BeyGoo

Informe

Capítulo 1

Inteligencia de amenazas sobre grupos de infostealer en América Latina

Introducción

En la región, los grupos cibercriminales han ido desarrollándose utilizando diversas estrategias para expandirse en las redes sociales, principalmente Telegram como medio de comunicación preferido.

Desde el punto de vista tecnológico, hemos observado la aparición de una familia de malware conocida como “stealers”, que se enfoca en la extracción de datos desde los navegadores de los usuarios mediante instalaciones silenciosas que no generan alertas en los dispositivos afectados.

En investigaciones recientes, se ha logrado identificar no solo grupos específicos de este tipo de malware, sino también su vinculación con otros tipos de delitos conexos. Estas asociaciones les permiten expandir eficazmente su red de obtención de información de usuarios legítimos. Además, han desarrollado métodos para obtener dinero utilizando técnicas tradicionales como el carding o la venta de tokens fraccionados para acceder a bases de datos.

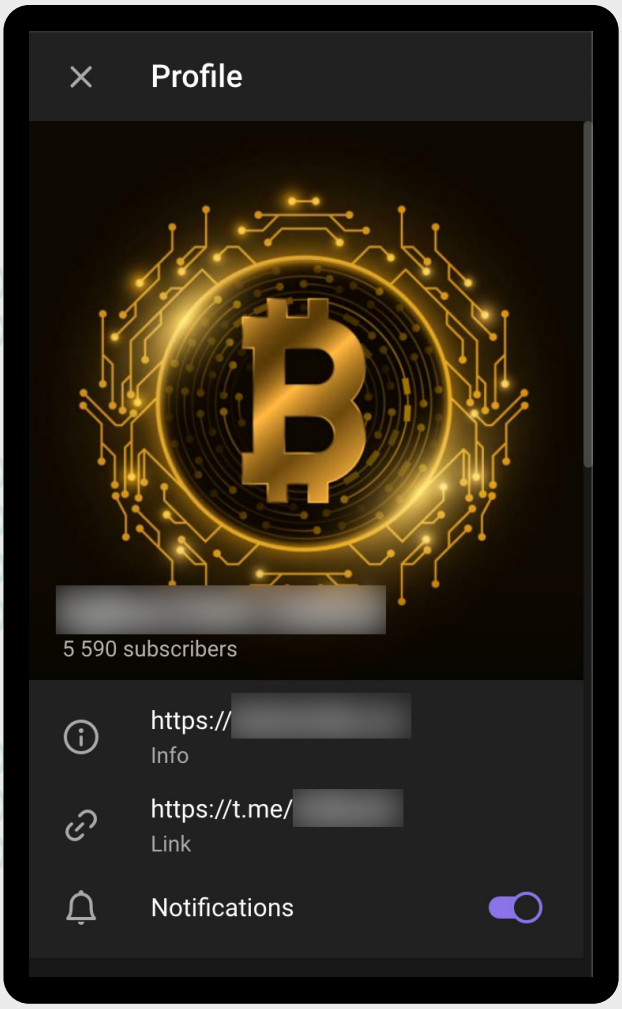
La denominación INFO-STEALERS surge después de compilar bases de datos en formato TXT que contienen correos electrónicos y contraseñas en un solo archivo, el cual puede ser distribuido on demand o bien con fracciones de los archivos para su libre descarga, por lo que es posible, en principio, obtener información sin necesidad de pagar en diferentes grupos.

