MONTHLY

Threat Intelligence Report

BeyGoo

FEBRERO 2026

Threat Actors, Campaigns and Industry Impact.

Based on proprietary detection and analysis.

Índice de contenidos

1. Resumen ejecutivo

El conjunto de incidentes analizados evidencia un nivel de riesgo elevado en los principales países de **Latinoamérica**, concentrando el 34,57% en Brasil, Argentina y Colombia. A su vez, **México** (25,10%) y **España** (14,81%) también presentan una exposición significativa. Este escenario se encuentra principalmente asociado a la exposición recurrente de información sensible y al aumento sostenido de la actividad de grupos de ransomware.

Estas amenazas incrementan de manera directa la probabilidad de interrupciones operativas, pérdidas económicas y sanciones regulatorias, especialmente en organizaciones con alta dependencia de sistemas digitales. Además, impactan significativamente en su reputación.

Los mayores niveles de criticidad se concentran en los sectores gubernamental (33,74%), educativo (7%), tecnológico (6,17%) y financiero (4,53%). La combinación de grandes volúmenes de datos, servicios esenciales y superficies de ataque expuestas amplifica el **impacto potencial sobre la continuidad del negocio, y la confianza de usuarios y ciudadanos**.

La recurrencia de actores que reutilizan y comercializan información previamente comprometida agrava este escenario, extendiendo el ciclo de riesgo más allá del incidente inicial.

2. Eventos relevantes

- **Filtraciones masivas de bases de datos gubernamentales**, exposición y comercialización de registros pertenecientes a organismos públicos en países como **México, Brasil, Perú, Colombia y Chile**, que incluyen información personal, fiscal, sanitaria y biométrica.

- Predominio de **combolists** en múltiples sectores en **Argentina, Chile y Colombia**, compuestas por credenciales generalmente recicladas, provenientes de brechas de seguridad tradicionales o compromisos derivados de malware tipo infostealer, con impacto tanto en organizaciones públicas como privadas.

- En **Brasil**, se registró un caso en el que quedó expuesta información sensible, con la publicación de bases de datos con información personal y sanitaria de ciudadanos del Estado de Pernambuco. Fue atribuida al actor *0x0dayToDay*, junto con la exposición de documentación asociada al Ministerio de Cultura de Brasil por parte del actor *breach3d*.

- **España y Perú** se vieron principalmente afectados por filtraciones dirigidas y la comercialización de bases de datos específicas, lo que sugiere campañas más selectivas y orientadas a objetivos concretos.

- Incremento de ataques de **ransomware** en sectores críticos, como salud, energía, transporte, manufactura y servicios profesionales, con volúmenes de datos exfiltrados que alcanzan cientos de gigabytes e incluso terabytes.

- **Campañas transnacionales de combolists**, afectaron a usuarios de Argentina, Chile, Colombia, México, España, Perú y Cuba, facilitando fraudes, accesos no autorizados y ataques posteriores.

- **Defacements** en portales institucionales, principalmente gubernamentales y educativos, con un impacto predominantemente reputacional y demostrativo, más que destructivo.

3. Panorama general de amenazas

Principales focos por país

El panorama global se presenta de la siguiente manera: **México** se posiciona nuevamente como el país más afectado por diferentes tipos de incidentes, concentrando el **25,10%** del total registrado.

En segundo lugar se ubica **España**, con valores muy similares, que representan el **14,81%** de los casos.

En el ámbito Latinoamericano, **Brasil** (14,40%), **Argentina** (11,93%) y **Colombia** (7,82%) se destacan como los países con mayor volumen de incidentes, acumulando en conjunto el **34,57%** del total analizado.

