INFORME

Actividad criminal en línea en América Latina

1er semestre / 2021

Qué encontrará en este informe

Principales datos de este informe

Haga clic en el número de página a continuación del dato para ir a la página correspondiente.

14 083

casos de phishing identificados en el 1er semestre de 2021 — página 5

2.5 mi

de credenciales expuestas en la Deep y Dark Web, servicios de paste y grandes filtraciones— página 7

687 mil

tarjetas de crédito y débito encontrados en el semestre, 94.7% estaban aún vigentes — página 8

- Caída del **32.04%** en la incidencia de casos de phishing del último semestre a este. — página 10
- **Brasil** es el campeón del ranking de países con más tarjetas de crédito y débito expuestos en América Latina y en el mundo. — página 13
- En América Latina, **Costa Rica** fue el segundo país con más filtraciones de tarjetas de crédito.

Más lento, 2021, por favor. ¡Muchas gracias!

Necesitamos un respiro. El 2021 ha sido un año intenso para quien trabaja en el mercado de ciberseguridad. Pero, finalmente, pasamos el inicio inquietante del año y podemos respirar hondo para seguir adelante.

En las próximas páginas de este informe, encontrará informaciones sobre comportamientos, tendencias y, principalmente, las cifras que identificó la plataforma Axur relacionadas a los diversos cibercrímenes.

El rayo X de las amenazas y fraudes digitales del segundo semestre del año en América Latina. En Axur, creemos que estas informaciones son muy valiosas para el día a día de las empresas. Saber cómo comportarse cuando se usa Internet, ya sea en la vida personal como profesional, es el primer paso para poder eliminar los muchas — realmente muchos — intentos de ataque de la ciberdelincuencia.

Nuestra misión es, y siempre será, hacer de la internet un lugar más seguro para las empresas, familia, amigos y conocidos. El ecosistema digital en el que vivimos sufre transformaciones cada minuto. Saber cómo protegerse es más que necesario para mantener una experiencia saludable en esta infinidad de recursos y conocimiento que llamamos Internet.

Fábio Ramos, CEO de Axur

Phishing

Axur detectó **14 083** casos de phishing durante el primer semestre de 2021.

Esto representa un 32.04% menos que en el semestre anterior, cuando detectamos 20 724 casos en América Latina (Figura 1). Se puede notar que el número de casos de phishing está disminuyendo gradualmente. Observamos este tipo de movimiento a nivel global.

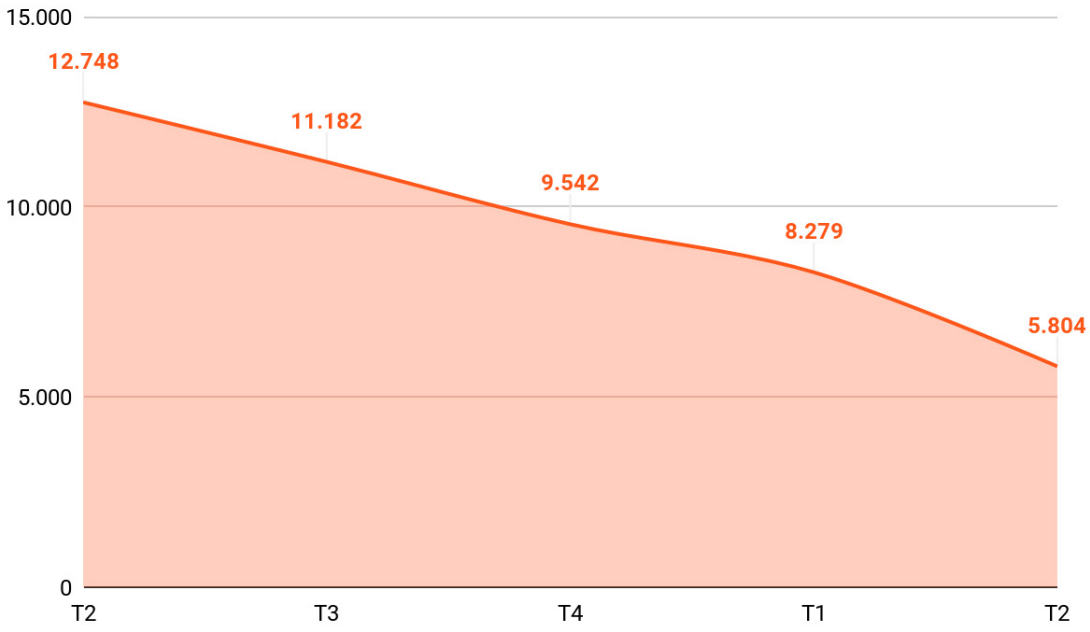

Figura 1. Cantidad trimestral de casos de phishing identificados en América Latina entre el segundo trimestre de 2020 y 2021.

Es esperable que en estos meses que anteceden al Black Friday, los números de phishing vuelvan a subir mucho porque el evento global de promociones, que se da principalmente en el e-commerce, es un gran atractivo para los ciberataques.

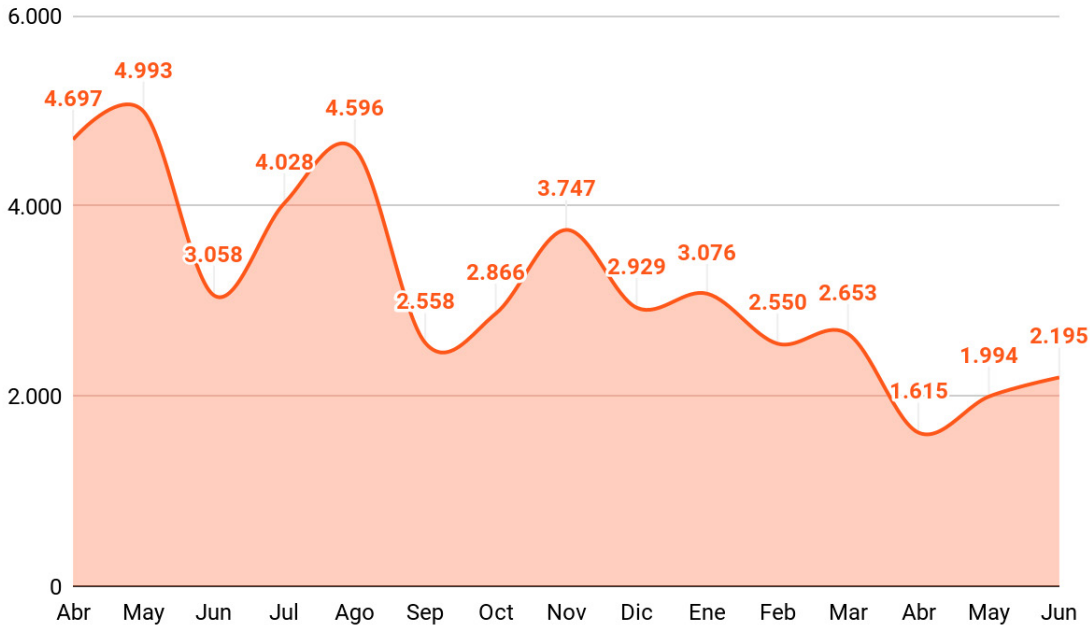

Figura 2. Cantidad mensual de casos de phishing identificados de abril de 2020 a junio de 2021.