FASES DE EXFILTRACIÓN DE INFORMACIÓN

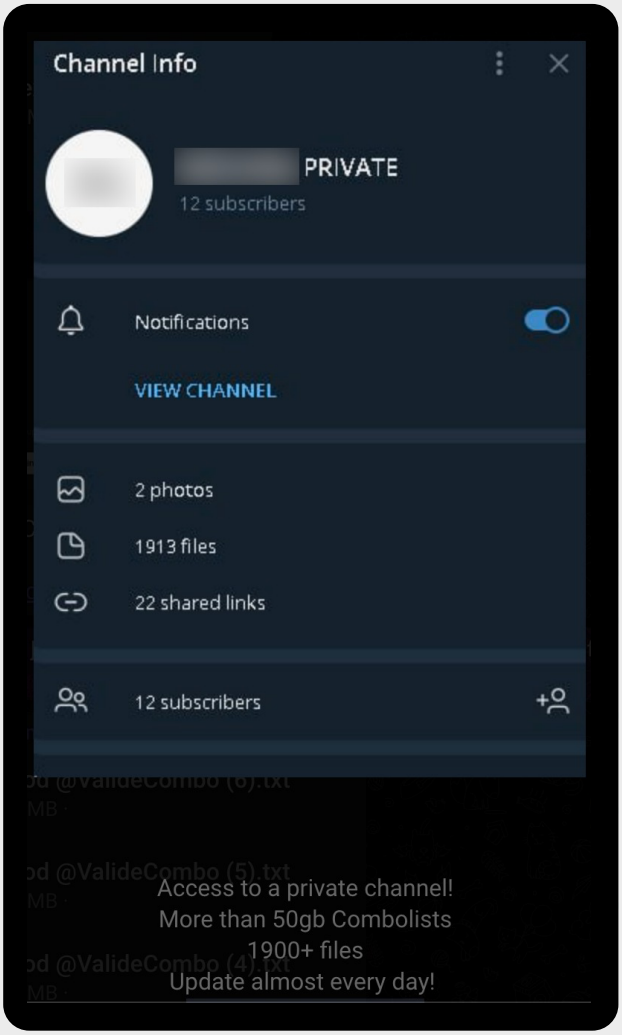
Armado de grupos de Telegram

Analizando uno de los grupos más prolíficos, con 5557 suscriptores y alcance en diferentes países, que ha tenido un impacto significativo en empresas como Google, Microsoft, Yahoo, Netflix, entre otras.

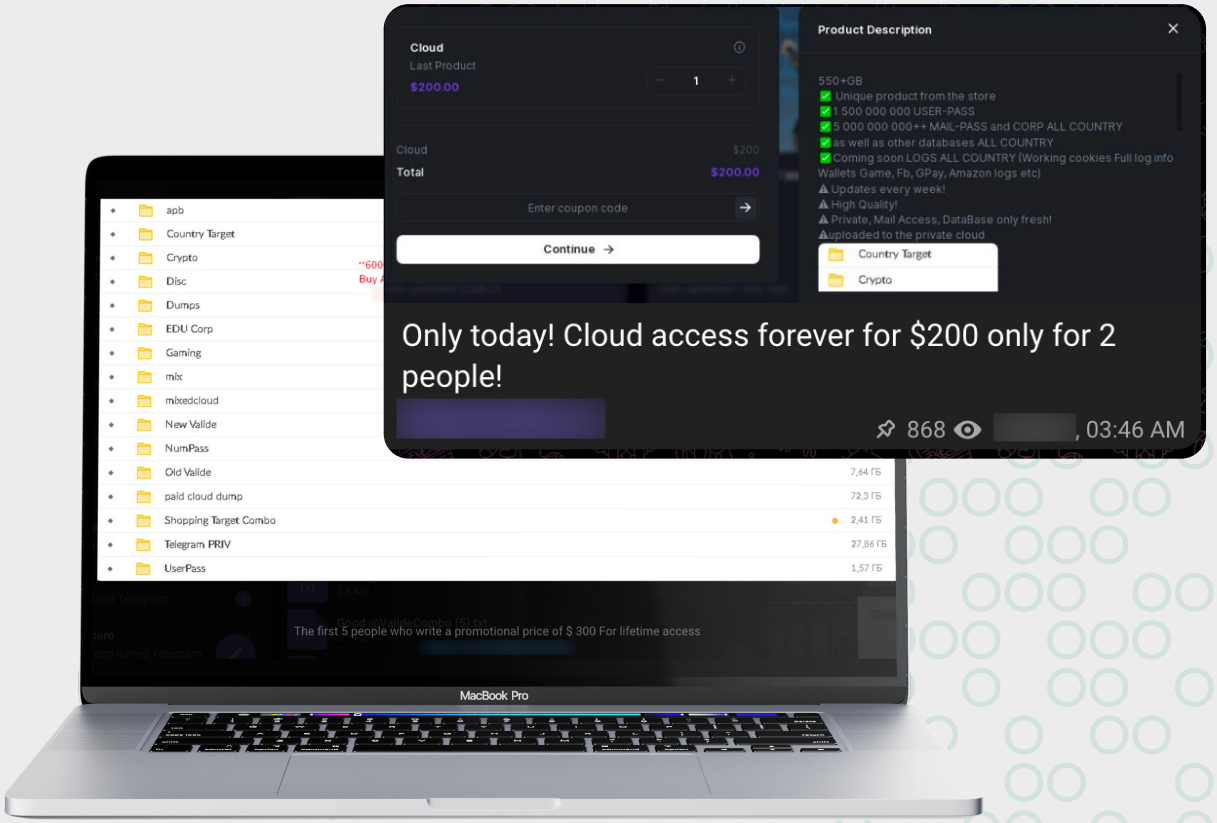
Este grupo ha logrado extraer alrededor de 3600 bases de datos en formato TXT, denominadas combolist, con un total de aproximadamente 5 gigabytes de información.