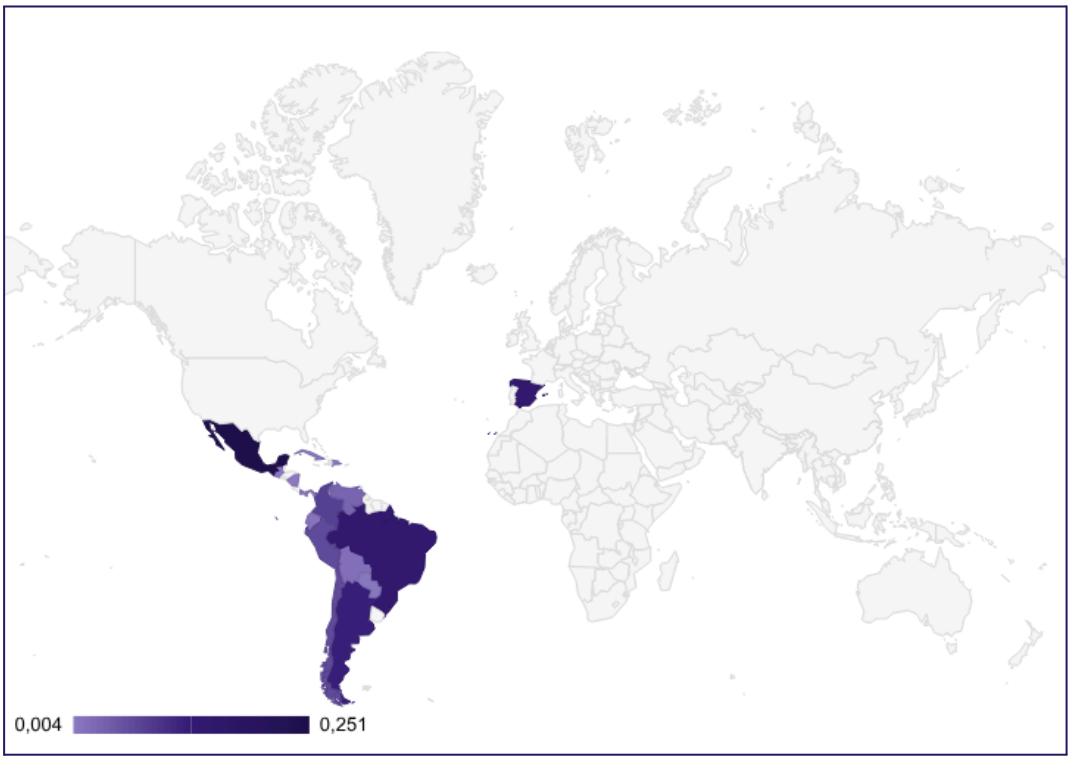
Chile, Perú y **Venezuela**, conforman una tercera franja de países afectados. Si bien se sitúan por debajo de la media regional, los tres registraron un incremento en la cantidad de incidentes respecto del mes anterior, lo que refuerza la necesidad de un seguimiento continuo y de no **subestimar** su evolución.

País	Incidentes %
México	25,10%
España	14,81%
Brasil	14,40%
Argentina	11,93%
Colombia	7,82%
Chile	6,58%
Perú	6,58%
Venezuela	3,29%
Mundial	2,06%
Bolivia	1,65%
Ecuador	1,23%
Cuba	0,82%
Panamá	0,82%
Paraguay	0,82%
Sudamérica	0,82%
Nicaragua	0,41%
Guatemala	0,41%
Dominicana	0,41%

Al comparar los valores con el período previo, se observa un aumento generalizado de incidentes en todos los países analizados.

País	Diciembre/25	Enero/26
Perú	5,57%	6,58%
Chile	4,26%	6,58%
Venezuela	1,97%	3,29%

La concentración de incidentes se representa mediante un mapa de calor en el siguiente gráfico geográfico, lo que permite identificar rápidamente las zonas con mayor impacto.