De los **14 083** casos registrados en el semestre, 4 279 fueron identificados en Brasil (30.4%), el país con el mayor número de casos de phishing en América Latina identificados por Axur. La ciberdelincuencia tiene segmentos preferidos: e-commerce, SaaS y WebMail, y bancos/empresas financieras.

Certificado SSL

Otro aspecto interesante para analizar es la preferencia de la ciberdelincuencia por la utilización del protocolo SSL. Habíamos alertado sobre esto desde hace ya un tiempo: “el candado verde no siempre significa que el ambiente es seguro”.

Incluso, este semestre confirmamos una nueva tendencia que se extendió entre la ciberdelincuencia al crear páginas de phishing: la utilización del certificado de Security Socket Layer, el famoso SSL. El 75% de los sitios fraudulentos de phishing identificados por Axur en el semestre contaban con el certificado HTTPS instalado en el momento de la detección.

> Axur identificó este movimiento desde el año pasado. Para 2022, se espera que esta tendencia se consolide como práctica entre la ciberdelincuencia.

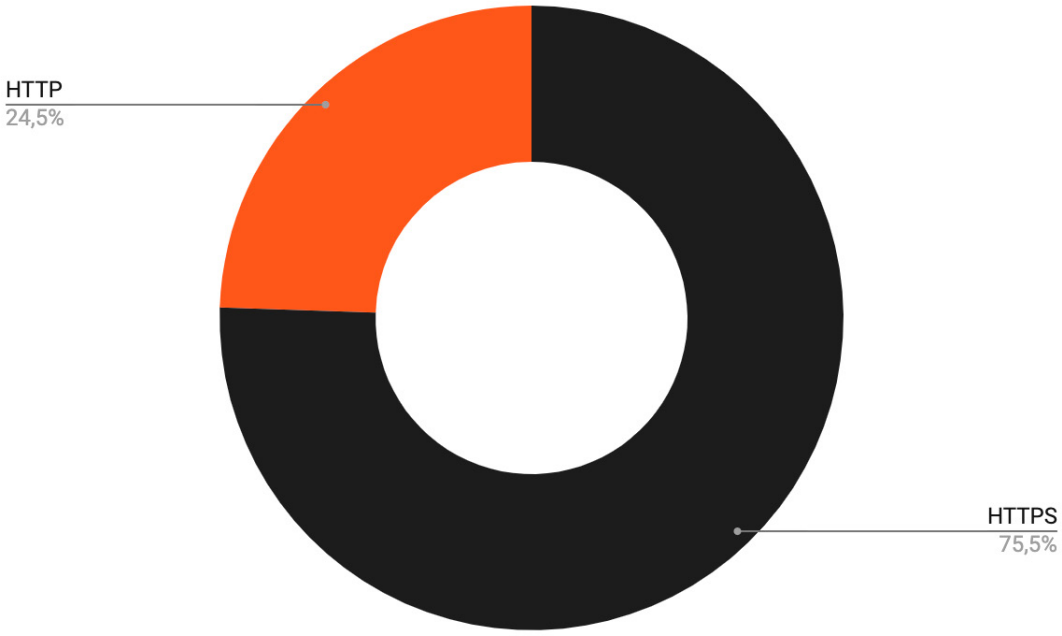

Figura 3. Porcentaje de dominios con y sin protocolo HTTPS.

Figura 4. Phishing detectado en el primer semestre de 2021 en una empresa del sector financiero.

Lo que influyó en esta caída fue la disminución en la incidencia del uso indebido de la marca en la búsqueda paga, los anuncios que vemos antes de los resultados de búsqueda orgánicos en motores de búsqueda como Google y Bing.

Filtración o exposición de credenciales

Se identificaron 2.5 mil millones de credenciales expuestas en el primer semestre de 2021.

2.32 mil millones en el primer trimestre del año y 181.5 millones en el segundo trimestre (Figura 5). El total de credenciales identificadas en el primer semestre de 2021 es 729.8% mayor del total que identificó Axur en el primer semestre de 2020. Mucho de esto se debe a las grandes filtraciones de datos que tuvieron lugar en Brasil. En el semestre, se expusieron 12 bases.

En el primer trimestre, COMB21, un compilado de filtraciones anteriores, por sí solo expuso 2.26 mil millones de credenciales de todo el mundo. Para una mejor comprensión de estos datos, a continuación presentamos dos gráficos que muestran la exposición mensual de credenciales: uno incluye COMB21 y el otro no.

En febrero de este año, cuando se identificó el COMB21, tuvimos el pico de detección de 2.27 mil millones de credenciales (Figura 5).

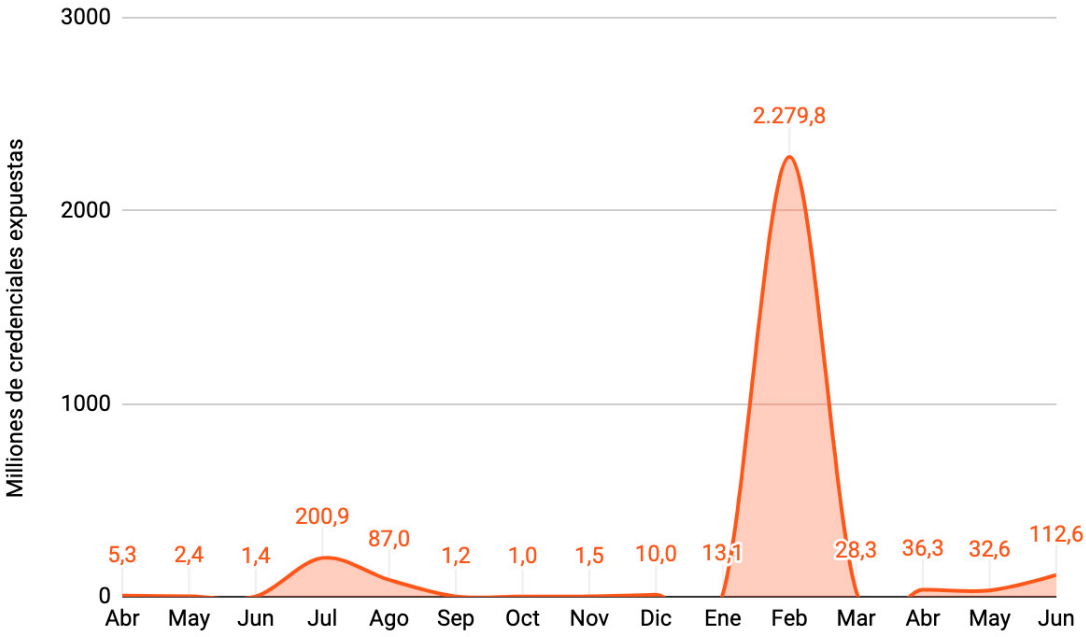

Figura 5. Volumen mensual de credenciales expuestas detectadas por Axur de abril de 2020 a junio de 2021.

