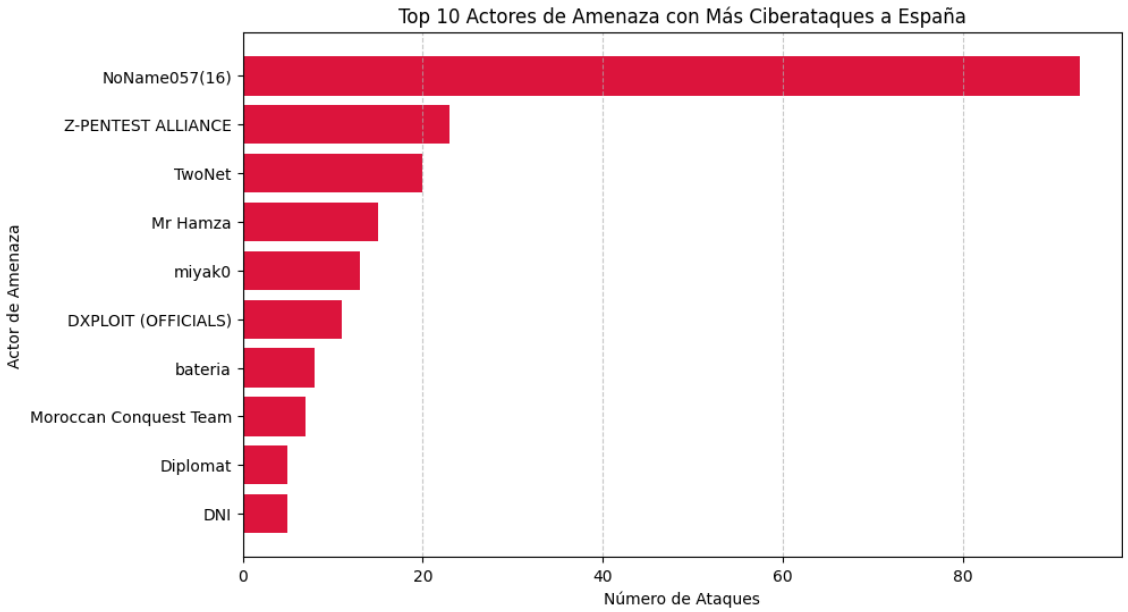
Además, en ocasiones se emplean técnicas de amplificación de ataques, donde el volumen de tráfico se incrementa aprovechando vulnerabilidades en servidores de DNS o protocolos de amplificación. Esto permite a los atacantes generar un volumen de tráfico mucho mayor al de un ataque convencional.

Algunos de estos ataques han sido anunciados en foros de la *darknet* y en canales de Telegram, lo que sugiere una coordinación por parte de grupos organizados con objetivos específicos. Este patrón revela una planificación estructurada y una posible alineación con los intereses de estados nación, como Rusia, que buscan ejercer presión sobre sus objetivos.

El papel de los grupos de hackers en los ciberataques

Los atacantes detrás de estos incidentes han sido atribuidos a grupos como 'Diplomat' y 'Z-PENTEST ALLIANCE'. Ambos son conocidos por sus operaciones de hostigamiento cibernético contra países de la OTAN, especialmente aquellos que han expresado un apoyo activo a Ucrania en el conflicto.

Estos grupos han mostrado capacidades avanzadas en términos de la ejecución de ciberataques, utilizando tanto técnicas de DDoS como otras formas de intrusión cibernética.



El grupo 'Diplomat', en particular, ha sido vinculado con ciberataques a gobiernos y organizaciones internacionales que se oponen a las políticas de Rusia. Por su parte, 'Z-PENTEST ALLIANCE' ha sido vinculado a operaciones de espionaje y desestabilización cibernética. Aunque no se ha confirmado su relación directa con el Kremlin, se cree que estos grupos operan con la protección implícita de Rusia o de actores afines.

Motivación política detrás de los ciberataques

El objetivo principal de estos ataques parece ser la desestabilización política, no solo a nivel nacional, sino también a nivel internacional. Los ciberataques de esta naturaleza forman parte de una guerra híbrida más amplia. En ella, acciones no convencionales como la desinformación, los ataques digitales y el espionaje se emplean para generar confusión, socavar la moral de la población y aumentar las tensiones internas y externas.

En este caso, los ataques DDoS tienen un objetivo claro: interrumpir la operatividad de las instituciones gubernamentales españolas y, a través de esa interrupción, mostrar la vulnerabilidad de un miembro de la OTAN que se ha mostrado fuertemente comprometido con el apoyo a Ucrania.

➡ Te puede interesar: 🎧 Código LISA – Los mayores ciberataques en la historia de la Ciberseguridad

Estos ataques no solo responden a las sanciones y presiones internacionales que enfrenta Rusia por su invasión, sino que también buscan imponer un costo a las naciones que respaldan a Ucrania.

La ciberseguridad, por lo tanto, se ha convertido en un componente clave dentro de la estrategia de guerra híbrida de Rusia. Al atacar infraestructuras críticas, Rusia no solo busca dañar a sus adversarios, sino también socavar la confianza en el gobierno y generar una sensación de inseguridad en la población.

Impacto en España y la respuesta del gobierno

A pesar de la naturaleza no destructiva de los ataques DDoS, el impacto de estos sobre la operatividad del gobierno y la confianza de los ciudadanos no debe subestimarse. La caída de los sitios web gubernamentales, aunque temporal, afecta la capacidad de los ciudadanos para acceder a servicios esenciales, como la asistencia en emergencias y la información vital proveniente de organismos oficiales.

En respuesta a estos ataques, España ha reforzado sus capacidades de defensa cibernética. El Centro Criptológico Nacional (CCN) y otros organismos de seguridad han incrementado la vigilancia y el monitoreo de la red para detectar y mitigar ataques en tiempo real. Asimismo, se ha solicitado la colaboración de otros aliados internacionales para fortalecer las defensas cibernéticas y compartir información sobre las amenazas emergentes.

Sin embargo, la respuesta efectiva a estos ataques requiere un enfoque integral que no solo incluya la defensa reactiva, sino también una estrategia proactiva que identifique y neutralice las amenazas antes de que se materialicen. Esto implica una mejora constante de las capacidades de inteligencia cibernética y una colaboración más estrecha entre los países miembros de la OTAN.