Evolución de las filtraciones y cambios relevantes

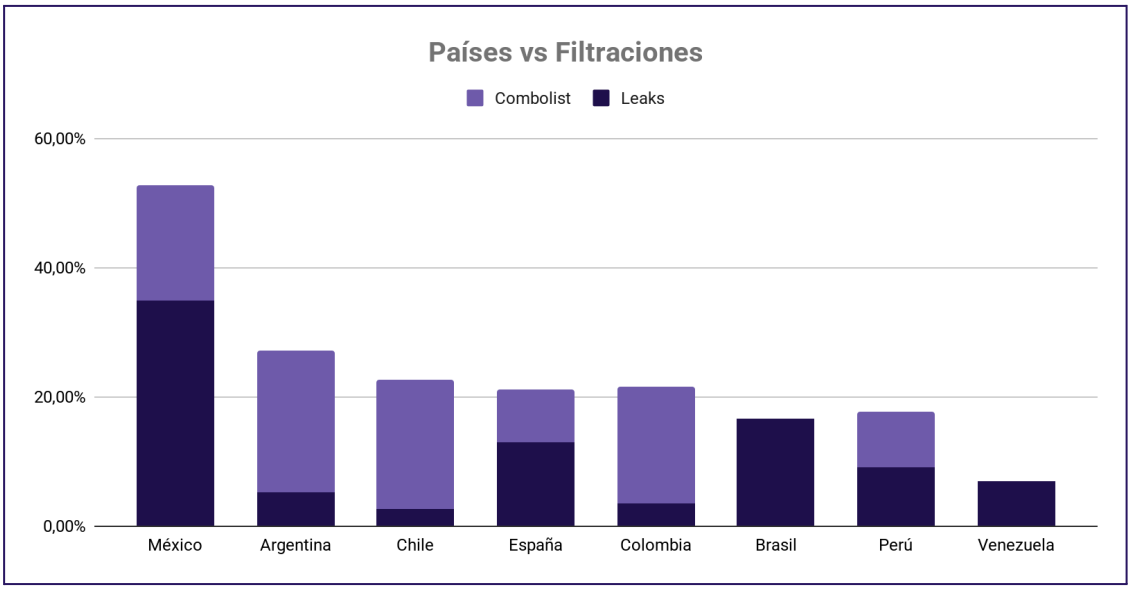
El panorama de amenazas se caracteriza por el predominio de **filtraciones**, **reventa de bases de datos y circulación de credenciales comprometidas** en los foros clandestinos. Si bien este patrón ya ha sido observado en períodos anteriores, se han incorporado nuevos países como víctimas de este tipo de incidentes.

Durante el período analizado, se registraron incidentes de filtración en múltiples países. **México** concentró el **52,78%** del total de los casos. Este porcentaje se compone de un 34,78% correspondiente a filtraciones dirigidas y reventa de bases de datos, y un 18% asociado a la circulación de *combolists*,

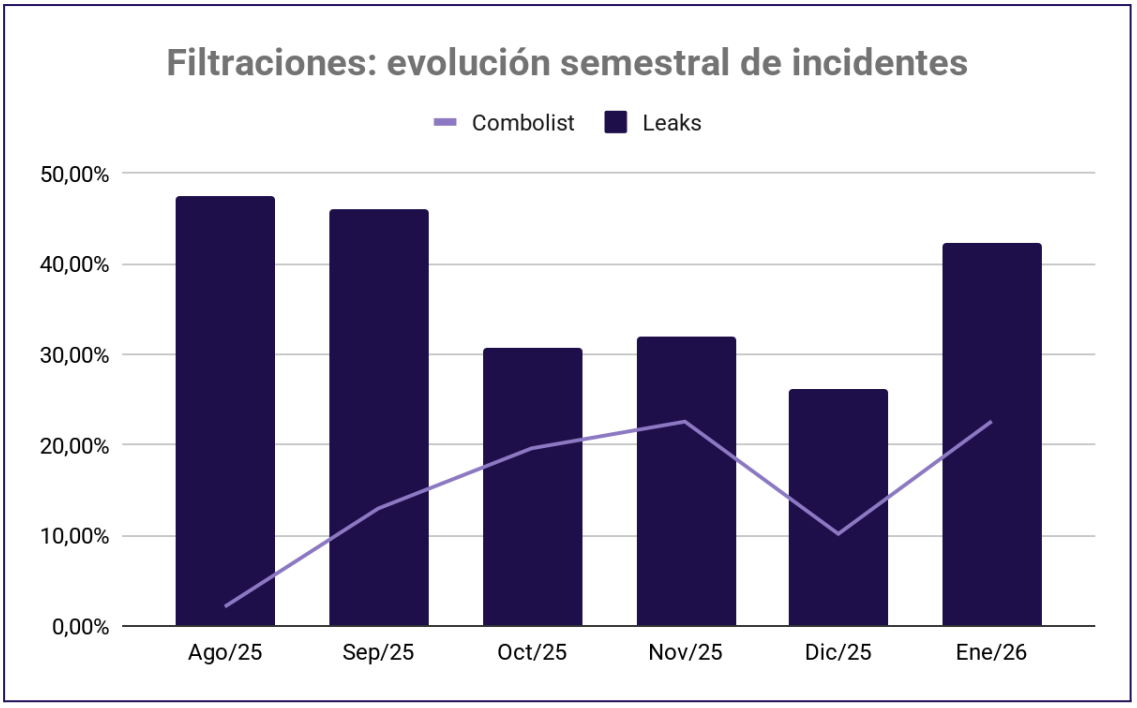
es decir, conjuntos de credenciales comprometidas que suelen originarse en brechas de seguridad tradicionales, como infecciones por malware del tipo *infostealer*.