En el mismo, se encuentra un sitio web que facilita el acceso al registro para convertirse en usuarios de la plataforma, con opciones para consumir una variedad de productos. También ofrece acceso a un grupo privado en Telegram, acceso a la nube y acceso al shopping de crypto target, y comercios anexos podrían estar relacionados con actividades de ciberdelito, destinados a financiar la estructura general del grupo.

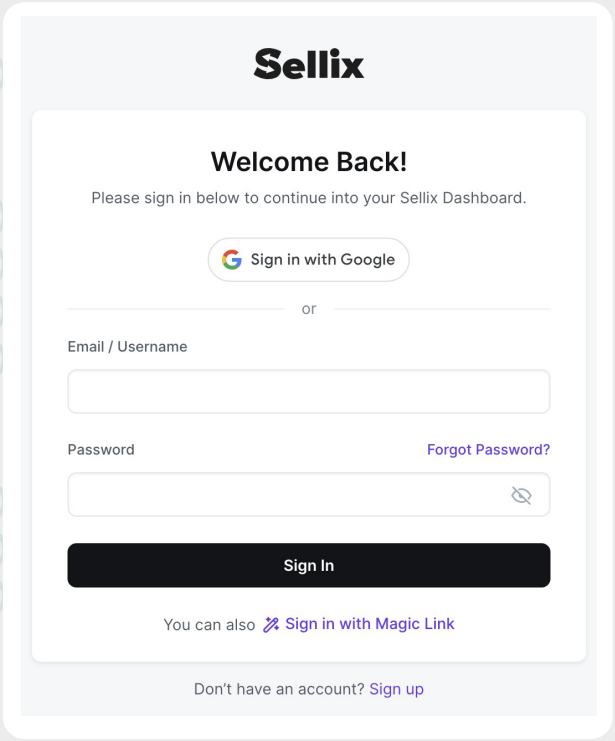


Inteligencias de amenazas sobre actores stealers en América Latina



El registro del dominio se presenta en dos niveles: en primer lugar, el dominio **Principal** del grupo, donde los componentes técnicos hacen referencia **Names Servers** vinculados a Rusia, con registros desde el año 2022

La empresa de hosting MCHOST ofrece un acceso al hosting por un valor mínimo de 158 rublos (USD 0.011). Es importante destacar que este servicio de hosting también ofrece servicios de VPS (Servidor Privado Virtual), que permiten una administración autónoma de servidores, así como servicios preferenciales adicionales.