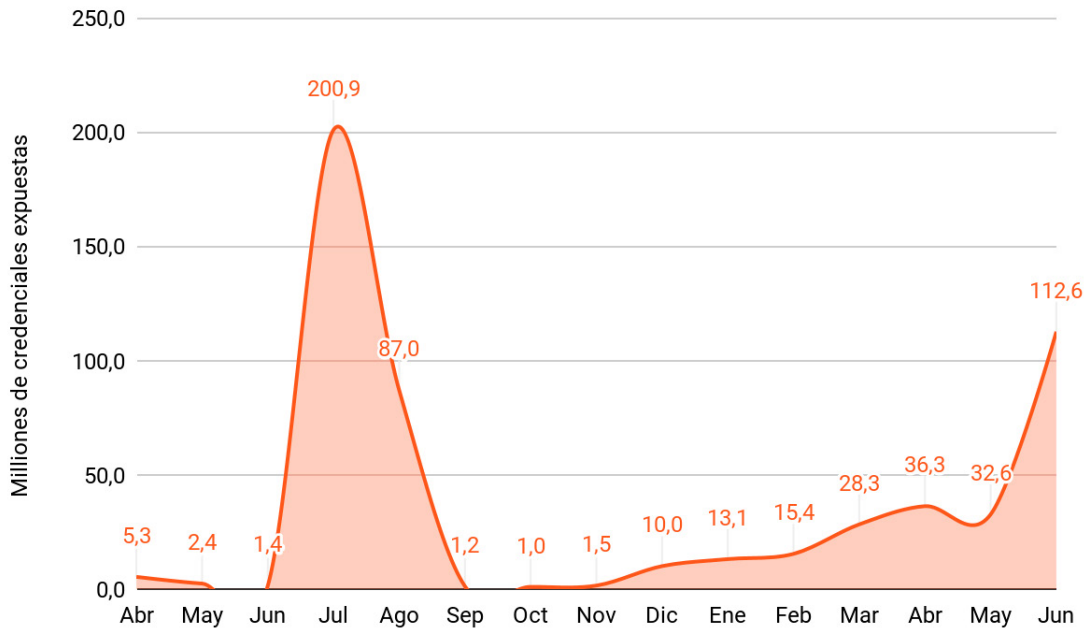

Figura 6. Volumen mensual de credenciales expuestas detectadas por Axur de abril de 2020 a junio de 2021 (sin COMB21).

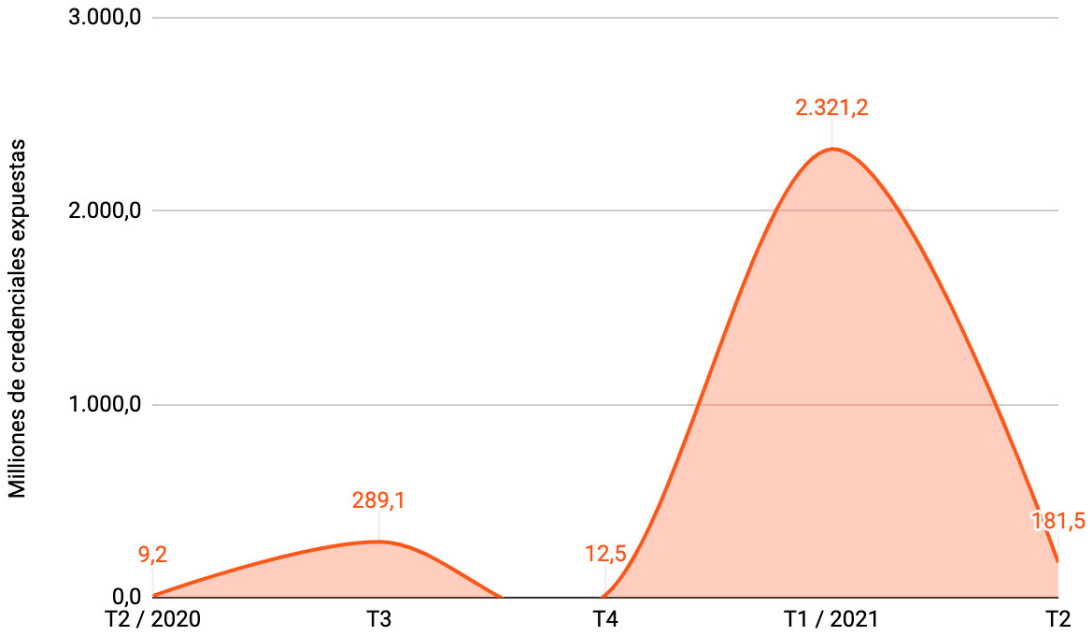

Figura 7. Volumen trimestral de credenciales expuestas detectadas por Axur entre 2020 y 2021.

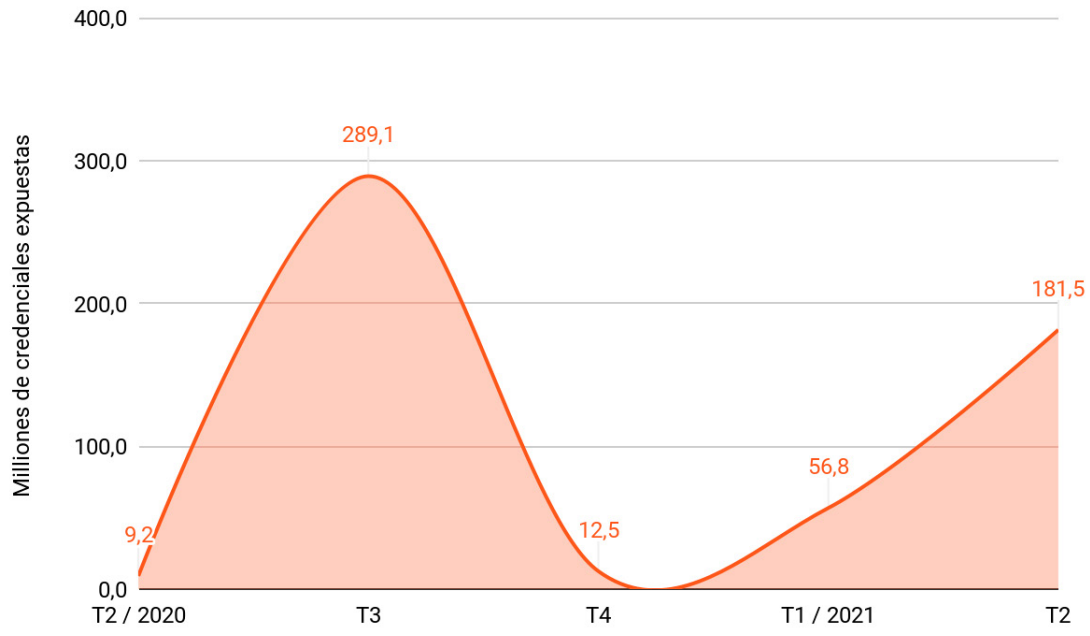

Figura 7. Volumen trimestral de credenciales expuestas detectadas por Axur entre 2020 y 2021.

Origen de las credenciales expuestas

Al analizar el origen de las credenciales, tenemos un volumen gigantesco presente en el COMB21, el cual en realidad es una filtración internacional. Dicho esto, veamos el origen de estas credenciales expuestas (Figura 9). Las 235.7 millones de credenciales expuestas en el primer semestre repartidas en los países de toda América Latina se conformó por grandes filtraciones que suman el 98.9% del total expuesto en el semestre.