Argentina, Chile y Colombia presentaron un comportamiento similar, con una mayor incidencia de credenciales comprometidas a través de **combolists**. En contraste, **España y Perú** evidenciaron un patrón inverso, registrando un mayor impacto asociado a **filtraciones dirigidas y a la reventa de bases de datos previamente comprometidas**.

Esta diferencia puede observarse de forma visual en el gráfico siguiente, donde se representa de manera acumulada la distribución de ambos tipos de filtraciones.



Además, analizamos el último **semestre** y observamos una leve disminución de este tipo de incidentes durante los meses de octubre, noviembre y diciembre; retornando a sus valores estables en el mes de enero de este año.



Luego del análisis, listamos las posibles causas de este comportamiento:

- **Retraso en las publicaciones:** muchas filtraciones ocurren, pero son publicadas semanas o meses después en foros clandestinos. Los actores de amenazas suelen buscar un momento más oportuno para publicar determinadas filtraciones y así maximizar su impacto o valor.

- **Reorientación de la actividad criminal:** durante el último trimestre del año suele observarse un mayor enfoque en fraudes financieros, estafas estacionales, phishing y campañas de ingeniería social, lo que implica una reducción temporal en la actividad vinculada a filtraciones de datos.

- **Mayor discreción operativa:** algunos grupos intentan pasar desapercibidos y disminuyen su actividad para evitar la atención de las fuerzas de seguridad. En los meses próximos a fin de año, coinciden con mayores operativos policiales y judiciales en varias regiones geográficas.

- **Mejoras en las defensas de las organizaciones:** como consecuencia de los cierres de ejercicio, auditorías y refuerzos operativos, se elevan los controles, esto incluye parches, revisión de accesos, monitoreo intensivo y más.

La disminución observada en el último trimestre del año no debe interpretarse como una reducción del riesgo, sino como un cambio en la dinámica de publicación y exposición de los incidentes.

En estas condiciones, la reorientación de los actores de amenazas hacia campañas de fraude basadas en ingeniería social adquiere particular relevancia, al verse amplificada por la insuficiencia de los controles técnicos.

4. Phishing avanzado: cuando una mala configuración convierte a un dominio en una trampa

Actores de amenazas y grupos maliciosos explotan **fallas de diseño** y **configuraciones incorrectas** en la infraestructura de correo electrónico y de red para ejecutar campañas de phishing altamente efectivas. Este tipo de ataques constituye un vector recurrente en esquemas de fraude e ingeniería social y tiende a intensificarse en períodos estacionales o coyunturales favorables para este tipo de delitos.

La técnica consiste en la **suplantación del dominio oficial** de la organización, haciendo que los correos electrónicos aparenten originarse desde los servidores de correo corporativos, cuando en realidad son generados desde una infraestructura externa maliciosa. Esto permite a los atacantes enviar correos de phishing significativamente más convincentes, reduciendo la probabilidad de generar dudas o sospechas a simple vista.