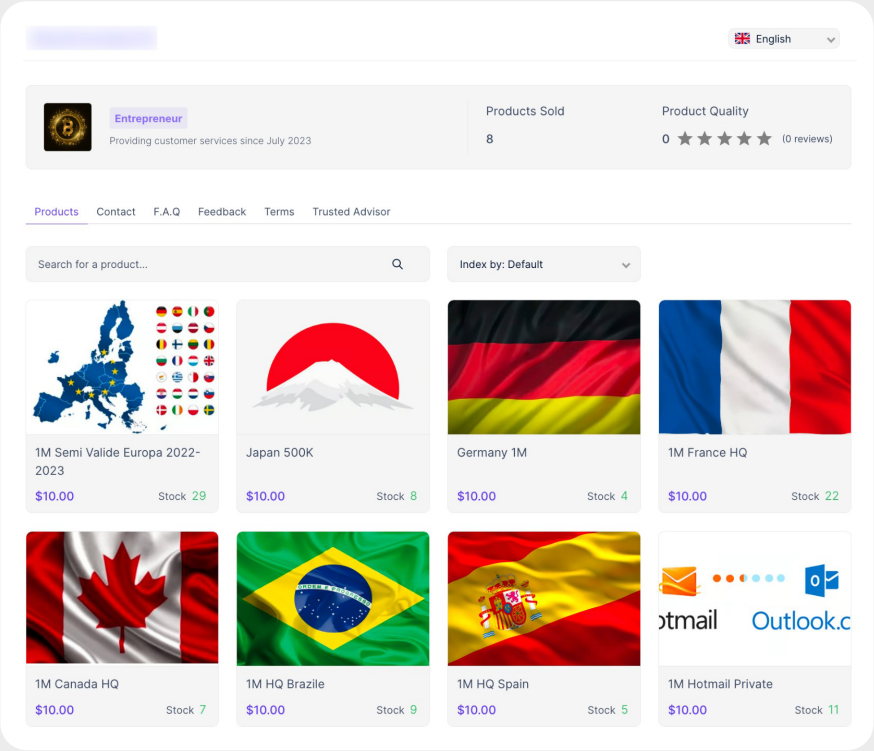


En un segundo nivel, se encuentra el dominio del registro de usuarios, el cual pertenece a una empresa llamada SELLIX. Esta empresa ofrece una estructura de comercio electrónico tipo Marketplace, proporcionando todas las herramientas necesarias para la gestión de negocios digitales.

La empresa, debidamente constituida en Estados Unidos, tiene presencia en plataformas de redes sociales como LinkedIn, Facebook e Instagram, además de contar con aplicaciones disponibles en Google Store. Esto sugiere que es un proveedor legítimo de comercio electrónico. Sin embargo, es importante tener en cuenta que la misma tecnología que utilizan empresas legítimas puede ser aprovechada por grupos de cibercriminales, pasando desapercibida en la internet tradicional o clearnet

Al entender la estructura de los dominios y analizar la forma en que se publican las combolist, podemos concluir que el negocio principal del grupo no radica en la venta directa de información en formato combolist. Más bien, esto parece ser utilizado como un anzuelo para ofrecer servicios de venta de información más complejos. Esto puede explicar por qué se permiten posibles descargas de todas las bases sin necesidad de registro.

Además, al analizar los enlaces proporcionados por el grupo de Telegram, observamos promociones de acceso a diferentes productos alojados dentro del Marketplace que ofrece Sellix