Los servicios de paste y para compartir texto representan el 1% de las exposiciones (2.35 millones de credenciales), y la Deep y Dark Web, el 0.1% (217 mil credenciales).

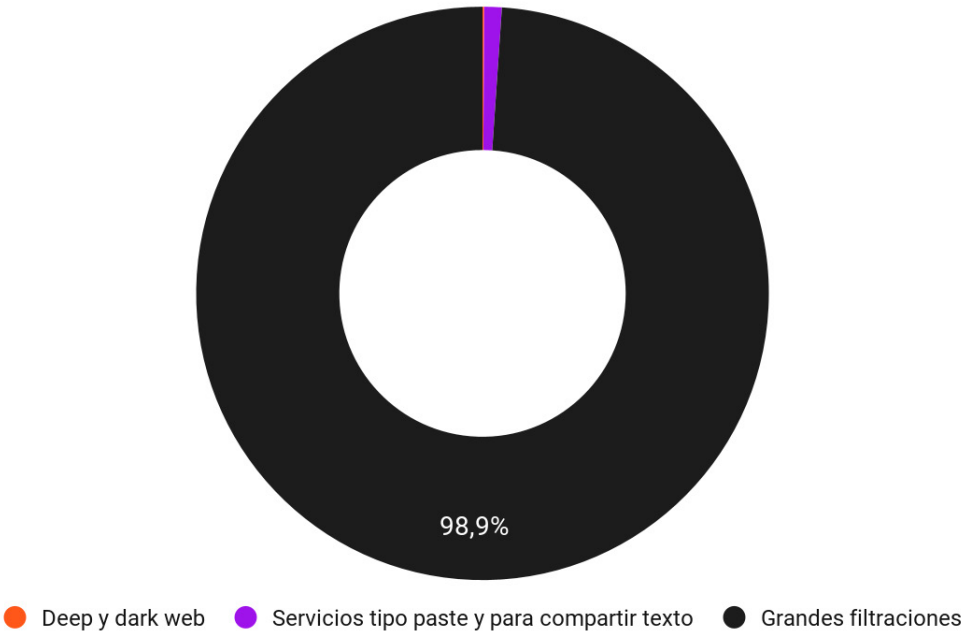

Figura 9. Origen de las credenciales expuestas encontradas por Axur en 2021.

Anatomía de las contraseñas encontradas

La contraseña “123456” continúa siendo la más utilizada entre las credenciales expuestas. En el primer semestre de 2021, 665 mil personas decidieron utilizarla como contraseña, lo que alcanza el 37.1% del total de detecciones. Esta cifra representa casi el doble de detecciones de la que está en segundo lugar, “123456789”, con 320 mil detecciones (17.9% del total), como se muestra en la Figura 10.

También vemos otras secuencias numéricas entre las 10 más utilizadas. Es importante destacar que en un ataque de Brute Force, estas contraseñas numéricas de hasta 9 dígitos se descubrirían muy fácilmente, en menos de 1 minuto.

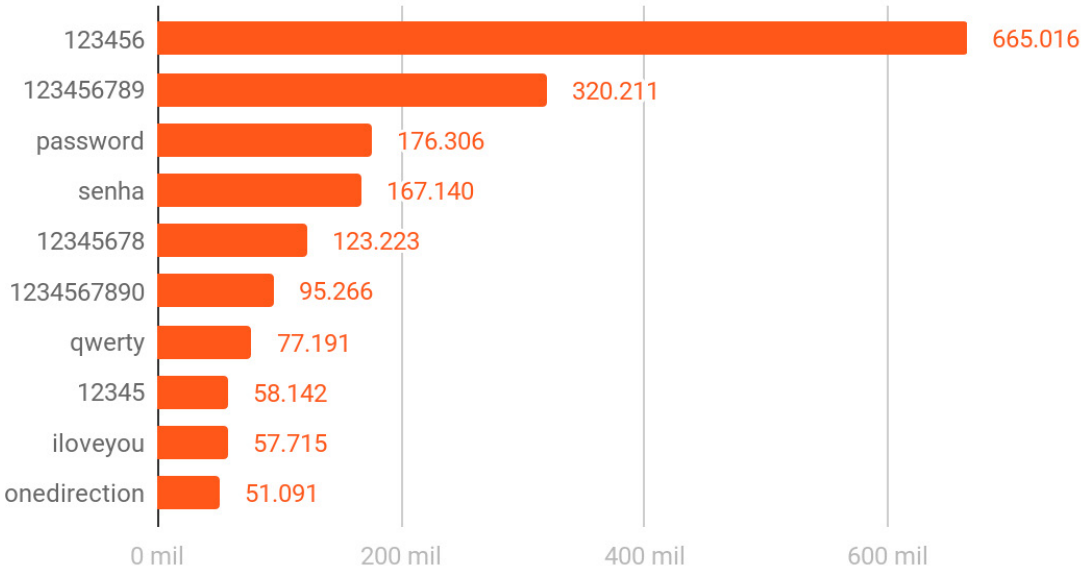

Figura 10. Ranking global de exposición de contraseñas detectadas por Axur en el primer semestre de 2021.

En cuanto a los tipos de contraseñas más utilizadas en el semestre, 65.2% de las credenciales encontradas por Axur están conformadas únicamente por letras mayúsculas (Figura 11).

El segundo tipo de contraseña más utilizada (15%) son las compuestas solamente por números. Vale recordar que en el caso de este tipo de contraseñas, si tienen entre 6 y 9 dígitos, mediante un ataque de Brute Force se podrían descubrir en un tiempo de 1 a 30 minutos, para lo que se necesita únicamente una computadora con la velocidad de 500 mil contraseñas por segundo.

ecciones de la que está en segundo lugar, “123456789”, con 320 mil detecciones (17.9% del total), como se muestra en la Figura 10.

También vemos otras secuencias numéricas entre las 10 más utilizadas. Es importante destacar que en un ataque de Brute Force, estas contraseñas numéricas de hasta 9 dígitos se descubrirían muy fácilmente, en menos de 1 minuto.

Por el contrario, las contraseñas más seguras, que contienen dos o más tipos de caracteres, ocupan solamente el 3.5%, una indicación de la preferencia de los internautas por contraseñas más fáciles de recordar.