Vector de ataque empleado

El vector de ataque se basa en la explotación de una configuración incorrecta de la seguridad del correo electrónico (SPF, DKIM y DMARC), lo que permite la suplantación de identidad. A través de este canal, los atacantes distribuyen campañas de phishing mediante plataformas PhaaS —Phishing as a Service—. En los casos detectados, se ha identificado el uso de **Tycoon2FA**, un servicio que facilita la creación de páginas falsas destinadas al robo de credenciales.

Microsoft, en sus informes de inteligencia[1], ha reportado que estas detecciones no son nuevas, pero se incrementaron a partir del mes de mayo de 2025.

Tycoon2FA

Es una plataforma de phishing como servicio —PhaaS— utilizada por ciberdelincuentes para **robar credenciales de acceso**. Es eficiente incluso en aquellos entornos que poseen la **autenticación multifactor (MFA) activada**.

Con esta herramienta, es posible crear y desplegar campañas de phishing avanzadas sin necesidad de conocimientos técnicos profundos. Además,

[1] Microsoft. (s. f.). Threat intelligence. Microsoft Security Blog. https://www.microsoft.com/en-us/security/blog/topic/threat-intelligence/?sort-by=newest-oldest&date=any

proporciona plantillas de páginas falsas que imitan servicios legítimos, como Microsoft 365, Google, entidades bancarias y más.

Se destaca entre otros PhaaS, por implementar técnicas de phishing en tiempo real (AiTM – Adversary-in-the-Middle) y de esta manera logra capturar: usuario y contraseña, cookies de sesión y códigos MFA. Ofrece infraestructuras listas para usar, desde el hosting y certificados TLS hasta una rotación de dominios.

Tycoon2FA se comercializa en los mercados clandestinos entre ciberdelincuentes: no es un software legítimo disponible públicamente. El costo del acceso inicia en USD 120[2] por 10 días y puede ascender a USD 320 o más, dependiendo del dominio, el período de acceso y las funcionalidades adicionales.

Procedimiento

Microsoft declaró que éste vector de ataque no es reciente, y que desde mayo de 2025 detectaron un aumento. Observaron campañas que aprovechan este vector para realizar estafas financieras contra organizaciones.

En octubre de 2025, Microsoft Defender para Office 365 **bloqueó más de 13 millones de correos electrónicos maliciosos vinculados a Tycoon2FA**, incluidos numerosos ataques que suplantaban dominios corporativos legítimos.

[2] Hamel, L., Guinivan, G., & Dawson, C. (2024, May 9). Unmasking Tycoon 2FA: A stealthy phishing kit used to bypass Microsoft 365 and Google MFA. Proofpoint. https://www.proofpoint.com/us/blog/email-and-cloud-threats/tycoon-2fa-phishing-kit-mfa-bypass

Aquellas entidades cuyos registros MX apuntan directamente a Office 365 cuentan con un mayor nivel de protección, dado que **Microsoft bloquea este tipo de suplantación de forma automática**.

Acciones recomendadas para prevenir estos ataques

- **Configurar correctamente los protocolos SPF, DKIM y DMARC:** se utilizan para autenticación de los correos electrónicos, trabajan en conjunto para verificar que los emails sean legítimos.
    - **SPF (Sender Policy Framework):** define qué servidores de correo están autorizados a enviar mensajes en nombre del dominio @empresa.com. Si un atacante intenta enviar un correo fraudulento utilizando ese dominio desde un servidor no autorizado, la validación SPF fallará y el mensaje será rechazado o clasificado como spam.
    - **DKIM (DomainKeys Identified Mail):** actúa como una firma digital del correo electrónico. El servidor emisor firma el mensaje, y el servidor receptor verifica que el contenido no haya sido alterado y que el correo proviene efectivamente del dominio declarado. Si el mensaje fue modificado o no cuenta con una firma válida, la verificación DKIM fallará.
    - **DMARC (Domain-based Message Authentication, Reporting and Conformance)**: permite definir la acción a aplicar sobre los correos que no superan las validaciones de SPF y/o DKIM. Las políticas disponibles son ***none*** (no realizar ninguna acción), ***quarantine*** (enviar el mensaje a spam) y ***reject*** (rechazar el correo). **Se recomienda configurar DMARC en quarantine o reject para mitigar eficazmente los correos fraudulentos.**
- **Verificar y asegurar los conectores de correo de terceros:** estos permiten que los correos pasen por un filtro antispam, un servicio de seguridad o un servidor de correo local. Algunos ejemplos: Mimecast, Proofpoint, Barracuda, Exchange local. Si estos conectores están mal configurados, se puede tomar un correo falso como legítimo. Por cada conector, se deberá verificar IP de origen y certificado válido.
- **Usar Microsoft Defender para Office 365:** permite detectar y bloquear correos de phishing, enlaces maliciosos y archivos peligrosos, incluso cuando los mensajes parecen internos, ayudando a prevenir el robo de credenciales y estafas.
- **Activar protecciones como Safe Links o Zero-hour auto purge (ZAP):** se recomienda activar protecciones adicionales para ayudar a detener ataques de phishing, incluso cuando los correos logran pasar los filtros iniciales.