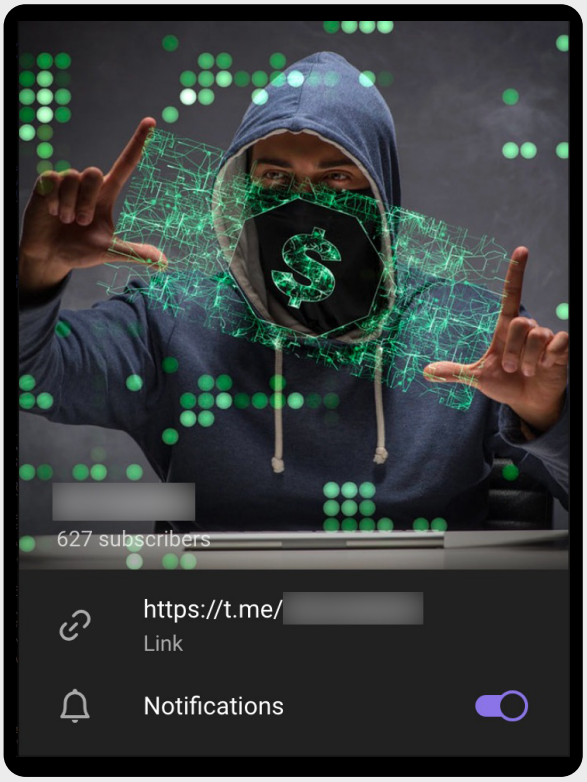


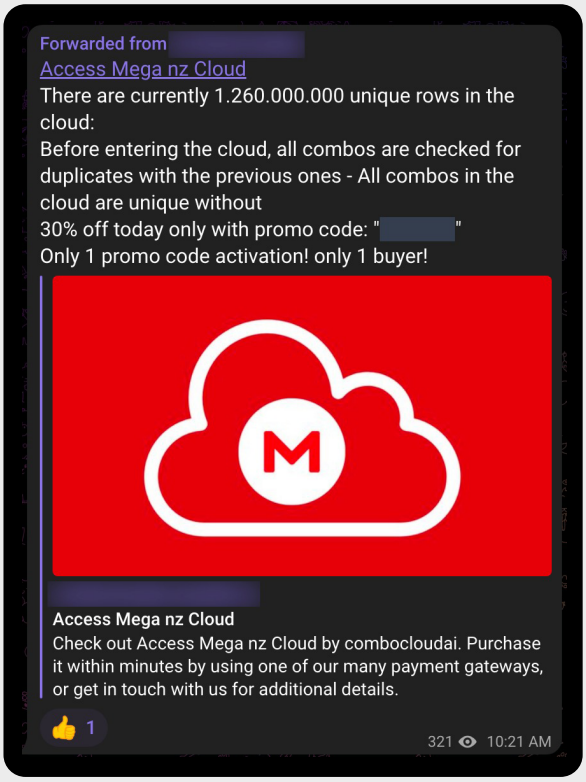
De los enlaces proporcionados se desprende otro dominio de venta de combo, con un diseño diferente. Esto sugiere que el grupo cibercriminal podría estar vendiendo su metodología de trabajo para obtener combolist regionales, o bien, diversificarse para vender en otras regiones, como es el caso de:

En este sitio podemos dar cuenta que las combolist están a la venta.

Por otro lado, el grupo ofrece otros enlaces a grupos de Telegram con menor cantidad de suscriptores lo cual nos hace pensar en tres posibles variables:

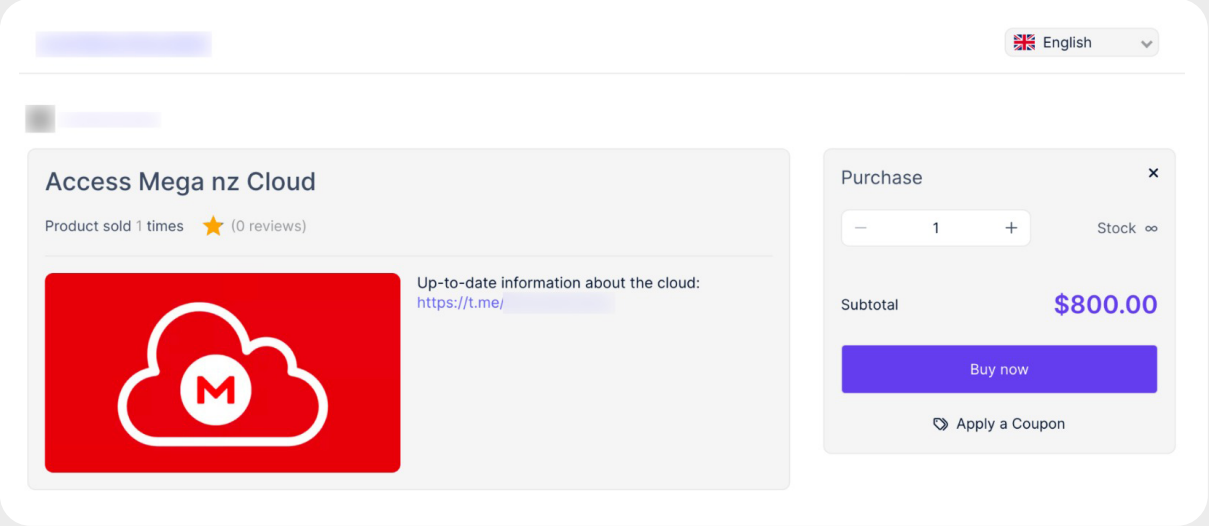
- Regionalización
- Venta de la metodología
- Productos exclusivos según perfil de cliente