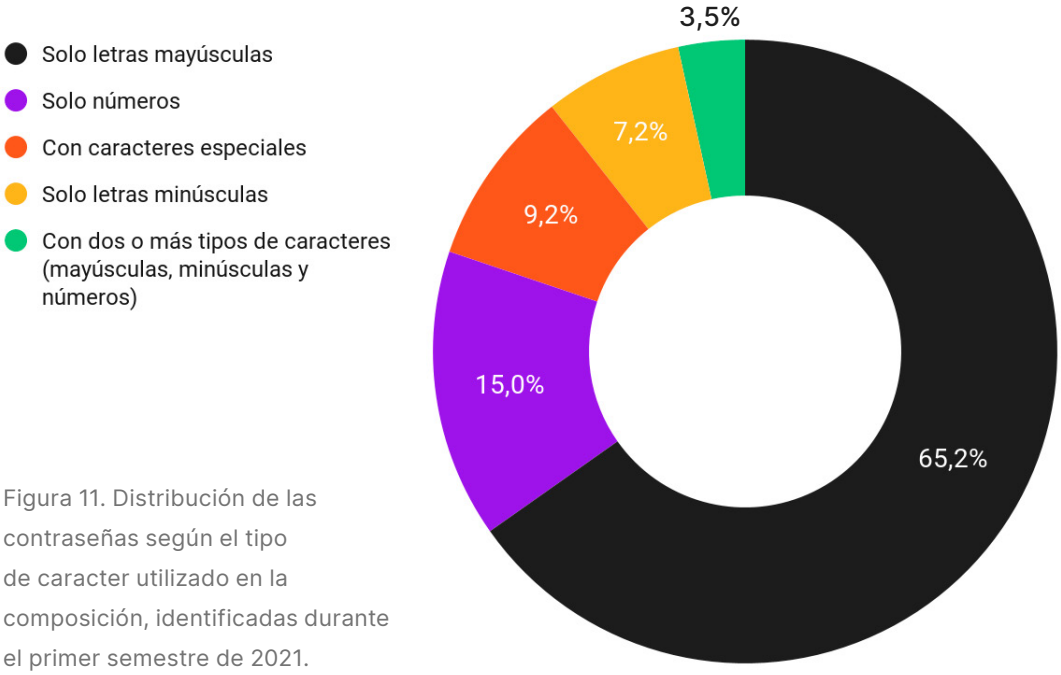

Figura 11. Distribución de las contraseñas según el tipo de caracter utilizado en la composición, identificadas durante el primer semestre de 2021.

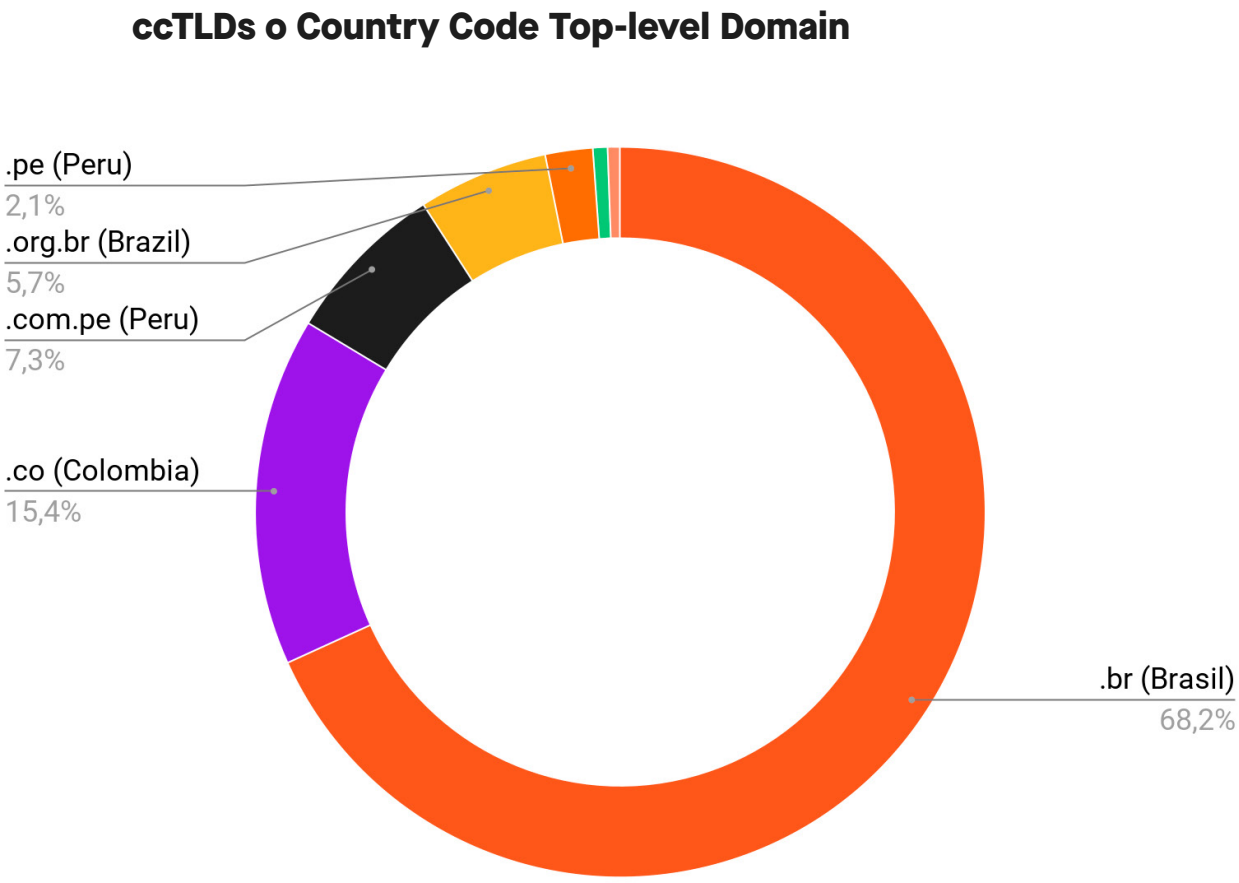

Figura 12. Ranking de ccTDLs de países latinoamericanos identificados en el primer semestre de 2021.

Durante el primer semestre, Brasil fue el gran campeón en exposición de credenciales (68.2%), con 17 grandes filtraciones que incluyeron credenciales incluso de los dominios gov.br del gobierno brasileño, entre otros datos filtrados.

Colombia quedó en segundo lugar con 15.4% de las credenciales expuestas en dominios .co.

Filtración o exposición de tarjetas de crédito y débito

Axur encontró 687 611 tarjetas de crédito y débito filtradas durante el primer semestre de 2021.1

De estas, 420 077 se identificaron en el primer trimestre del año y 267 921 en el segundo. Abril tuvo un pico de detecciones con 211 403 tarjetas expuestas (Figura 13).