- **Safe Links:** verifica los enlaces incluidos en los correos electrónicos; protege al usuario cuando hace clic, no solo cuando llega el correo y bloquea enlaces que llevan a páginas falsas o maliciosas, aunque el enlace parezca legítimo.

- **ZAP:** es una protección automática que elimina o pone en cuarentena correos maliciosos, actúa incluso después de que el mensaje llegó a la bandeja de entrada, usa nueva información de amenazas para reaccionar rápidamente. Un correo de phishing puede ser eliminado automáticamente si luego se confirma que es peligroso.

__Safe Links__ analiza y bloquea enlaces maliciosos, mientras que __ZAP__ elimina automáticamente correos peligrosos que ya llegaron a la bandeja de entrada.

- **Implementar autenticación multifactor resistente al phishing (sin contraseñas):** ello protege las cuentas de los usuarios incluso si caen en un correo falso. A diferencia del inicio de sesión tradicional con usuario y contraseña, este tipo de autenticación requiere métodos más seguros como: huella digital o reconocimiento facial, llaves de seguridad o aplicaciones de autenticación seguras.

- **Capacitar a los usuarios para identificar correos sospechosos es fundamental:** pues la tecnología por sí sola no es suficiente para detener todos los ataques de phishing. Se recomienda implementar un programa de capacitación anual y periódico, que sea dinámico, entretenido y fácil de llevar, de modo que los usuarios no lo perciban como una carga adicional. Asimismo, se pueden ofrecer incentivos o premios para fomentar la participación y el compromiso.

5. Análisis de contexto

En este marco, el **riesgo** ya no es exclusivamente tecnológico y pasa a tener un carácter **operativo** y **estratégico**, donde la persistencia de actores, la reutilización de datos comprometidos y la dependencia de infraestructuras digitales amplifican el **impacto** de cada incidente.

Esta situación no solo exige medidas reactivas, sino una gestión del riesgo orientada a la anticipación, la resiliencia y la reducción del impacto a largo plazo.

Implicancias y proyección del escenario

Un incidente puntual puede escalar rápidamente y afectar múltiples servicios o dependencias críticas, generando **implicancias operativas** relevantes.

Las reiteradas filtraciones y accesos no autorizados producen un **efecto acumulativo del riesgo**, agravado por la reutilización de la información comprometida meses después del incidente original y por la creciente dependencia de servicios de terceros.

En paralelo, la brecha entre la sofisticación de los actores de amenazas y las capacidades de prevención y respuesta de muchas organizaciones continúa ampliándose, lo que permite proyectar un **incremento sostenido** de incidentes vinculados a la monetización de datos, la extorsión y la afectación de servicios esenciales.

6. Fuentes de información

El presente informe ha sido elaborado a partir de fuentes, análisis e investigaciones propias, enfocadas en los incidentes de ciberseguridad registrados en el mes de enero 2026. Su contenido se sustenta en información obtenida de diversos entornos, entre ellos foros clandestinos, canales de la deep y dark web, plataformas OSINT y medios especializados en ciberseguridad.

Seguinos en LinkedIn

y enterate de todas las novedades

beygooapp beygoo.io