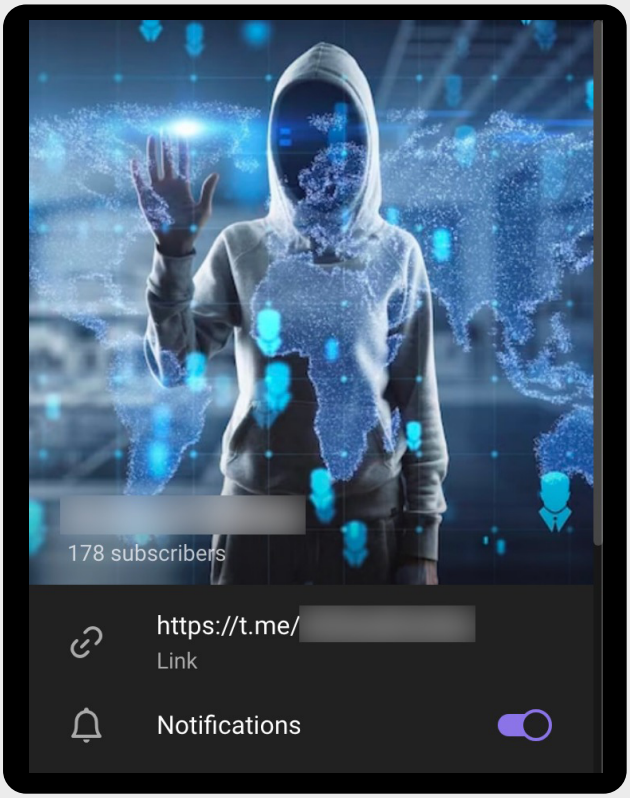


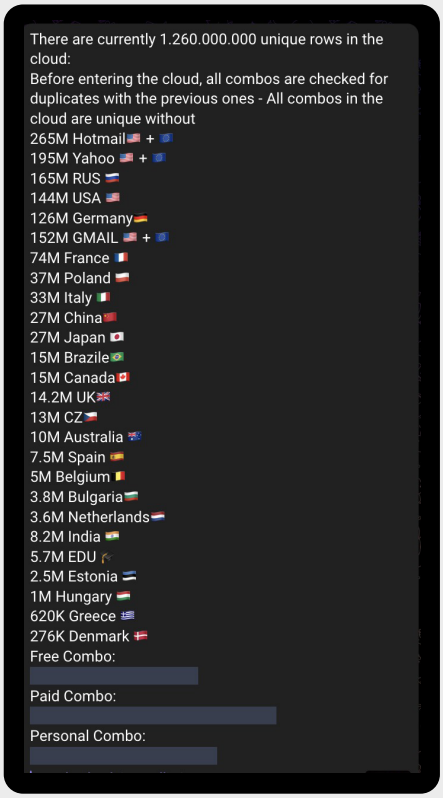
A medida que avanzamos en el análisis del grupo de Telegram, encontramos enlaces que hacen referencia a tecnología, como el acceso a bases en MEGA, también ubicados dentro del grupo principal que estamos analizando.

Al ingresar al enlace, nos encontramos con el acceso para obtener las bases de datos, pero también nos encontramos con un acceso nuevo a otro grupo de Telegram.



Cuenta con muy pocos miembros, pero con la base de datos más grande de Estados Unidos y la Unión Europea.





Be ***proactive,***
Be **safe,**
BeyGoo.

Solicitá tu Quick View y

¡Vive el Poder de la Protección de Riesgos Digitales!

beygoo.io

hello@beygoo.io

@beygooapp