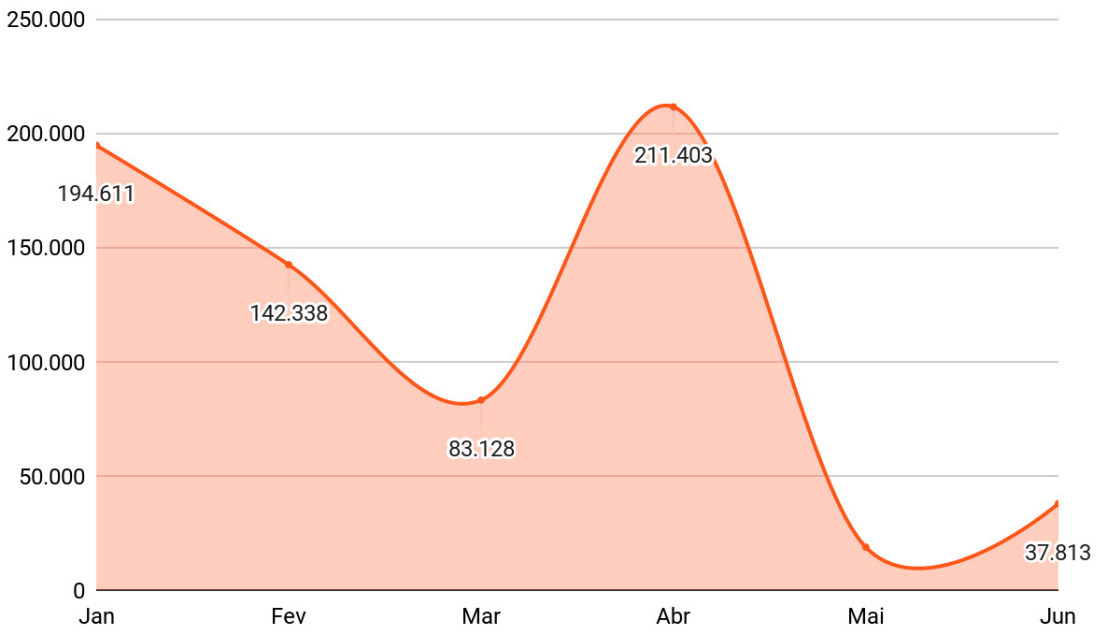

Figura 13. Cantidad de tarjetas de crédito y débito expuestas por mes en el primer semestre de 2021.

Países más expuestos en América Latina

El 95.3% de las tarjetas detectadas por Axur fueron de origen brasileño. Brasil sigue liderando el ranking de exposiciones de tarjetas de crédito y débito en América Latina y el mundo. Costa Rica quedó en segundo lugar en el ranking latinoamericano con 1.5% de las detecciones, seguida de México con un 1%.

Colombia, Argentina, Ecuador, Puerto Rico, Chile, Perú, Bolivia, Panamá, República Dominicana, Paraguay y Venezuela también entraron al ranking y suman el 2.2% del total de exposiciones.

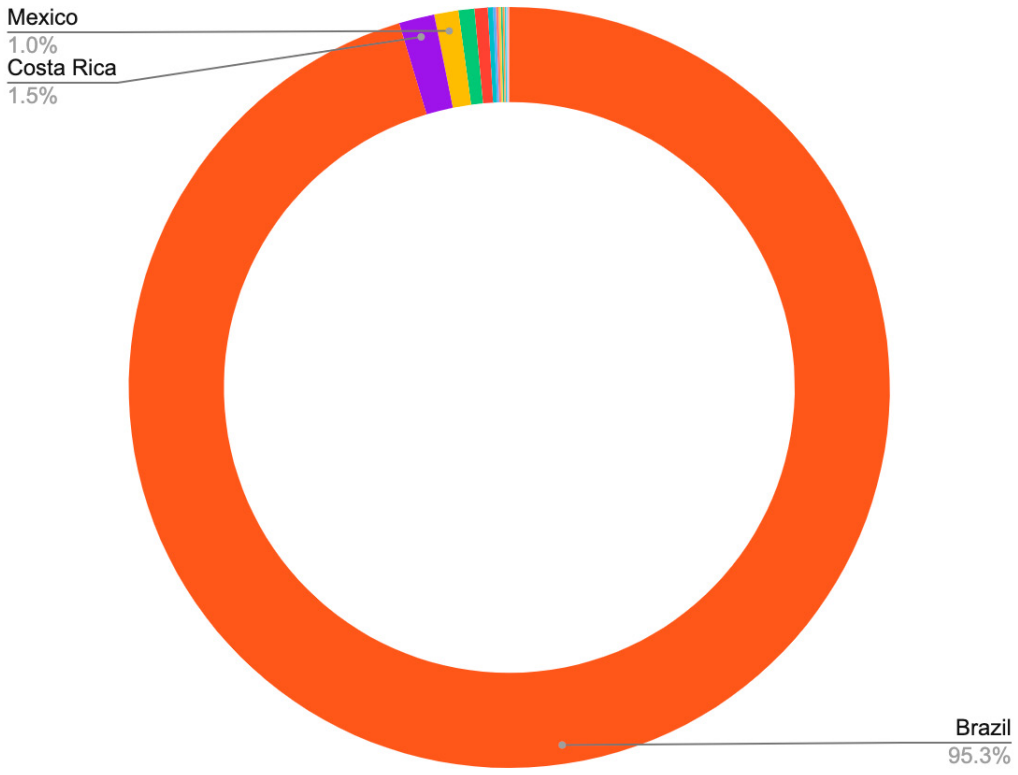

Figura 14. Porcentaje de países con más tarjetas de crédito y débito expuestas en el primer semestre de 2021 en América Latina.

BINs

Axur detectó 48 442 BINs expuestos en el primer semestre en 16 países de América Latina. Brasil sigue en primer lugar con 44 435 de las tarjetas detectadas relacionadas a BINs brasileros, lo que representa el 91.7% del total. En el semestre, entre las 15 primeras posiciones del ranking de BINs más expuestos, los BINs brasileños ocupan las primeras 10 posiciones. (Figura 15).

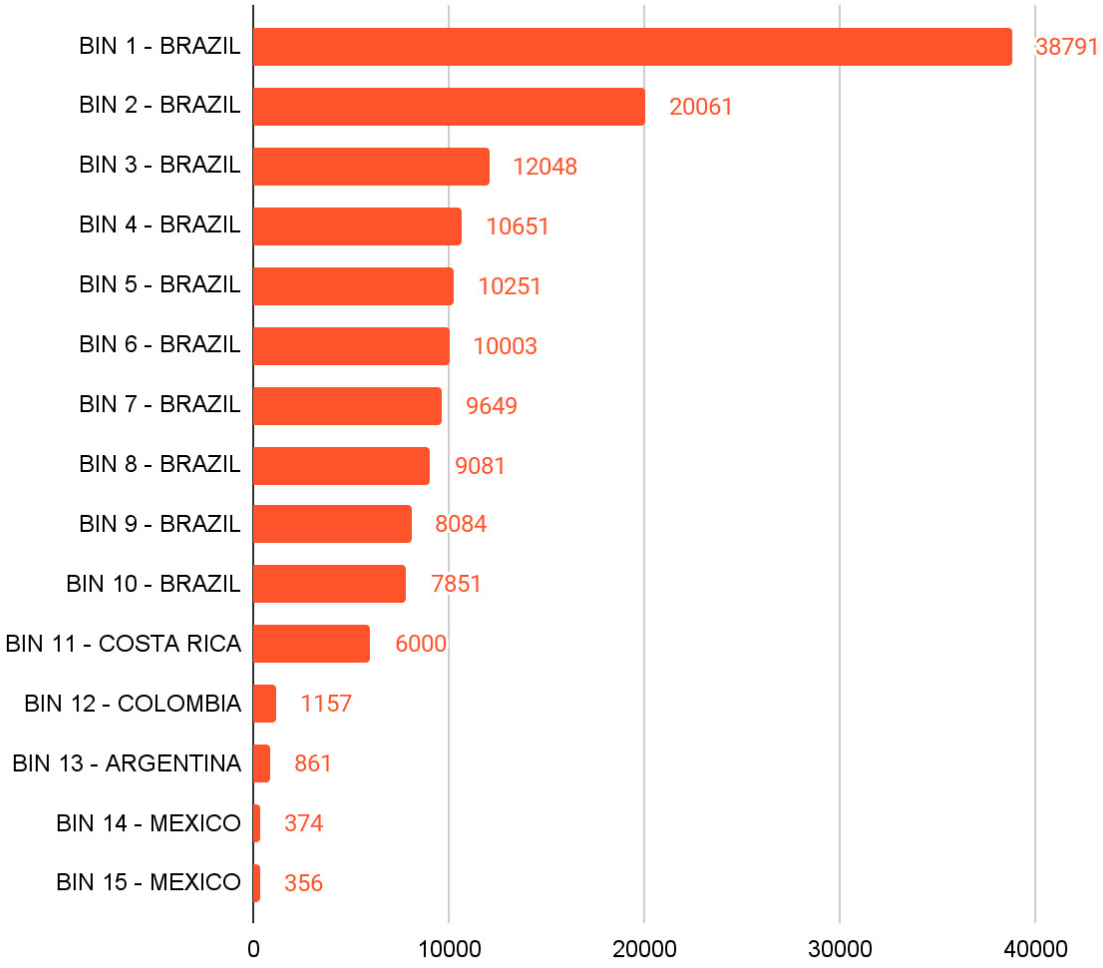

Figura 15. Ranking de América Latina de los 15 BINs com más exposiciones de tarjetas de crédito y débito en el primer semestre de 2021.

Por detrás de Brasil, están Costa Rica (6067), Mexico (4161), Colombia (1953) y Argentina (554), ocupando las posiciones restantes del Top 5 (Figura 16).

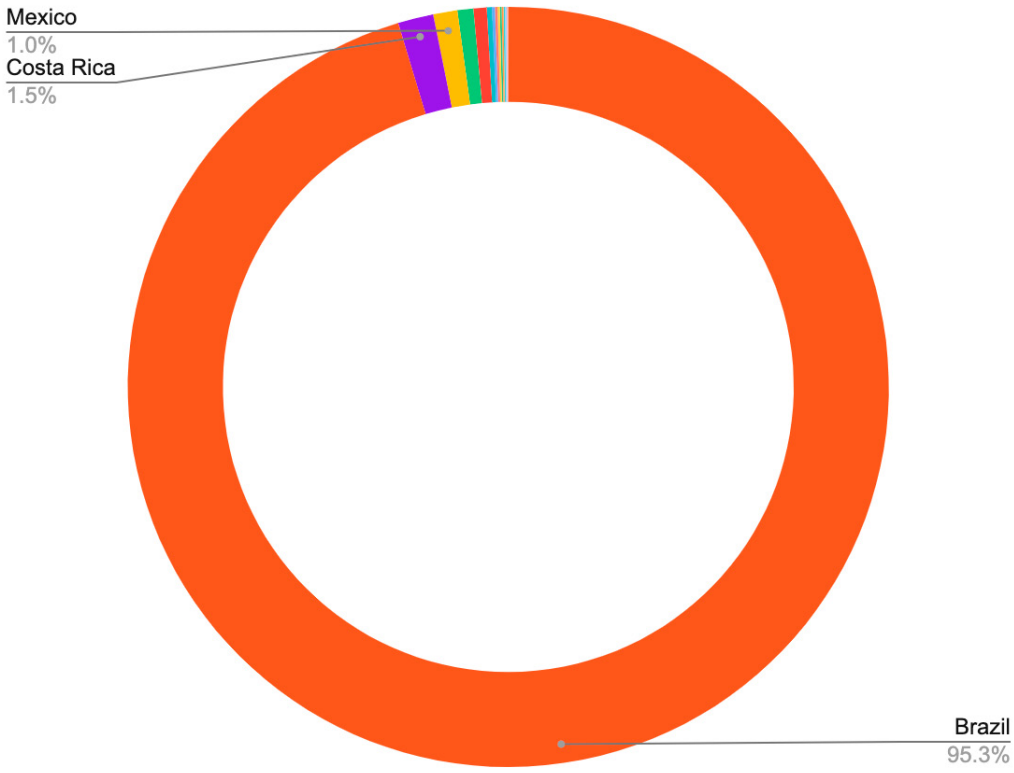

Figura 16. Porcentaje de BINs identificados por país durante el primer semestre de 2021.

Vigencia de las tarjetas de crédito

Durante el primer semestre de este año, el 94.7% de las tarjetas de crédito y débito identificadas por Axur estaban vigentes al momento de la detección. Esto suma un total de 651 167 tarjetas válidas para que los ciberdelincuentes pudieran usarlas.

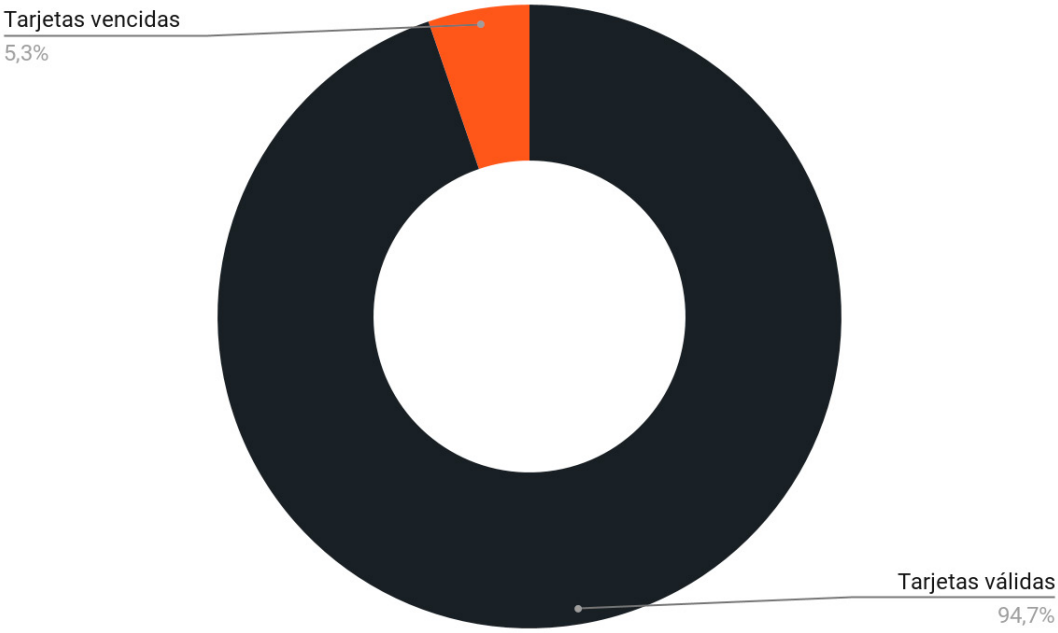

Figura 17. Porcentaje de tarjetas de crédito y débito vigentes en el momento de su detección durante todo el semestre de 2021.

Infracciones de uso de marca

Tuvimos una caída de 18.1% en el volumen total de incidentes de marca en América Latina, que pasó de 138 199 en el semestre pasado a 116 999 en este primer semestre de 2021.

Lo que influyó en esta caída fue la disminución en la incidencia del uso indebido de la marca en la búsqueda paga, los anuncios que vemos antes de los resultados de búsqueda orgánicos en motores de búsqueda como Google y Bing.

Los perfiles falsos en redes sociales continúan ganando cada vez más popularidad entre la ciberdelincuencia: del semestre pasado para acá, registramos un crecimiento del 6.9%, lo que suma 2492 perfiles más encontrados respecto al período anterior.

Mientras tanto, el uso indebido de marca en búsquedas pagadas volvió a crecer después de un año consecutivo en caída. El crecimiento es del 4.4%.

Un punto de atención es el crecimiento del 14.7% en las aplicaciones móviles fraudulentas. En este trimestre, se identificaron 3356 apps falsas vinculadas a las marcas más famosas.

También es interesante analizar el acumulado anual, que nos muestra un crecimiento de 225.1% entre el segundo trimestre de 2020 y el de 2021 en la identificación de aplicaciones falsas.

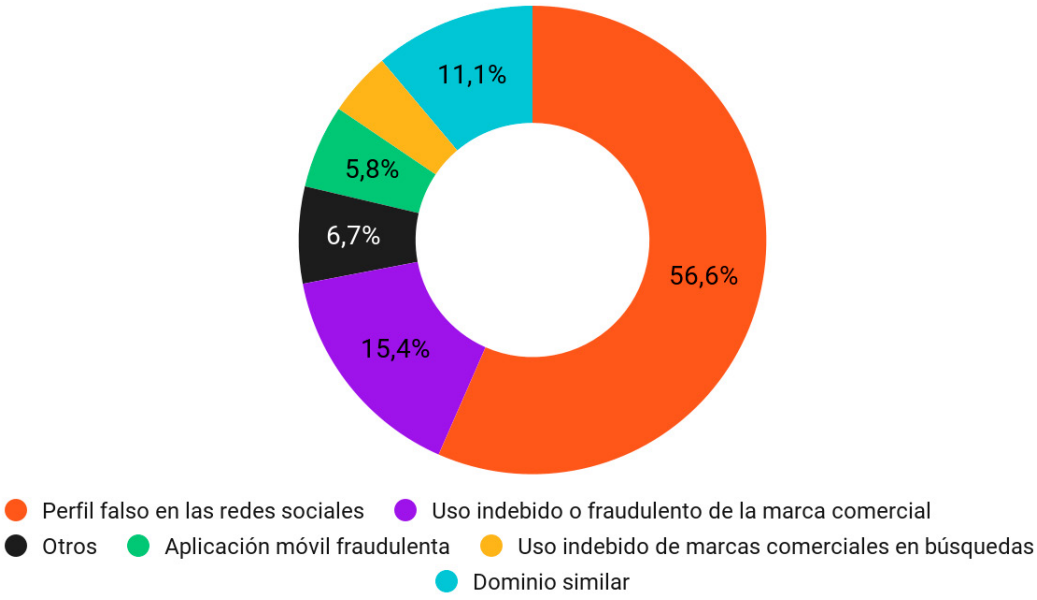

Figura 18. Porcentaje total de incidentes de uso de marca del segundo semestre de 2021.

Glosario

- **Deep web:**
  es la web no accesible mediante mecanismos de búsqueda e indexación (como Google).
- **Dark web:**
  es la web a la que acceden únicamente navegadores específicos, como la red TOR.
- **Phishing:**
  sitio falso y fraudulento enviado con el propósito de capturar datos personales, como contraseñas y números de tarjetas de crédito.
- **Spear phishing:**
  forma de enviar el phishing dirigido a una persona o empresa específica.
- **Malware:**
  software malicioso que se instala en computadoras y se disemina mediante técnicas de ingeniería social. En general, se hacen pasar por marcas financieras para capturar datos sensibles de consumidores.
- **Riesgo digital:**
  peligros que generan perjuicios financieros y están fuera del perímetro de actuación de la empresa. En términos técnicos, todo lo que sucede fuera de la protección de los firewalls.
- **ccTLDs:**
  los country code top-level domain son los dominios principales en Internet utilizados y reservados para países o territorios independientes. Siempre tienen dos letras.
- **ISP (Internet Service Provider):**
  del inglés, Proveedor de Servicios de Internet, este término se refiere a empresas que proveen, a través de sus servicios, acceso a Internet.

¡Acceda al diccionario de riesgos digitales en nuestro blog y vea más definiciones!

Detección y procedimientos

Todas las informaciones incluidas en este informe se obtuvieron a partir del monitoreo diario por parte de Axur de millones de URL y artefactos maliciosos.

Las detecciones se realizan en la web superficial, y en la deep y dark web. Se utilizan tecnologías que permiten automatizar los procesos y aumentar la visibilidad en forma de datos:

- ✓ **Colectores**

  Axur cuenta con una estructura de colectores propios con todas las fuentes de señales posibles (diariamente se procesan millones de emails considerados spam y se evalúan cerca de 780 millones de URL por mes).

- ✓ **Machine learning**

  Axur lo usa para disminuir exponencialmente los tiempos de detección. El procedimiento se realiza a partir del análisis de los componentes de la URL, de elementos en el contenido de las páginas, y del uso de la visión computacional, lo que permite la identificación de patrones que se enseñan y ponen a prueba. Esto posibilita los más elevados niveles de aciertos.

Con estas técnicas, Axur logra entregar resultados precisos y hace posible la visualización de amenazas potenciales e incidentes de manera práctica y clara. Todas las detecciones se realizan en la plataforma Axur One, donde también es posible llevar a cabo las acciones de tratamiento.

Para saber sobre las detecciones de su marca y/o conocer los productos de protección contra riesgos digitales de Axur, contáctenos.

Vea también

Ransomware: ¿Qué es y cómo protegerse?

El ransomware ha sido una amenaza para las empresas de todo el mundo. Entienda exactamente cómo funciona y lo que su empresa debe hacer para protegerse.

Perfiles falsos: el impacto de no eliminarlos

El impacto de los perfiles falsos va mucho más allá del perjuicio financiero. Los daños a la reputación de su empresa, a veces, pueden ser catastróficos.

Actividad criminal en línea en América Latina en 2020

Recuerde el lanzamiento de nuestro último informe con las cifras del año 2020 sobre la actividad criminal en línea y compárelo con los datos de este nuevo informe.

Informe realizado por:

Hugo Moura
Textos

Patrick Santos
Diseño

Sobre Axur

Líder en monitoreo, reacción y eliminación de riesgos y amenazas digitales en Internet, con foco en crear experiencias digitales más seguras para las empresas y sus consumidores.

Mediante el uso de automatizaciones y machine learning, realizamos el monitoreo de la web superficial, así como de la deep y dark web, para ofrecer protección contra riesgos como el uso abusivo de marca, la suplantación de identidad, phishing, aplicaciones fraudulentas, ventas no autorizadas y filtraciones de datos.

Para obtener más información, visite axur.com y conozca el blog Deep Space, blog.axur.com.

Contacto para prensa

Letícia Olivares
+55 51 3012 2987
press@axur.com

Direcciones

EUA
535 Mission Street – 14th floor
San Francisco, CA 94105

Singapura
109 North Bridge Road
Cityhall District, 179097

Brasil
Rua Mostardeiro, 322 – 15º andar
Porto Alegre, RS 90430-000